Stylianakis, Charalampos (2016) *Braid groups, mapping class groups, and Torelli groups.* PhD thesis.

Braid groups, mapping class groups, and Torelli groups

by

Charalampos Stylianakis

A thesis submitted to the
College of Science and Engineering
at the University of Glasgow
for the degree of
Doctor of Philosophy

April 2016

To my parents and my sister

Abstract

This thesis discusses subgroups of mapping class groups of particular surfaces. First, we study the Torelli group, that is, the subgroup of the mapping class group that acts trivially on the first homology. We investigate generators of the Torelli group, and we give an algorithm that factorizes elements of the Torelli group into products of particular generators.

Furthermore, we investigate normal closures of powers of standard generators of the mapping class group of a punctured sphere. By using the Jones representation, we prove that in most cases these normal closures have infinite index in the mapping class group. We prove a similar result for the hyperelliptic mapping class group, that is, the group that consists of mapping classes that commute with a fixed hyperelliptic involution. As a corollary, we recover an older theorem of Coxeter (with 2 exceptional cases), which states that the normal closure of the m^{th} power of standard generators of the braid group has infinite index in the braid group.

Finally, we study finite index subgroups of braid groups, namely, congruence subgroups of braid groups. We discuss presentations of these groups and we provide a topological interpretation of their generating sets.

Acknowledgement

I would like to express my ineffable gratitude towards my PhD advisor Tara Brendle. Her guidance, patience, aid, and support throughout my PhD is of extreme importance and is greatly appreciated.

I am grateful to my parents, Charalampos Stylianakis, Maria Stylianaki, and my sister Irini Stylianaki for their support and their belief in me throughout this long journey. Without them I would not get that far and make my childhood dream come true.

I would also like to thank my office mates Duncan McCoy, Paul Slevin, Paul Gilmartin, Amene Asgari, Ying Shi, Jorge Castillejos for the lovely time we had all together. Special thanks to Duncan McCoy who was always there with an answer in crucial moments of my research. I am also grateful to my friends Gabrielle Tornetta, Charis Chanialidis, Nikos Papasarantopoulos, Sotiria Karafoulidou, Dimitrios Gkoutzelis, Konstantina Noutsi, Katerina Kostaki, George Chatzitheodosiou, Yana Staneva, and Stephanie Sherbanova for their encouragement and support during my PhD. The time they spent for and with me is really precious.

I would like to express my very great appreciation to Louis Funar, Gwyn Bellamy, Brendan Owens, and Andrew Wilson for the helpful conversations and their support.

Finally, I would like to thank my examiners, Vaibhav Gadre and Paolo Bellingeri for their valuable comments on my thesis.

Declaration

This thesis is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution. Except where explicit reference is made to the contribution of others.

Charalampos Stylianakis

Contents

List of Figures

Chapter 1

Introduction

Let $\Sigma_{g,n}^b$ be a surface of genus g with n marked points and b boundary components. In this thesis we are interested in the cases $g \geq 0, n \geq 0$ and $b = 0, 1, 2$. The mapping class group of $\Sigma_{g,n}^b$, denoted by $\mathrm{Mod}(\Sigma_{g,n}^b)$, consists of those isotopy classes of homeomorphisms that preserve both the orientation of $\Sigma_{g,n}^b$ and the set of marked points, and fix the boundary pointwise. If $n = 0$ we will write Σ_g^b, if $b = 0$ we will write $\Sigma_{g,n}$, and if $b = n = 0$, we will simply write Σ_g.

In the first part of this thesis we study the Torelli group $\mathcal{I}(\Sigma_g^b)$, that is, the subgroup of $\mathrm{Mod}(\Sigma_g^b)$ that acts trivially on the homology group $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ when $b = 0, 1$. Particularly, we will focus on the generators of $\mathcal{I}(\Sigma_g^b)$. In the second part we will study the structure of the groups $\mathrm{Mod}(\Sigma_{0,n}^1)$, and $\mathrm{Mod}(\Sigma_{0,n})$ via their linear representations. It is important to mention that $\mathrm{Mod}(\Sigma_{0,n}^1)$ is isomorphic to the braid group B_n, while $\mathrm{Mod}(\Sigma_{0,n})$ is a quotient of B_n.

Part 1

Let T_c denote a Dehn twist about a curve c. We give the definition of a Dehn twist in Chapter 3. If c is a nonseparating simple closed curve, then we can choose a finite number of T_c (one for each c) to generate $\mathrm{Mod}(\Sigma_g^b)$ for $b = 0, 1$ [30, 42]. The group $\mathrm{Mod}(\Sigma_g^b)$ acts on the surface Σ_g^b, and hence, on $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$.The latter action gives the following representation:

$$\mathrm{Mod}(\Sigma_g^b) \to \mathrm{Aut}(\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})).$$

If $b = 0, 1$, the action of $\mathrm{Mod}(\Sigma_g^b)$ on $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ preserves a symplectic form. Thus, the above representation is symplectic and is given by

$$\Phi : \mathrm{Mod}(\Sigma_g^b) \to \mathrm{Sp}_{2g}(\mathbb{Z}).$$

If $g = 1$ and $b = 0$, then Φ is an isomorphism [20, Theorem 2.5]. Otherwise, the representation Φ is not faithful. We define $\ker(\Phi) = \mathcal{I}(\Sigma_g^b)$ and we call it the Torelli group.

The work of Powell and Birman shows that the Torelli group is infinitely generated by two conjugacy classes of elements. Particularly, $\mathcal{I}(\Sigma_g^b)$ is generated by Dehn twists about separating curves, and bounding pair maps, that is, elements of the form $T_c T_{c'}^{-1}$ such that the curves c, c' are homologous, meaning that they represent the same element in $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ [51, Theorem 2]. The latter result was improved by Johnson, who proved that bounding pair maps suffice to generate the Torelli group $\mathcal{I}(\Sigma_g^b)$ when $g \geq 3$ [33, Theorem 2]. Later, Johnson proved that for $g \geq 3$ and $b = 0, 1$ the Torelli group $\mathcal{I}(\Sigma_g^b)$ is finitely generated by providing a large set S of bounding pair maps [35, Main theorem]. The cardinality of S grows exponentially with respect to the genus g of the surface Σ_g^b. Since Johnson proved that the rank of $\mathrm{H}_1(\mathcal{I}(\Sigma_g^b), \mathbb{Z}/2)$ grows cubically with respect to g [34, Theorem 4], he conjectured that there should be a smaller generating set for $\mathcal{I}(\Sigma_g^b)$ which grows cubically with respect to g. In the same paper Johnson proved that $\mathcal{I}(\Sigma_3)$ is generated by 35 elements, while $\mathcal{I}(\Sigma_3^1)$ is generated by 42 elements, and these are the minimum number of such elements.

Recently Putman proved the Johnson's conjecture by proving that $\mathcal{I}(\Sigma_g)$ is generated by $57\binom{g}{3}$ elements [54, Theorem A], and later Church-Putman improved the latter result by proving that $\mathcal{I}(\Sigma_g)$ is generated by $42\binom{g}{3}$ elements [14, Theorem H]. Particularly, they considered the set $G = \bigcup_{1 \leq i \leq \binom{g}{3}} \mathcal{I}(\Sigma_g) \cap \mathcal{I}(S_i)$, where S_i are surfaces of genus 3 with 1 boundary component embedded in Σ_g. Then they proved that every element of $\mathcal{I}(\Sigma_g)$ admits a factorization of elements of G.

Church-Putman's proofs do not include examples of elements of $\mathcal{I}(\Sigma_g)$ as a product of elements of G. The goal of Part 1 of the thesis is to provide such examples. More precisely, In Section 3.3.3 we give an algorithm for factoring certain elements of $\mathcal{I}(\Sigma_4)$ into G. In Section 3.3.4 we use this algorithm to give a constructive proof of Church-Putman's theorem:

Theorem A *The groups $\mathcal{I}(\Sigma_g)$ and $\mathcal{I}(\Sigma_g^1)$ are generated by $42\binom{g}{3}$ elements.*

Theorem A is restated as Theorem 3.6 in this thesis. The proof of Theorem A enables us to seek a better result for $\mathcal{I}(\Sigma_g)$. More particularly, we can construct relations between generators of $\mathcal{I}(\Sigma_g^1)$ to minimize the generating set of $\mathcal{I}(\Sigma_g)$ further.

Part 2

In Part 2 we study the structure of the mapping class groups $\mathrm{Mod}(\Sigma_{0,n}^1)$ and $\mathrm{Mod}(\Sigma_{0,n})$, where $\Sigma_{0,n}^1$ is the n^{th} punctured disc, $\Sigma_{0,n}$ is the n^{th} punctured sphere, and the hyperelliptic mapping class group $\mathrm{SMod}(\Sigma_g^b)$ for $b = 0, 1, 2$.

Motivation. The group $\mathrm{Mod}(\Sigma_{0,n}^1)$ is isomorphic to the braid group B_n on n strands. A result by Artin states that B_n is generated by half-twists, that is, homeomorphisms that interchange two marked points [11, Sections 1.2, 1.3]. The braid group B_n surjects onto S_n and the kernel is called the pure braid group PB_n. The pure braid group is generated by squares of half-twists. Thus, the quotient of B_n by the normal closure of a square of a half twist is isomorphic to the symmetric group S_n. Motivated by the latter fact, Birman asked whether the normal closure of T_c^2 in $\mathrm{Mod}(\Sigma_g)$ has infinite index if $g \geq 3$ [9, Question 28]. It is well known that the normal closure of T_c^2 has finite index in $\mathrm{Mod}(\Sigma_g)$ when $g = 1$ or 2.

Humphries answered Birman's question by proving that, in fact, the normal closure of T_c^2 has finite index in $\mathrm{Mod}(\Sigma_g)$ for every g [30, Theorem 1]. Let $\mathrm{SMod}(\Sigma_g)$ denote the hyperelliptic mapping class group, that is, those elements of $\mathrm{Mod}(\Sigma_g)$ that commute with a fixed hyperelliptic involution (an element of order 2 of $\mathrm{Mod}(\Sigma_g)$ that acts as $-\mathrm{Id}$ on $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$). In the same paper Humphries used the fact that $\mathrm{Mod}(\Sigma_2) = \mathrm{SMod}(\Sigma_2)$ to show that if $m \geq 4$, then the normal closure of T_c^m has infinite index in $\mathrm{Mod}(\Sigma_2)$ [30, Theorem 4]. In fact, Humphries used the Jones representation for $\mathrm{Mod}(\Sigma_{0,2g+2})$ and proved that the quotient of $\mathrm{Mod}(\Sigma_{0,6})$ by the normal closure of the m^{th} power of a half twist is an infinite group. His result follows by the surjective homomorphism

$$\mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2}),$$

defined by the double cover $\Sigma_g \to \Sigma_{0,2g+2}$. In Theorem 6.5 in Chapter 6, we extend Humphries' result as follows:

Theorem B *The normal closure of the m^{th} power of a half-twist has infinite index in* $\mathrm{Mod}(\Sigma_{0,n})$ *if $n \geq 6$ is even and $m \geq 5$.*

In fact, in the same chapter we extend this result further, namely, by proving Theorem 6.7, which is stated as Theorem C below.

Theorem C *The quotient* $\mathrm{Mod}(\Sigma_{0,n})$ *by the closure of the* m^{th} *power of a half-twist contains a free group of rank 2, if* $n \geq 6$ *is even, and* $m \notin \{2,4,6,10\}$ *if* m *is even, and* $m \notin \{1,3\}$ *if* m *is odd.*

Theorem C gives a stronger result than Theorem B for some m. Nevertheless, the methods we use to prove them are different. The proof of Theorem B uses an explicit matrix calculation of the Jones representation in Chapters 5 and 6. In fact we give a new approach to the Jones representation by using a different definition of the Hecke algebras and we use the notion of W-graphs introduced by Kazhdan-Lusztig. In the proof of Theorem C we show how to modify the Burau representation, so that its image is contained in the Jones representation.

Construction of the Jones representation. Let $H(q, 2g+2)$ be a Hecke algebra with a complex parameter q, that is, the quotient of the group algebra $\mathbb{Z}[q^{\pm 1}]B_n$ by the relation $\sigma_i^2 - 1 - (q - q^{-1})\sigma_i$. There is a representation $B_{2g+2} \to H(q, 2g+2)$ from the braid group into the group of units of $H(q, 2g+2)$. We can think of $H(q, 2g+2)$ as a quotient of the group algebra of B_{2g+2} over $\mathbb{Z}[q^{\pm 1}]$. Thus, any representation of $H(q, 2g+2)$ will give a representation for B_{2g+2}. We can think of $\mathrm{Mod}(\Sigma_{0,2g+2})$ as a quotient group of the braid group B_{2g+2}. Jones observed that in some cases we can modify the representations of $H(q, 2g+2)$ so that we can define representations for $\mathrm{Mod}(\Sigma_{0,2g+2})$ [38, Section 10].

Assume that q is not a root of unity. The set of irreducible representations of the Hecke algebra $H(q, 2g+2)$ is in bijective correspondence with the set of Young diagrams of size $2g+2$. When the Young diagram has the shape of a rectangle, we show that under a modification, the corresponding irreducible representation of $H(q, 2g+2)$ gives a representation of $\mathrm{Mod}(\Sigma_{0,2g+2})$. We also explain a method for explicitly computing matrices of the irreducible representations of $H(q, 2g+2)$ in this case by using the notion of W-graphs (see Chapter 5). If $g = 2$, we explicitly calculate the matrices of the representation of $\mathrm{Mod}(\Sigma_{0,2g+2})$. Our calculations are equivalent to those of Jones, but we make different choices of parameters and hence, the resulting matrices are slightly different. When $g \geq 3$, the calculations are much more complicated and we will not compute the full matrices explicitly. However, we will show that the matrices have a particular block form for $g \geq 3$ that is sufficient for the required calculations (see

Theorem 5.6).

Results for braid groups. As mentioned earlier, the braid group B_n is isomorphic to $\mathrm{Mod}(\Sigma_{0,n}^1)$. A similar result as in Theorem B holds for the braid group B_n. Coxeter used hyperbolic geometry to prove that the normal closure of the m^{th} power of a half-twist has finite index in B_n if and only if $(n-2)(m-2) < 4$ [16, Section 10]. As a corollary of Theorem B, we recover Coxeter's theorem when $n \geq 4$ and $m \geq 5$.

Theorem D *The normal closure of the m^{th} power of a half-twist has infinite index in the braid group B_n, if $n \geq 4$, and $m \geq 5$.*

Theorem D is Corollary 6.8 in this thesis. Also, the proof of Theorem D is independent from Coxeter's proof.

By Theorem D we have that the normal closure of the m^{th} power of a half twist in the braid group B_n has infinite index when $n \geq 4$ and $m \geq 5$. By considering subgroups of B_n generated by the normal closure of more braids, we can obtain finite index subgroups. In this thesis, specifically, in Chapter 8, we are interested in a particular class of finite index subgroups, namely congruence subgroups of braid and symplectic groups.

We briefly give the definition of congruence subgroups. Let $G(\mathbb{Z})$ be a subgroup of $GL_k(\mathbb{Z})$. The projection $\mathbb{Z} \to \mathbb{Z}/d$ extends to projections $GL_k(\mathbb{Z}) \to GL_k(\mathbb{Z}/d)$ and $G(\mathbb{Z}) \to G(\mathbb{Z}/d)$ with kernels denoted by $GL_k(\mathbb{Z})[d]$ and $G(\mathbb{Z})[d]$ respectively. The groups $GL_k(\mathbb{Z})[d]$ and $G(\mathbb{Z})[d]$ are called level-d *principal congruence subgroups* of $GL_k(\mathbb{Z})$ and $G(\mathbb{Z})$, respectively. In general a finite index subgroup H of G is a level-d congruence subgroup if H contains a level-d principal congruence subgroup.

Now consider braid groups B_n. As we see in Chapter 4, B_n is identified with a subgroup of $\mathrm{Aut}(F_n)$, where F_n is the free group of rank n. In fact, this identification arises from the action of B_n on $\pi_1(\Sigma_{0,n}^1) \cong F_n$, which induces an injective homomorphism $B_n \hookrightarrow \mathrm{Aut}(F_n)$. Consider a finite index characteristic subgroup H of F_n. The projection $F_n \to F_n/H$ extends to a homomorphism $B_n \to \mathrm{Aut}(F_n/H)$, and the kernel is called a congruence subgroup of B_n [46, Section 2]. It is proved that every finite index subgroup of PB_n (the subgroup of B_n that fixes the punctures of the disc $\Sigma_{0,n}^1$) is a congruence subgroup [46, Theorem 1.1].

In Chapter 8 we focus on a particular class of congruence subgroups of B_n, namely the kernels of $B_n \to \mathrm{Sp}_{n-1}(\mathbb{Z}/d)$ if n is odd, and $B_n \to (\mathrm{Sp}_n(\mathbb{Z}/d))_y$ if n is even, where $(\mathrm{Sp}_n(\mathbb{Z}/d))_y$ is the stabilizer subgroup of $\mathrm{Sp}_n(\mathbb{Z}/d)$ fixing one vector y. We denote the kernels by $B_n[d]$ and we call them the *level-d congruence subgroups* of braid groups B_n.

Wanjryb found a finite presentation of $\mathrm{Sp}_{n-1}(\mathbb{Z}/p)$, $(\mathrm{Sp}_n(\mathbb{Z}/p))_y$ as a quotient of the braid group when p is prime [56, Theorem 1]. This presentation gives normal generators of the group $B_n[p]$. Our first result on the on the congruence subgroups is presented below in Theorem E, which is given as Theorem 8.9 in the thesis.

Theorem E. *There is a topological interpretation of the normal generators of $B_n[p]$, when p is prime.*

Theorem E was inspired by the work of Powell for the Torelli group. Birman had found a presentation of the symplectic group over $\mathbb{Z}$ and this presentation gives normal generators of the Torelli group. Then, Powell gave a topological interpretation of those normal generators.

The number of the generators we describe in Theorem E is infinite. When $n = p = 3$ we obtain finite number of generators for $B_3[3]$. Furthermore, we make some progress on the result of Wanjryb on the presentation of $\mathrm{Sp}_n(\mathbb{Z}/p)$.

Theorem F. *The groups $\mathrm{Sp}_{n-1}(\mathbb{Z}/p)$ if n is odd and $(\mathrm{Sp}_n(\mathbb{Z}/p))_y$ if n is even, admit a presentation as a quotients of the pure braid group PB_n.*

This result is given as Theorem 8.13 in the thesis. As we see in Section 8.2.4, Theorem F is a step closer to finding normal generators of $B_n[m]$ for $m = 2p_1p_2...p_k$ and $m = 4p_1p_2...p_k$, where p_i are prime numbers. In the case $m = 2p$, where p is prime we achieve the latter claim by finding normal generators for $B_n[2p]$.

Factor groups of congruence subgroups of braid groups. Ultimately, we calculate factor groups of congruence subgroups of braid groups.

In Chapter 4 we show that the braid group B_n surjects onto the symmetric group S_n by sending half-twists in B_n to transpositions in S_n. The kernel of this map is well known to be the pure braid group PB_n. Also, by a result established by A'rnold the group PB_n is isomorphic to $B_n[2]$ [4]. See also [12, Section 2] for further discussion. Therefore, we have $B_n/B_n[2] \cong S_n$. We generalize this result as stated in the following theorem, which is Theorem 8.15 in the thesis.

Theorem G. For p prime number, the group $B_n[p]/B_n[2p]$ is isomorphic to S_n.

Part I

The Torelli group

Chapter 2

Algebraic topology and the symplectic group

In this chapter we introduce basic background material to be utilized throughout the thesis. In the first three sections we will recall the basics of surfaces, curves, fundamental groups, and the homology groups of surfaces. In Section 2.4 we define the symplectic group of matrices as a subgroup of the automorphism group of a homology group.

2.1 Surfaces and curves

For $b, n, g \in \mathbb{Z}^{\geq 0}$ we denote by $\Sigma_{g,n}^b$ an orientable surface with b boundary components, n punctures, and g genus holes as indicated in Figure 2.1. If $n = 0$ or $b = 0$ we omit the index. For example, Σ_g denotes the surface of genus g without punctures and boundary components. According to the classification theorem of surfaces, every connected orientable surface is homeomorphic to $\Sigma_{g,n}^b$ for some $b, n, g \in \mathbb{Z}^{\geq 0}$ [45, Theorem 5.1]. In this thesis we only consider the cases $g \geq 0, n \geq 0$ and $0 \leq b \leq 2$.

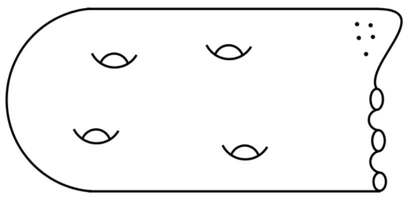


Figure 2.1: An example of a surface of genus 4, 3 boundary components, and 5 punctures.

Curves, and arcs. Consider a surface Σ. A *path* γ is an embedding $\gamma : [0, 1] \to \Sigma$. If $\gamma(0) = \gamma(1)$, then γ is called a *simple closed curve*, otherwise γ is called an *arc*.

Two curves $\gamma, \gamma' : [0,1] \to \Sigma$ are homotopic if $F : [0,1] \times [0,1] \to \Sigma$ is a homotopy, such that $F(x,0) = \gamma(x)$ and $F(x,1) = \gamma'(x)$, for all $x \in [0,1]$. A curve that is not homotopic to a boundary component or a puncture is called *essential*. We denote a homotopy class of a curve γ by $[\gamma]$. Let $c, d \in \Sigma$ be two curves. We define the *geometric intersection number* $i([c],[d])$ by the following formula:

$$i([c],[d]) = \min\{c \cap d \mid c \in [c], d \in [d]\}.$$

Consider two oriented simple closed curves a, b. We define the *algebraic intersection number* to be the sum of the indices of the intersection points of a, b, where an intersection point has index $+1$ if the orientation of the intersection agrees with the orientation of Σ, and the intersection point has index -1 otherwise.

2.2 Fundamental groups

In this section we recall the fundamental group of a surface Σ, and its unit tangent bundle $U\Sigma$.

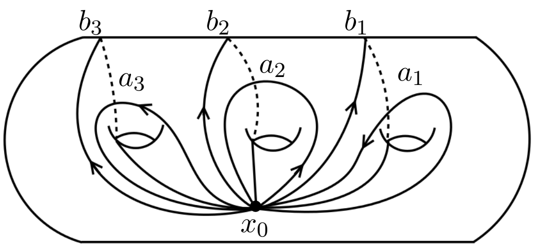


Figure 2.2: Generators of the fundamental group.

Fundamental group of a surface Σ. Let Σ_g be a surface of genus g. Consider the simple closed curves a_i, b_i indicated in Figure 2.2. It is well known that the presentation

$$\langle a_1, b_1, a_2, b_2, ..., a_g, b_g \mid \prod_{i=1}^{g} [a_i, b_i] = 1 \rangle$$

characterizes the fundamental group $\pi_1(\Sigma_g, x_0)$, [45, Example 5.3].

Consider a surface Σ_g^1 of genus g with one boundary component. If we attach a disc on the boundary of Σ_g^1, we obtain a surface Σ_g. Hence, we have an inclusion $\Sigma_g^1 \hookrightarrow \Sigma_g$. We let x_1 be a fixed point on the boundary of Σ_g^1, and x_0 be a fixed point in the interior of Σ_g, obtained by x_1 after we attach the disc. Thus, we get a surjective homomorphism

$\phi_* : \pi_1(\Sigma_g^1, x_1) \to \pi_1(\Sigma_g, x_0)$ [29, Proposition 1.26]. Consider the curves a_i, b_i indicated in Figure 2.3 on the top. We have that $\prod_{i=1}^{g}[a_i, b_i]$ is a separating simple closed curve in Σ_g^1, parallel to its boundary. The element $\prod_{i=1}^{g}[a_i, b_i]$ is trivial in $\pi_1(\Sigma_g, x_0)$, but it is not trivial in $\pi_1(\Sigma_g^1, x_1)$. From the presentation of $\pi_1(\Sigma_g, x_0)$ above we deduce that the kernel of the map ϕ_* is generated by $\prod_{i=1}^{g}[a_i, b_i]$. Therefore, the group $\pi_1(\Sigma_g^1, x_1)$ is a free group of rank $2g$, with generators a_i, b_i, where $i \leq g$.

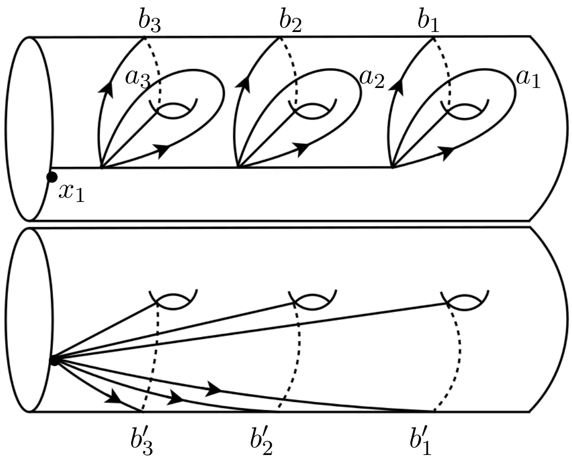


Figure 2.3: Generators of the fundamental group.

We mention here that the curves b'_i shown in the bottom of Figure 2.3 are obtained by composing the curves a_i, b_i. More particularly, $b'_k = \prod_{i=1}^{k-1}[a_i, b_i]a_k b_k a_k^{-1}$. We use this fact later on in Section 3.3.

In what follows advice Figure 2.4. Consider a surface Σ_g^2 of genus g with two boundary components, and choose a point x_0 in one of the boundaries of Σ_g^2. We denote by q_1 the boundary component including x_0, and by q_2 the boundary component which does not include x_0. Consider the inclusion $\Sigma_g^2 \hookrightarrow \Sigma_g^1$, induced by gluing a disc on q_2. Also we denote by δ_2 the simple closed curve starting at x_0, going around q_2, and ending at x_0. By orienting δ_2 appropriately, the product $\prod_{i=1}^{g}[a_i, b_i]\delta_2$ is a simple closed curve starting at x_0 going around q_1 and ending up to x_0. The curve δ_2 is nontrivial in Σ_g^2, but becomes trivial in Σ_g^1. We have that $\pi_1(\Sigma_g^2, x_0)$ is a free group generated by δ_2, a_i, b_i where $i \leq g$, and the kernel of the epimorphism

$$\pi_1(\Sigma_g^2) \to \pi_1(\Sigma_g^1)$$

is generated by δ_2.

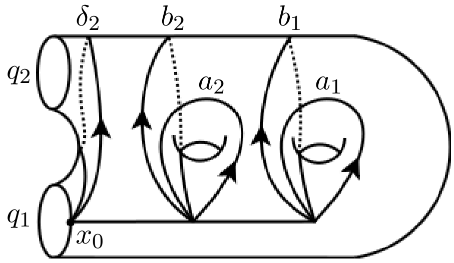


Figure 2.4: Generators of the fundamental group of a surface with two boundary components.

Commutator subgroups of $\pi_1(\Sigma_g^b)$. For $b \leq 2$, consider the fundamental group $\pi_1(\Sigma_g^b)$, generated by a_i, b_i if $b = 0, 1$, and by a_i, b_i, δ_2 if $b = 2$. Consider the commutator subgroup $\pi_1'(\Sigma_g^b) = [\pi_1(\Sigma_g^b), \pi_1(\Sigma_g^b)]$ of $\pi_1(\Sigma_g^b)$. For $i = 1, ..., g$ we set $S = \{a_i, b_i, \delta_2\}$ if $b = 0, 1$, and $S = \{a_i, b_i\}$ if $b = 2$. The commutator subgroup $\pi_1'(\Sigma_g^b)$ is generated by all conjugates of $[x, y]$, where $x, y \in S$ [52, Lemma A.1].

Fundamental group of the unit tangent bundle. Let Σ_g^b be a smooth surface of genus g with b boundary components. Consider a simple closed curve $\gamma : [0, 1] \to \Sigma_g^b$. We differentiate $\gamma(t)$. At each point $\gamma(t_0) = p$, where $t_0 \in (0, 1)$, we have a vector $\gamma'(t_0)$. This vector lies in a *tangent plane* $T_p\Sigma_g^b$. For a formal definition about tangent spaces see for example Isham's book [32, Section 2.3.2]. The *tangent bundle* $T\Sigma_g^b$ is defined as

$$T\Sigma_g^b = \bigcup_{p \in \Sigma_g^b} T_p\Sigma_g^b.$$

We denote by $\|\gamma'(t_0)\|$ the norm of $\gamma'(t_0)$. The *unit tangent bundle* $U\Sigma_g^b$ is defined by

$$U\Sigma_g^b = \{u \in T\Sigma_g^b \mid u = \frac{\gamma'(t_0)}{\|\gamma'(t_0)\|}\}.$$

Every point of $U\Sigma_g^b$ is described by a pair (p, u), where $p \in \Sigma_g^b$, and $u \in T_p\Sigma_g^b$ is a unit vector based on p. There is a fibration $U\Sigma_g^b \to \Sigma_g^b$ with fiber $\mathbb{S}^1$. For $b \geq 1$ we compute the fundamental group of $U\Sigma_g^b$ as follows [29, Proposition 1.12]:

$$\pi_1(U\Sigma_g^b) = \pi_1(\Sigma_g^b \times \mathbb{S}^1) = \pi_1(\Sigma_g^b) \times \pi_1(\mathbb{S}^1) = \pi_1(\Sigma_g^b) \times \mathbb{Z}.$$

2.3 Homology groups

For $b \leq 2$, we have $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z}) = \pi_1(\Sigma_g^b)/\pi_1'(\Sigma_g^b)$, where $\pi_1'(\Sigma_g^b)$ stands for the commutator subgroup of $\pi_1(\Sigma_g^b)$. If $b = 0, 1$, consider the curves x_i, y_i depicted in Figure 2.5 on the left. These curves represent the standard generators of $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ [20, Subsection 6.1.2].

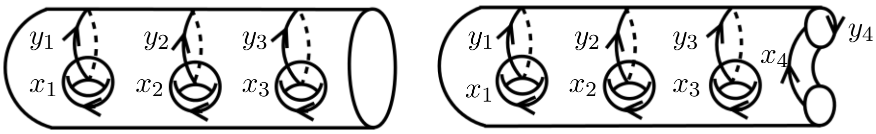


Figure 2.5: Standard generators for $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$, and $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$.

Partitioned homology groups. We denote by q_1, q_2 the boundary components of Σ_g^2. Let p_1, p_2 be two points lying in q_1, q_2 respectively. We set $P = \{q_1, q_2\}$ and $Q = \{p_1, p_2\}$. We also denote by $[h]$ the homology class of h. Consider the relative homology group $\mathrm{H}_1(\Sigma_g^2, Q, \mathbb{Z})$ and the quotient $\mathrm{H}_1(\Sigma_g^2, Q, \mathbb{Z})/\langle [q_1] + [q_2] \rangle$. We define $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ to be $\mathrm{H}_1(\Sigma_g^2, Q, \mathbb{Z})/\langle [q_1] + [q_2] \rangle$. The group $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ contains elements of the form $[h]$, such that h is either a simple closed curve, or h is a simple arc with endpoints at p_1, p_2.

Consider the inclusion $\phi : \Sigma_g^2 \hookrightarrow \Sigma_{g+1}$ induced by gluing the boundary components q_1, q_2. Under this inclusion arcs in Σ_g^2 are mapped to simple closed curves in Σ_{g+1}. The inclusion ϕ induces an inclusion $\phi_* : \mathrm{H}_1^P(\Sigma_g, \mathbb{Z}) \hookrightarrow \mathrm{H}_1(\Sigma_{g+1}, \mathbb{Z})$. Thus, we can think of $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ as a subgroup of $\mathrm{H}_1(\Sigma_{g+1}, \mathbb{Z})$. For $i \leq g$, consider the curves x_i, y_i indicated on the right of Figure 2.5. The homology classes of these curves generate a subgroup of $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$, denoted by V, which is isomorphic to $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$. The arc x_{g+1} generates the cyclic infinite group $\mathbb{Z}$. Thus, we have:

$$\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z}) = V \oplus \mathbb{Z} < \mathrm{H}_1(\Sigma_{g+1}, \mathbb{Z}).$$

See for example [12, Section 2.1] for similar description of $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$.

2.4 Symplectic and homology groups

Here we define the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ and then we consider it as a subgroup of the automorphism group of $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ when $b = 0, 1$, and of $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ when $b = 2$.

Definition of the symplectic group. Let V be a module of finite rank over $\mathbb{Z}$ and consider a bilinear pairing $\hat{\imath} : V \wedge V \to \mathbb{Z}$ satisfying $\hat{\imath}(u, u) = 0$ for $u \in V$. The *radical* of V is the set $\mathrm{rad}(V)$ of all $u \in V$ such that $\hat{\imath}(u, v) = 0$ for all $v \in V$. A pairing $\hat{\imath}$ on V is called *primitive* if for every linear functional $f : V \to \mathbb{Z}$, satisfying $f(\mathrm{rad}(V)) = 0$, there is an $u \in V$ such that $f(v) = \hat{\imath}(u, v)$ for all $v \in V$. A primitive pairing $\hat{\imath}$ on V is called a *symplectic pairing*, or a *symplectic form* if $\mathrm{rad}(V) = 0$. A $\mathbb{Z}$-module endowed with a symplectic pairing is called a *symplectic module*. Every symplectic module admits a basis $y_1, x_1, ..., y_g, x_g$ such that $\hat{i}(x_i, x_j) = \hat{i}(y_i, y_j) = 0$, $\hat{i}(y_i, x_j) = \delta_{i,j}$, where $\delta_{i,j}$ stands for the Kronecker delta.

The automorphism group of a $\mathbb{Z}$-module V of rank n is $\mathrm{Aut}(V)$ and is equal to $\mathrm{GL}_n(\mathbb{Z})$. Assume that V is symplectic with rank $2g$. The *symplectic group* $\mathrm{Sp}_{2g}(\mathbb{Z})$ consists of automorphisms of V that preserve the symplectic pairing $\hat{i}$.

Alternatively, let J be the $2g \times 2g$ matrix

$$\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix},$$

where I_g stands for the $g \times g$ identity matrix. For every square matrix A, we denote by A^T its transpose. The symplectic group is defined to be

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \{A \in \mathrm{GL}(2g, \mathbb{Z}) \mid A^T J A = J\}.$$

Generators for $\mathrm{Sp}_{2g}(\mathbb{Z})$**.** Consider a symplectic basis $\{y_i, x_i\}$ for $i \leq g$. The group $\mathrm{Sp}_{2g}(\mathbb{Z})$ is generated by the following automorphisms [20, Theorem 6.1]:

Transvection: $(y_1, x_1, y_2, x_2, ..., y_g, x_g) \mapsto (y_1 + x_1, x_1, y_2, x_2, ..., y_g, x_g)$,

Factor rotation: $(y_1, x_1, y_2, x_2, ..., y_g, x_g) \mapsto (x_1, -y_1, y_2, x_2, ..., y_g, x_g)$,

Factor mix: $(y_1, x_1, y_2, x_2, ..., y_g, x_g) \mapsto (y_1 - x_2, x_1, y_2 - x_1, x_2, ..., y_g, x_g)$,

Factor swap: $(..., y_i, x_i, y_{i+1}, x_{i+1}, ...) \mapsto (..., y_{i+1}, x_{i+1}, y_i, x_i, ...)$.

Automorphisms of the homology group of a surface. Assume first that $b = 0, 1$. We have that $\mathrm{H}_1(\Sigma_g) = \mathrm{H}_1(\Sigma_g^1, \mathbb{Z}) = \mathbb{Z}^{2g}$ with generators y_i, x_i as indicated in Figure 2.5 on the left. The algebraic intersection number $\hat{i}$ described in Section 1.1 satisfies all the conditions of a symplectic pairing. Thus, $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$ is a symplectic module. Therefore, the automorphisms of $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$ that preserve $\hat{i}$, form the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$. The same is true for $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$.

The homology group $\mathrm{H}_1(\Sigma_g^2, \mathbb{Z})$ is isomorphic to $\mathbb{Z}^{2g+1}$. We have $2g$ generators represented by a choice of curves such as $\{y_i, x_i\}$, $i \geq g$ indicated in Figure 2.5, plus one generator represented by one boundary component. The automorphisms of $\mathrm{H}_1(\Sigma_g^2, \mathbb{Z})$

preserving the algebraic intersection number of curves, form a subgroup of $\mathrm{GL}_{2g+1}(\mathbb{Z})$, denoted by $\mathcal{A}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$. Obviously, $\mathcal{A}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$ is not isomorphic to a symplectic group, since the rank of $\mathcal{A}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$ is not even. Furthermore, $\mathcal{A}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$ does not have a symplectic structure, that is, there is not a symplectic group containing $\mathcal{A}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$. To see this, consider the submodule V of $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z})$ with basis $\{y_i, x_i\}$, where $i = 1, ..., g$. Then $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z})$ splits as the direct sum $V \oplus \mathbb{Z}$, where the cyclic group $\mathbb{Z}$ is generated by the homology class of one of the boundary components, namely q_1. We will explain that the group generated by the homology class of q_1 is the non symplectic part of $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z})$. We can embed Σ_g^2 into a surface Σ_{g+1}^1 as indicated in Figure 2.6 for $g = 4$. The group $\mathrm{H}_1(\Sigma_{g+1}^1,\mathbb{Z})$ is a symplectic module, but the embedding $\Sigma_g^2 \to \Sigma_{g+1}^1$

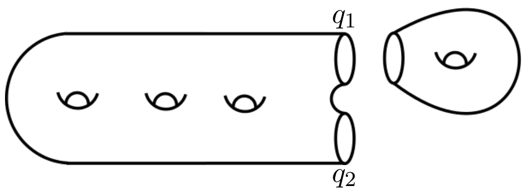


Figure 2.6: An embedding of Σ_3^2 into Σ_4^1.

does not imply an injection $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}) \to \mathrm{H}_1(\Sigma_{g+1}^1,\mathbb{Z})$, since $[q_1] \neq 0$ in $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z})$, but $[q_1] = 0$ in $\mathrm{H}_1(\Sigma_{g+1}^1,\mathbb{Z})$. If we embed Σ_g^2 into Σ_{g+1}^1 by gluing a pair of pants on the two boundary components of Σ_g^2, then we would have $[q_2] = 0$ in $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z})$, but $[q_2] \neq 0$ in $\mathrm{H}_1(\Sigma_{g+1}^1,\mathbb{Z})$. In the general case, if we could find an embedding of Σ_g^2 into Σ, such that the map $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}) \to \mathrm{H}_1(\Sigma,\mathbb{Z})$ was injective, and $\mathrm{H}_1(\Sigma,\mathbb{Z})$ was a symplectic module, then by the isomorphism class of symplectic modules this would imply an injection $\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}) \to \mathrm{H}_1(\Sigma_{g+1}^1,\mathbb{Z})$ of the previous examples.

On the other hand, the group $\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}) = \mathbb{Z}^{2g+1}$ is generated by the simple closed curves y_i, x_i for $i \leq g$ plus a simple arc x_{g+1} as indicated on the right hand of Figure 2.5. We denote by $\mathcal{A}(\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}))$ the subgroup of $\mathrm{Aut}(\mathrm{H}_1(\Sigma_g^2,\mathbb{Z}))$ consisting of automorphisms that preserve the algebraic intersection number $\hat{i}$. Recall from the previous section the inclusion $\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}) \hookrightarrow \mathrm{H}_1(\Sigma_{g+1},\mathbb{Z})$, induced by gluing the boundaries of Σ_g^2. The latter inclusion implies an inclusion $\mathcal{A}(\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z})) < \mathrm{Sp}_{2g+2}(\mathbb{Z})$. The group $\mathcal{A}(\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}))$ acts on $\mathrm{H}_1(\Sigma_{g+1},\mathbb{Z})$, stabilizing the generator y_{g+1}. Hence, $\mathcal{A}(\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}))$ is the subgroup of $\mathrm{Sp}_{2g+2}(\mathbb{Z},\mathbb{Z})$, stabilizing one vector in $\mathrm{H}_1(\Sigma_{g+1},\mathbb{Z})$. From now on we denote $\mathcal{A}(\mathrm{H}_1^P(\Sigma_g^2,\mathbb{Z}))$ by $(\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$ as the subgroup stabilizing y_{g+1}.

Chapter 3

Torelli group

In this chapter we introduce the mapping class group and the Torelli group. The aim of this chapter is to describe a set of generators for Torelli groups.

3.1 Mapping class group

In this section we define the mapping class group $\mathrm{Mod}(\Sigma_{g,n}^b)$. We also give generators for $\mathrm{Mod}(\Sigma_g^b)$, namely Dehn twists. Finally we explain how inclusions between different surfaces induce homomorphisms between mapping class groups. The structure of this section mainly follows Chapters 2 and 3 of Farb-Margalit's book [20].

3.1.1 Definition and examples

Let $\Sigma_{g,n}^b$ be a surface of genus g with n marked points and $b \leq 2$ boundary components. We denote by $\mathcal{B}$ the boundary components of $\Sigma_{g,n}^b$. Let $\mathrm{Homeo}^+(\Sigma_{g,n}^b, \mathcal{B})$ be the group of orientation-preserving homeomorphisms of $\Sigma_{g,n}^b$ that restrict to the identity on $\mathcal{B}$. We endow $\mathrm{Homeo}^+(\Sigma_{g,n}^b, \mathcal{B})$ with the compact open topology. The *mapping class group* of $\Sigma_{g,n}^b$, denoted by $\mathrm{Mod}(\Sigma_{g,n}^b)$, is defined to be

$$\mathrm{Mod}(\Sigma_{g,n}^b) = \pi_0(\mathrm{Homeo}^+(\Sigma_{g,n}^b, \mathcal{B})).$$

Equivalently, $\mathrm{Mod}(\Sigma_{g,n}^b)$ consists of isotopy classes of elements of $\mathrm{Homeo}^+(\Sigma_{g,n}^b, \mathcal{B})$, where isotopies are required to fix the boundary pointwise. Elements of $\mathrm{Mod}(\Sigma_{g,n}^b)$ are called *mapping classes*. Homeomorphisms that act on $\Sigma_{g,n}^b$ are not mapping classes, but they represent mapping classes. In the rest of the thesis we denote a mapping class by a homeomorphism that represents this particular mapping class.

Note: If $\Sigma_{g,n}^b$ is different from an annulus or a disc, we can substitute homotopies instead of isotopies [20, Theorem 1.12]. Furthermore, consider the group $\mathrm{Diff}^+(\Sigma_{g,n}^b, \mathcal{B})$

of diffeomorphisms that preserve the orientation of $\Sigma_{g,n}^b$ and restrict to the identity on $\mathcal{B}$. In the definition of $\mathrm{Mod}(\Sigma_{g,n}^b)$ we can use $\mathrm{Diff}^+(\Sigma_{g,n}^b, \mathcal{B})$ instead of $\mathrm{Homeo}^+(\Sigma_{g,n}^b, \mathcal{B})$ [20, Theorem 1.13].

As an example of a nontrivial element of $\mathrm{Mod}(\Sigma_{g,n}^b)$, one can consider a rotation of the surface Σ_g as indicated in Figure 3.1 for $g = 3$. This is a homeomorphism of order g. For every essential simple closed curve a in Σ_g we have the pairwise nonisotopic simple closed curves $a, h(a), h^2(a), ..., h^{g-1}(a)$. In the next section we give more examples of elements of $\mathrm{Mod}(\Sigma_{g,n}^b)$.

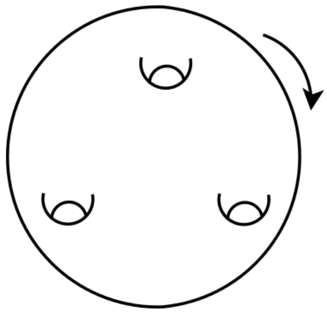


Figure 3.1: Nontrivial element of $\mathrm{Mod}(\Sigma_3)$ of order 3.

Examples of mapping class groups. Here we describe the mapping class group of the disc $D = \Sigma_0^1$, the sphere $\mathbb{S}^2$, the once-punctured sphere $\Sigma_{0,1}$, and the torus Σ_1. Later we see more examples of $\mathrm{Mod}(\Sigma_g^b)$. The lemma below is known as the *Alexander trick* [20, Lemma 2.1].

Lemma 3.1. *The group* $\mathrm{Mod}(D)$ *is trivial.*

Proof. We define $D = \{z \in \mathbb{C} \mid |z| \leq 1\}$. Consider a homeomorphism $\phi : D \to D$ with $\phi|_{\partial D}$ equal to the identity. We define

$$F(z,t) = \begin{cases} (1-t)\phi(\frac{z}{1-t}), & \text{if } 0 \leq |z| < 1-t, \\ z, & \text{if } 1-t \leq |z| \leq 1. \end{cases}$$

for $0 \leq t < 1$ and we also define $F(z, 1)$ to be the identity map of D. Then, F is an isotopy from ϕ to the identity. $\square$

In order to compute $\mathrm{Mod}(\Sigma_{0,1})$, we identify $\Sigma_{0,1}$ with the plane $\mathbb{C}$. Consider a homeomorphism $\phi : \mathbb{C} \to \mathbb{C}$. Then ϕ is isotopic to the identity via $F(z,t) = (1-t)z + t\phi(z)$.

Hence, $\mathrm{Mod}(\Sigma_{0,1})$ is also trivial. For $\mathrm{Mod}(\mathbb{S}^2)$, every homeomorphism in $\mathbb{S}^2$ can be modified by an isotopy so that it fixes a point in $\mathbb{S}^2$. Since the group $\mathrm{Mod}(\Sigma_{0,1})$ is trivial, then $\mathrm{Mod}(\mathbb{S}^2)$ is trivial.

An example of a nontrivial mapping class group is $\mathrm{Mod}(\Sigma_1)$. Every homeomorphism that acts on Σ_1, it also acts on $\mathrm{H}_1(\Sigma_1, \mathbb{Z})$. This action induces a homomorphism

$$\mathrm{Mod}(\Sigma_1) \to \mathrm{Aut}(\mathrm{H}_1(\Sigma_1, \mathbb{Z})) \cong \mathrm{SL}_2(\mathbb{Z}).$$

In fact, this homomorphism is actually an isomorphism, hence, $\mathrm{Mod}(\Sigma_1)$ is not trivial [20, Theorem 2.5].

3.1.2 Dehn twists

In this section we describe a particular type of elements of $\mathrm{Mod}(\Sigma_{g,n}^b)$, namely Dehn twists, which were first introduced by Max Dehn [17]. Dehn twists turn out to be the generators of the mapping class group. Hence, we show some of their properties, and we then provide a finite generating set of $\mathrm{Mod}(\Sigma_g)$.

Twist map in annulus. Consider the annulus $A = \mathbb{S}^1 \times [0, 1]$. Let $T : A \to A$ be the *twist map* defined by

$$T(\theta, t) = (\theta + 2\pi t, t).$$

To understand the action of T on A, we apply T on an arc in A. Consider the arc depicted on the left hand side of the Figure 3.2. On the right hand side of the same figure we indicate the resulting arc after applying the action of T on A.

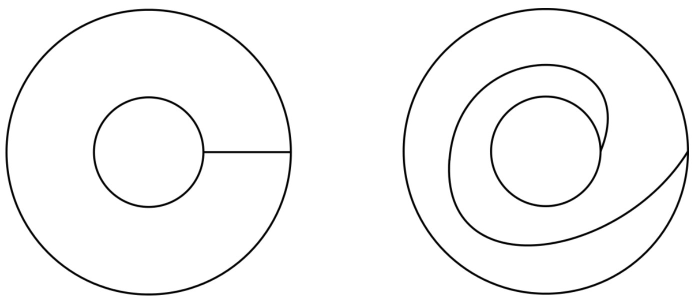


Figure 3.2: Action of a twist on an arc in A.

It is easy to see that T fixes the boundary of A pointwise. Moreover, we could have used $\theta - 2\pi t$ instead of $\theta + 2\pi t$. Our choice is referred to as a ‘left twist’, while the other is a 'right twist'.

Dehn twist in a general surface. Consider a surface $\Sigma = \Sigma_{g,n}^b$ and let a be an essential simple closed curve in Σ. Let N be a regular neighborhood of a and choose an orientation preserving homeomorphism $\phi : A \to N$. We obtain a homeomorphism $T_a : \Sigma \to \Sigma$ defined by

$$T_a(x) = \begin{cases} \phi \circ T \circ \phi^{-1}(x), & \text{if } x \in N, \\ x, & \text{if } x \notin N, \end{cases}$$

for every $x \in \Sigma$. The homeomorphism T_a is called the *Dehn twist* about a. The Dehn twist T_a is a well defined mapping class, since all regular neighborhoods of a are homeomorphic. Furthermore, two isotopic simple closed curves define the same Dehn twist.

We can understand T_a by examining its action on isotopy classes of simple closed curves in Σ. If b is another simple closed curve nonisotopic to a and such that $i(a, b) = 0$, then $T_a(b) = b$. Otherwise, if $i(a, b) \neq 0$, then the isotopy class of $T_a(b)$ is determined by the following rule: each segment of b crossing a is replaced with a segment that informally speaking 'turns left, follows a all the way around, and then turns right'. We indicate two examples of Dehn twists in Figure 3.3.

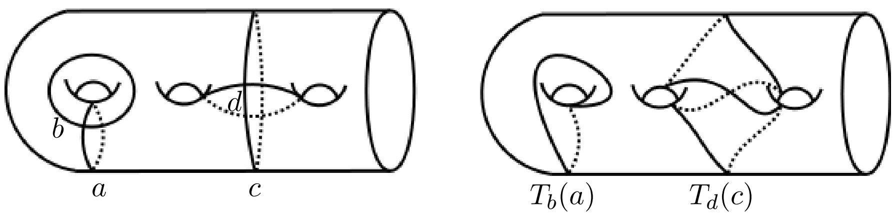


Figure 3.3: Examples of Dehn twists.

Properties of Dehn twists. Below we give some important properties of Dehn twists which are required for the further discussion in the following chapters.

Let a and b be two isotopy classes of simple closed curves in Σ; let k be an integer. A direct calculation shows that

$$i(T_a^k(b), b) = |k| i(a, b)^2.$$

For more details see Paris-Rolfsen [49, Proposition 3.3]. As a consequence we have that

Dehn twists have infinite order in $\mathrm{Mod}(\Sigma)$.

For $f \in \mathrm{Mod}(\Sigma)$, for any isotopy class of simple closed curve a, and $k \in \mathbb{Z}$ we have

$$T^k_{f(a)} = f T^k_a f^{-1}.$$

If $k = 1$, the formula above is described as follows: the homeomorphism f^{-1} takes a regular neighborhood of $f(a)$ to a. Then T_a twists the neighborhood of a and f takes the twisted neighborhood of a back to neighborhood of $f(a)$. So the result is a Dehn twist about $f(a)$. The same argument holds for $k > 1$. As a consequence, we have that for a fixed k, the homeomorphisms T^k_a are conjugate.

Let a, b be two isotopy classes of simple closed curves. We have $i(a, b) = 1$ if and only if

$$T_a T_b T_a = T_b T_a T_b.$$

The relation above is called the *braid relation* [20, Propositions 3.11 & 3.13]. Finally, if $i(a, b) \geq 2$, then relations between T_a and T_b do not exist [20, Theorem 3.14].

Finite set of generators. Dehn twists are generators of $\mathrm{Mod}(\Sigma^b_g)$. Lickorish proved that $\mathrm{Mod}(\Sigma_g)$ is generated by Dehn twists about the curves indicated in Figure 3.4 [42]. Later, Humphries improved Lickorish's result by proving that $\mathrm{Mod}(\Sigma_g)$ is generated by Dehn twists about the curves c_i, b_1 with $0 \leq i \leq 2g$ as showing in Figure 3.4 [31].

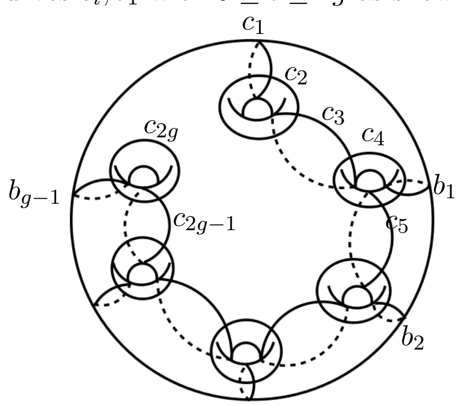


Figure 3.4: The Lickorish generators for $\mathrm{Mod}(\Sigma_g)$.

3.1.3 Birman exact sequence

Here we explain how inclusions on surfaces induce homomorphism on mapping class groups. This method allows us to give proofs by inductions on mapping class groups. As a result we find one of the most important short exact sequences in the study of mapping class groups, namely the Birman exact sequence.

Inclusion homomorphisms. Consider a surface Σ. Let Σ' be a subsurface of Σ. We have an inclusion $j : \Sigma' \to \Sigma$. We describe how the map j induces a homomorphism $j_* : \mathrm{Mod}(\Sigma') \to \mathrm{Mod}(\Sigma)$. An element of $\mathrm{Mod}(\Sigma')$ is represented by a homeomorphism $f : \Sigma' \to \Sigma'$. We extend f as the identity in $S = \Sigma \setminus \Sigma'$ and we call the new homeomorphism f'. Obviously, $f' : \Sigma \to \Sigma$. We define $j_*(f) = f'$. Let f'' be a homeomorphism isotopic to f'. Then there is a homotopy H_t that, when restricted to S, connects $f''|_S$ to the identity. Composing H_t by a homotopy connecting f with $f''|_{\Sigma'}$, we deduce that $j_* : \mathrm{Mod}(\Sigma') \to \mathrm{Mod}(\Sigma)$ is a well defined map. In fact j_* is a homomorphism. If S is not homeomorphic to an annulus, open disc, or an open punctured disc, then j_* is injective [20, Theorem 3.18] (see also [49, Theorem 4.1, Corollary 4.2]).

Capping the boundary of Σ_g^1. Consider the inclusion $j : \Sigma_g^1 \to \Sigma_g$ defined by gluing a disc D to the boundary of Σ_g. It is easy to see that the induced homomorphism $j_* : \mathrm{Mod}(\Sigma_g^1) \to \mathrm{Mod}(\Sigma_g)$ is surjective. Particularly, every $f \in \mathrm{Mod}(\Sigma_g)$ can be isotoped such that the result acts as the identity on D. We have an exact sequence:

$$1 \to K \to \mathrm{Mod}(\Sigma_g^1) \to \mathrm{Mod}(\Sigma_g) \to 1.$$

Our aim in the subsection is to characterize the kernel K. Consider an element $f \in K$ and let F_t be an isotopy with $F_0 = f$ and F_1 be the identity in Σ_g. We fix a point $d \in D$ and a unit vector $u \in T_d\Sigma_g$ (the tangent space at d). For each $t \in [0, 1]$ we get a point $F_t(d)$, and a vector $F_t(u)$. The induced path is a loop in $U\Sigma_g$ (unit tangent bundle of Σ_g) at (d, u). We denote this loop by $\phi(f)$. We end up with a map $\phi : K \to \pi_1(U\Sigma_g, (d, u))$. To show that ϕ is well defined, consider two isotopies F_t, F_t' with $F_0 = F_0' = f$ and $F_1 = F_1'$ as the identity in Σ_g. For every $t \in [0, 1]$, the isotopies F_t, F_t' define two paths in $\mathrm{Diff}^+(\Sigma_g)$. But since $\mathrm{Diff}^+(\Sigma_g)$ is contractible [28, Theorem 2], there is a homotopy from F_t to F_t'. Thus, $\phi(f)$ is well defined up to homotopy. The map $\phi : K \to \pi_1(U\Sigma_g, (d, u))$ is a homomorphism, and more particularly an isomorphism [35, Lemmas 2 and 3] (see also [7] for similar inclusions of surfaces with more than one boundary components).

The sequence

$$1 \to \pi_1(U\Sigma_g, (d,u)) \to \mathrm{Mod}(\Sigma_g^1) \to \mathrm{Mod}(\Sigma_g) \to 1$$

is well known in the literature as the *Birman exact sequence*. The injective homomorphism $\pi_1(U\Sigma_g, (d,u)) \to \mathrm{Mod}(\Sigma_g^1)$ is known as the *disc-pushing* map.

Describing the disc-pushing map. Consider a curve $\tilde{\gamma}$ in $\pi_1(U\Sigma_g, (d,u))$. Since every point of $\tilde{\gamma}$ lies in a tangent space of Σ_g, we can represent $\tilde{\gamma}$ by a smooth curve $\gamma : [0,1] \to \Sigma_g$ with $\gamma(0) = \gamma(1) = d$. Let N be a regular neighborhood of γ and denote by a, b the boundary of N. For each $t \in [0,1]$, the map $\gamma(t)$ traces a path in Σ_g bounded by a and b. We can understand this trace by considering an arc crossing N. The disc containing the point d moves around in the path of γ, pushing the arc as in Figure 3.5. The result is the product of Dehn twists $T_b T_a^{-1} \in \mathrm{Mod}(\Sigma_g^1)$. Therefore, the disc-pushing map $\pi_1(U\Sigma_g, (d,u)) \to \mathrm{Mod}(\Sigma_g^1)$ is defined by

$$\tilde{\gamma} \mapsto T_b T_a^{-1}.$$

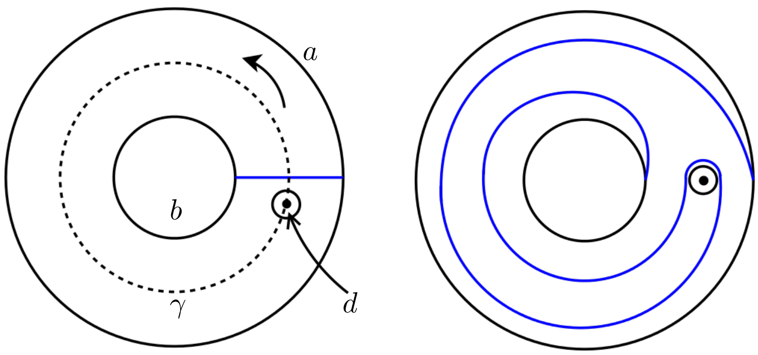


Figure 3.5: Action of the disc-pushing map.

3.2 Torelli group

In this section we define the Torelli group $\mathcal{I}(\Sigma_g^b)$, where $g \geq 2$ and $n \leq 2$. We can think of $\mathcal{I}(\Sigma_g^b)$ as the subgroup of the mapping class group $\mathrm{Mod}(\Sigma_g^b)$ that acts on the homology of the surface as the identity. We distinguish between two cases. In the first case we define the Torelli group for surfaces with at most one boundary component; in the second case we define $\mathcal{I}(\Sigma_g^2)$.

3.2.1 Symplectic representation

Consider a closed surface Σ_g and let $\mathrm{Mod}(\Sigma_g)$ be its mapping class group. Every mapping class is represented by homeomorphisms that act on curves of Σ_g. However, every oriented curve represents a homology class in $\mathrm{H}_1(\Sigma_g, \mathbb{Z}) = \mathbb{Z}^{2g}$. Therefore, every $f \in \mathrm{Mod}(\Sigma_g)$ induces an automorphism $f_* : \mathrm{H}_1(\Sigma_g, \mathbb{Z}) \to \mathrm{H}_1(\Sigma_g, \mathbb{Z})$. We recall that $\mathrm{Aut}(\mathbb{Z}^{2g}) = \mathrm{GL}_{2g}(\mathbb{Z})$. We have a linear representation

$$\mathrm{Mod}(\Sigma_g) \to \mathrm{GL}_{2g}(\mathbb{Z}).$$

Since $\mathrm{Mod}(\Sigma_g)$ preserves the algebraic intersection number $\hat{i} : \mathrm{H}_1(\Sigma_g, \mathbb{Z}) \times \mathrm{H}_1(\Sigma_g, \mathbb{Z}) \to \mathbb{Z}$, it follows that the image of the linear representation above lies inside $\mathrm{Sp}_{2g}(\mathbb{Z})$. Thus, we get a linear representation

$$\rho : \mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}_{2g}(\mathbb{Z}),$$

which we call *symplectic representation*. Our aim in this subsection is to compute the image of ρ and describe its kernel.

Consider two curves $a, b \in \Sigma_g$ and their homology classes $[a], [b] \in \mathrm{H}_1(\Sigma_g, \mathbb{Z})$ respectively. The image of $T_b(a)$ under the map ρ is defined as $\rho(T_b(a)) = [a] + \hat{i}(a, b)[b]$ [20, Proposition 6.3]. Hence, the image of a Dehn twist in $\mathrm{Sp}_{2g}(\mathbb{Z})$ is a transvection as defined in Section 2.4. A transvection associated to a Dehn twist T_b is denoted by $T_{[b]}$, where $[b]$ stands for the homology class of b.

Theorem 3.2. *The symplectic representation is surjective.*

Proof. Consider the symplectic basis $\{y_i, x_i\}$ as indicated on the right hand side of the Figure 3.6. To prove that the homomorphism ρ is surjective, we only need to find mapping classes that map into generators of $\mathrm{Sp}_{2g}(\mathbb{Z})$. Recall the generators described in Section 2.4, transvection, factor rotation, factor swap, and factor mix. We have seen that every Dehn twist is mapped to a transvection. It is convenient to describe the homeomorphisms in terms of Dehn twists in what follows.

Consider the curves c_1, c_2 in Figure 3.4, and let y_1, x_1 denote their homology classes, respectively. Then we have $\rho(T_{c_1}T_{c_2}T_{c_1}(c_1)) = x_1$, and $\rho(T_{c_1}T_{c_2}T_{c_1}(c_2)) = -y_1$. Consequently, $\rho(T_{c_1}T_{c_2}T_{c_1})$ acts as the factor rotation on $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$.

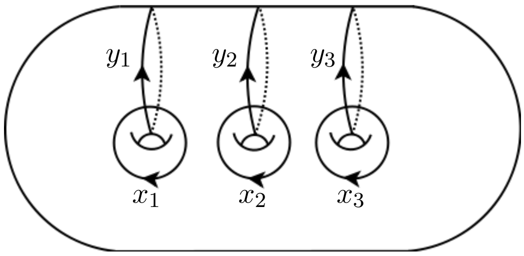


Figure 3.6: Standard generators for $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$.

Consider the curve c depicted on the right hand side of the Figure 3.7, and let $[c] = y_2 - y_1$ be its homology class. Consider also the curves c_1, c_2, c_4, b_1 in Figure 3.4, and let y_1, x_1, x_2, y_2 be their homology classes, respectively. We define the homeomorphism $h = T_{c_1}^{-1} T_{b_1}^{-1} T_c$. We have $\rho(h(c_1)) = y_1 - x_2$, $\rho(h(c_2)) = x_1$, $\rho(h(b_1)) = y_2 - x_1$, $\rho(h(c_4)) = x_2$. Consequently, $\rho(h)$ acts as the factor mix on $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$.

Finally, in a genus g surface we have $g - 1$ factor swaps. We prove the existence of a swap homeomorphism in the first two genus holes as depicted in Figure 3.7. The other cases are similar. Consider the curve d with homologous class $[d] = [y_1] + [x_2]$ as indicated on the right hand side of the Figure 3.7.

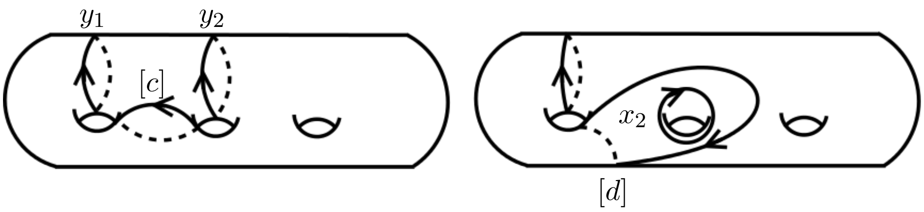


Figure 3.7: The curves c, d.

We define the homeomorphism $f = (T_{c_4} T_{b_1} T_d T_{c_2} T_{c_1})^3$. A direct calculation shows that $\rho(f)$ acts as the factor swap. □

Recall that $\mathrm{Mod}(\Sigma_g)$ is generated by $2g + 1$ Dehn twists. From Theorem 3.2 we deduce that $\mathrm{Sp}_{2g}(\mathbb{Z})$ is generated by $2g + 1$ transvections.

The inclusion $\Sigma_g^1 \subset \Sigma_g$ induces an isomorphism between $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ and $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$. Furthermore, we have a surjective homomorphism $\mathrm{Mod}(\Sigma_g^1) \to \mathrm{Mod}(\Sigma_g)$ as described in Section 3.1.3. Therefore, we get a surjective representation

$$\mathrm{Mod}(\Sigma_g^1) \to \mathrm{Sp}_{2g}(\mathbb{Z}).$$

The kernel of the symplectic representation. Consider a surface Σ_g^b with $b \leq 1$ and $g \geq 1$. If $g = 1$ and $b = 0$, then $\mathrm{Mod}(\Sigma_1) = \mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{Sp}_2(\mathbb{Z})$ as we have seen in Section 3.1.1. So in this case the symplectic representation is faithful. Unfortunately this is not the case when $g \geq 2$. Hence, we have a short exact sequence

$$1 \to \mathcal{I}(\Sigma_g^b) \to \mathrm{Mod}(\Sigma_g^b) \to \mathrm{Sp}_{2g}(\mathbb{Z}) \to 1,$$

where $b \leq 1$, and $g \geq 2$.

Definition 3.1 The group $\mathcal{I}(\Sigma_g^b)$ is called the *Torelli group* and it contains mapping classes that act trivially on $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$.

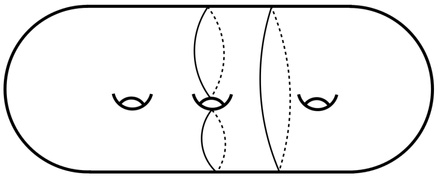


Figure 3.8: Bounding pair curves, and a separating curve.

We describe two important kinds of elements of $\mathcal{I}(\Sigma_g^b)$. Consider the curve d depicted in Figure 3.8. The curve d is a separating curve, which is represented by a commutator in $\pi_1(\Sigma_g^b)$, hence, $[d] = 0$ in $\mathrm{H}_1(\Sigma_1^b, \mathbb{Z})$. For every $u \in \mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$, we have

$$\rho(T_d)(u) = T_{[d]}(u) = u + \hat{i}(u, [d])[d] = u + \hat{i}(u, 0)0 = u.$$

Thus, for every separating curve $d \in \Sigma_g^b$, we have $T_d \in \mathcal{I}(\Sigma_g^b)$.

Let $a, e \in \Sigma_g^b$ be two curves, such that $[a] = [e] \in \mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$. Such a pair of curves is called *bounding pair* of curves. For example, consider the curves a, e depicted in Figure 3.8. These two curves separate the surface Σ_g^b into two connected components. A homeomorphism of the form $T_a T_e^{-1}$ is called a *bounding pair map*, or a bounding pair for short. For every $u \in \mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$, we have

$$\rho(T_a T_e^{-1})(u) = T_{[a]} T_{[e]}^{-1}(u) = T_{[a]} T_{[a]}^{-1}(u) = u.$$

Hence, we have $T_a T_e^{-1} \in \mathcal{I}(\Sigma_g^b)$. As we see later on in Section 3.3, bounding pair maps and Dehn twists about separating curves generate $\mathcal{I}(\Sigma_g^b)$.

3.2.2 The Torelli group of Σ_g^2

Here we define the Torelli group on a surface of genus $g \geq 2$ with two boundary components. Firstly, we explain why we cannot apply the definition of Section 3.2.1.

We recall that the Torelli group is defined as the kernel of the symplectic representation of the mapping class group. But as we have seen in Section 2.4, $\mathrm{H}_1(\Sigma_g^2, \mathbb{Z})$ is not a symplectic module. We could define the Torelli group of Σ_g^2 by simply considering it as a subgroup of $\mathrm{Mod}(\Sigma_g^2)$, consisting of mapping classes that act trivially on $\mathrm{H}_1(\Sigma_g^2, \mathbb{Z})$. But taking into account the example of Figure 2.6, the Dehn twist T_{q_1} is an element of $\mathcal{I}(\Sigma_{g+1}^1)$, but not an element of $\mathcal{I}(\Sigma_g^2)$.

Defining the Torelli group of Σ_g^2. Consider the partition $P = \{q_1, q_2\}$, where q_1, q_2 are the boundary components of Σ_g^2, and let $\mathrm{H}_1^P(\Sigma_g^2)$ be the homology group with respect to P, as defined in Section 2.3. Consider also a surface Σ_{g+1} obtained from Σ_g^2 by gluing together the boundary components q_1, q_2. We have an inclusion $j : \Sigma_g^2 \to \Sigma_{g+1}$ and a homomorphism $j_* : \mathrm{Mod}(\Sigma_g^2) \to \mathrm{Mod}(\Sigma_{g+1})$.

Definition 3.2 The Torelli group of the surface Σ_g^2 with respect to partition P is $\mathcal{I}(\Sigma_g^2, P) = j_*^{-1}(\mathcal{I}(\Sigma_{g+1}))$. Then $\mathcal{I}(\Sigma_g^2, P)$ is the subgroup of $\mathrm{Mod}(\Sigma_g^2)$ that acts trivially on $\mathrm{H}_1^P(\Sigma_g^2)$.

The definition of $\mathcal{I}(\Sigma_g^2, P)$ is independent of the choice of the embedding described above [52, Theorem 3.3]. In the rest of the thesis we write $\mathcal{I}(\Sigma_g^2)$ instead of $\mathcal{I}(\Sigma_g^2, P)$.

Next we describe elements of $\mathcal{I}(\Sigma_g^2)$. Consider a curve d in Σ_g^2 such that $[d] = 0$ in $\mathrm{H}_1^P(\Sigma_g^2)$. The curve d is a separating curve. However, not all separating curves have zero homology class in $\mathrm{H}_1^P(\Sigma_g^2)$. Then we have $T_d \in \mathcal{I}(\Sigma_g^2)$, where T_d is called a Dehn twist about a P-separating curve. Consider also two curves a, b such that $[a], [b] \in \mathrm{H}_1^P(\Sigma_g^2)$ and $[a] = [b]$. For example, the curves a, b in Figure 3.9 are homologous in $\mathrm{H}_1^P(\Sigma_g^2)$, while the curves c, d are not homologous in $\mathrm{H}_1^P(\Sigma_g^2)$. The homeomorphism $T_a T_b^{-1} \in \mathcal{I}(\Sigma_g^2)$ is called a P-bounding pair map.

We denote by $\mathcal{I}(\Sigma_g, c)$ the stabilizer subgroup of $\mathcal{I}(\Sigma_g)$ fixing a curve $c \in \Sigma_g$. Consider the inclusion $j : \Sigma_g^2 \to \Sigma_{g+1}$ described above. Let q_1, q_2 denote the boundaries of Σ_g^2 and let $q = j(q_1) = j(q_2)$ denote the resulting curve in Σ_{g+1}. We have a short exact

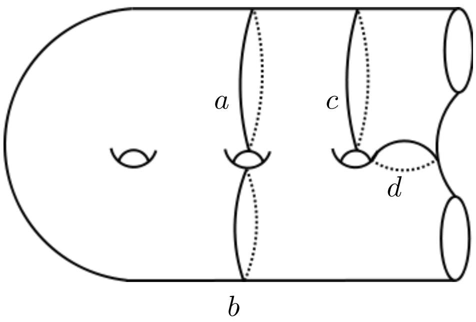


Figure 3.9: Examples of curves in Σ_g^2.

sequence [20, Theorem 3.18]

$$1 \to \langle T_{q_1} T_{q_2}^{-1} \rangle \to \mathrm{Mod}(\Sigma_g^2) \to \mathrm{Mod}(\Sigma_g, q) \to 1$$

where $\mathrm{Mod}(\Sigma_g, c)$ the stabilizer subgroup of $\mathrm{Mod}(\Sigma_g)$ fixing a curve $c \in \Sigma_g$. But since, $T_{q_1} T_{q_2}^{-1} \in \mathcal{I}(\Sigma_g^2)$, we get

$$1 \to \langle T_{q_1} T_{q_2}^{-1} \rangle \to \mathcal{I}(\Sigma_g^2) \to \mathcal{I}(\Sigma_g, q) \to 1.$$

3.2.3 Birman exact sequence for the Torelli group

In Section 3.1.3 we defined the following Birman exact sequence for the mapping class group:

$$1 \to \pi_1(U\Sigma_g, (d, u)) \to \mathrm{Mod}(\Sigma_g^1) \to \mathrm{Mod}(\Sigma_g) \to 1.$$

In this section we define a version of the Birman exact sequence for the Torelli group. More particularly, for $g \geq 2$ and $b \leq 2$ we describe the following sequence:

$$1 \to K \to \mathcal{I}(\Sigma_g^b) \to \mathcal{I}(\Sigma_g^{b-1}) \to 1.$$

It is obvious that the homomorphism $\mathcal{I}(\Sigma_g^b) \to \mathcal{I}(\Sigma_g^{n-1})$ is surjective. Our aim is to characterize the kernel K of the Birman exact sequence, and describe the disc-pushing map $K \to \mathcal{I}(\Sigma_g^b)$.

Case $b = 1$**.** In this case we see that the kernel of the map $\mathcal{I}(\Sigma_g^1) \to \mathcal{I}(\Sigma_g)$ is isomorphic to $\pi_1(U\Sigma_g, (d, u))$.

Recall from Section 2.2 that $\pi_1(U\Sigma_g, (d, u)) = \pi_1(\Sigma_g, d) \times \mathbb{Z}$. In what follows we will write $\pi_1(U\Sigma_g), \pi_1(\Sigma_g)$ instead of $\pi_1(U\Sigma_g, (d, u)), \pi_1(\Sigma_g, d)$ respectively. Recall also from Section 3.1.3 the disc pushing map $\pi_1(U\Sigma_g, (d, u)) \to \mathrm{Mod}(\Sigma_g^1)$, defined by $\tilde{\gamma} \to T_a T_e^{-1}$, where $\tilde{\gamma}$ is a smooth simple closed curve in Σ_g, and a, e denote the boundary curves of the regular neighborhood of $\tilde{\gamma}$ in Σ_g. The curves a, e also bound the boundary of Σ_g^1. Hence, $[a] = [e]$ up to a sign. Therefore, $T_a T_e^{-1} \in \mathcal{I}(\Sigma_g^1)$.

Case $b = 2$. Consider the short exact sequence

$$1 \to K \to \mathcal{I}(\Sigma_g^2) \to \mathcal{I}(\Sigma_g^1) \to 1,$$

obtained by gluing a disc on one of the boundaries. The group K is contained in $\pi_1(U\Sigma_g^1)$ but it is not all of it. In fact $K < \pi_1(\Sigma_g^1)$. Putman proved that K is isomorphic to $[\pi_1(\Sigma_g^1), \pi_1(\Sigma_g^1)]$ [52, Theorem 1.2]. Thus, every commutator in $[\pi_1(\Sigma_g^1), \pi_1(\Sigma_g^1)]$ gives a homeomorphism in $\mathcal{I}(\Sigma_g^2)$. Before we describe the disc-pushing map, we explain why the Birman exact sequence splits.

We denote by q_1, q_2 the boundaries of Σ_g^2. Consider the map $\pi_* : \mathcal{I}(\Sigma_g^2) \to \mathcal{I}(\Sigma_g^1)$, induced by gluing a disc on the boundary q_1 of Σ_g^2. If we glue a pair of pants on the boundary of Σ_g^1, we end up with a surface homeomorphic to Σ_g^2. Hence, we have an inclusion $\rho : \Sigma_g^1 \hookrightarrow \Sigma_g^2$. By extending every homeomorphism of $\mathcal{I}(\Sigma_g^1)$ by the identity on the pair of pants we end up with a homomorphism $\rho_* : \mathcal{I}(\Sigma_g^1) \to \mathcal{I}(\Sigma_g^2)$, such that for $f \in \mathcal{I}(\Sigma_g^2)$, the image $\rho_*(\pi_*(f))$ is the identity in $\mathcal{I}(\Sigma_g^2)$. Therefore, the Birman exact sequence splits and we have $\mathcal{I}(\Sigma_g^2) \cong K \ltimes \mathcal{I}(\Sigma_g^1)$.

Now we want to describe the disc-pushing map $K \to \mathcal{I}(\Sigma_g^2)$. Since K is isomorphic to $[\pi_1(\Sigma_g^1), \pi_1(\Sigma_g^1)]$, we would like to describe how a commutator in K is mapped into an element of $\mathcal{I}(\Sigma_g^1)$ by the disc-pushing map. We choose a base fixed point x_0 for $\pi_1(\Sigma_g^1)$ in the interior of Σ_g^1 away from the boundary, as indicated on the left hand side of the Figure 3.10. Then every commutator is a product of separating simple closed curves [52, Lemma A.1]. Consider a separating curve crossing the fixed point. Then the surface deformation retracts on the surface on the right hand side of the 3.10. Furthermore, the group $\mathcal{I}(\Sigma_g^1)$ acts on $[\pi_1(\Sigma_g^1), \pi_1(\Sigma_g^1)]$, that is, the commutator subgroup of $\pi_1(\Sigma_1)$. After this action the fixed point always ends up in the boundary of the surface Σ_g^1. Taking

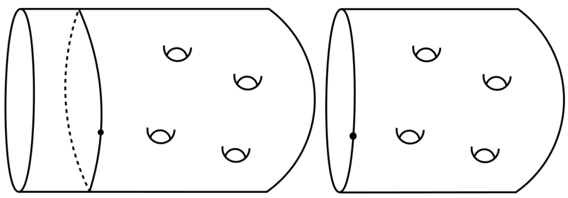


Figure 3.10: Deformation retraction of $\Sigma_{g,1}$.

into consideration the above retraction we can always choose a separating simple closed curve. Let η be that commutator which is a simple closed curve in K. On the right hand side of the Figure 3.11, we show an example of η. Denote the boundaries of $\Sigma_{g,2}$

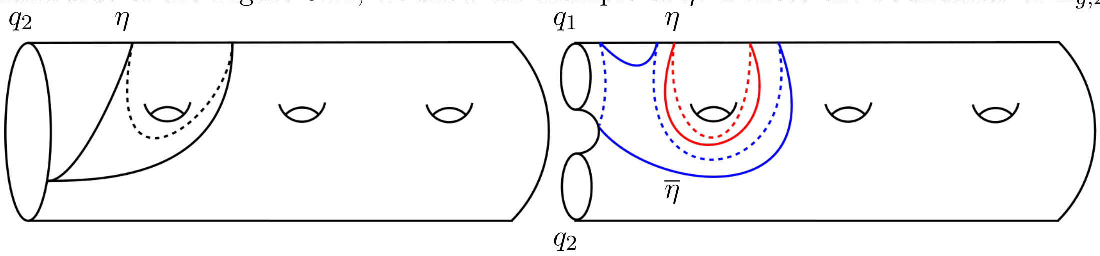


Figure 3.11: Disc-pushing map.

by q_1 and q_2, and the boundary of $\Sigma_{g,1}$ by q_2. Then the disc-pushing map is defined to be

$$\eta \to (T_{q_1} T_{\overline{\eta}}^{-1}) T_\eta$$

for curves η and $\overline{\eta}$ depicted on the right hand side of the Figure 3.11. This map is well defined [52, Section 4.1].

3.3 Generating the Torelli group

This section is devoted to present a generating set for the Torelli group $\mathcal{I}(\Sigma_g^b)$ when $b = 0, 1$. First, we describe a finite generating set of bounding pair maps for $\mathcal{I}(\Sigma_g^b)$ introduced by Johnson [35]. This generating set grows exponentially with respect to g. Johnson also conjectured that there is a finite generating set that grows cubically with respect to g [35, Section 5]. This conjecture was proved by Putman [54, Theorem A], and later it was improved by Putman-Church [14, Theorem H]. Our aim in this section is to describe the generators of Theorem H [14] and give a different proof. Throughout this section we denote by C_i, B_i the generators T_{c_i}, T_{b_i} depicted in Figure 3.4.

3.3.1 Chain maps

We describe a finite set of bounding pair maps, suggested by Johnson [35], who proved that this set generates $\mathcal{I}(\Sigma_g^b)$ when $b = 0, 1$.

An *odd-chain* in Σ_g^b is an ordered collection $(a_1, a_2, ..., a_m)$ of odd number of simple closed curves with the following properties:

1. The curves a_i, a_{i+1} intersect transversely in a single point, such that the algebraic intersection number between a_i, a_{i+1} is $+1$.

2. If $|i-j|>1$, then $a_i \cap a_j = \emptyset$.

The length of an odd-chain is equal to the number of curves that it contains. It is easy to see that the boundary of a regular neighborhood of an odd-chain contains only two curves that represent the same element in $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$. Consider an odd-chain $(a_1, a_2, ..., a_m)$ and let a, a' be the curves of the boundary of a regular neighborhood of $(a_1, a_2, ..., a_m)$. Then the map $T_a T_{a'}^{-1}$ is denoted by $[a_1, a_2, ..., a_m]$, and we call it *chain map.* If $g \in \mathrm{Mod}(\Sigma_{g,n})$, then $g * T_a T_{a'}^{-1} = g T_a T_{a'}^{-1} g^{-1} = T_{g(a)} T_{g(a')}^{-1}$. Likewise, we write $g * [a_1, a_2, ..., a_m]$ for $g[a_1, a_2, ..., a_m]g^{-1} = [g(a_1), g(a_2), ..., g(a_m)]$.

Let a_i, a_{i+1} be two curves of an odd-chain $(a_1, a_2, ..., a_m)$. We define the sum $a_i + a_{i+1} = T_{a_{i+1}}(a_i)$. The sum is well defined since the composition of Dehn twist is a well defined operation. An *odd subchain* of $(a_1, a_2, ..., a_m)$ is a chain of the form $(k_1, k_2, ..., k_l)$ such that l is an odd number with $l < m$, and

$$k_j = a_{i_j} + a_{i_j+1} + ... + a_{i_{j+1}-1}, k_{j+1} = a_{i_{j+1}} + a_{i_{j+1}+1} + ... + a_{i_{j+2}-1}.$$

Consider the curves c_i depicted in Figure 3.4; consider also the odd-chain $(c_1, c_2, ..., c_{2g+1})$. An odd subchain of the form

$$(c_{i_1} + c_{i_1+1} + ... + c_{i_2-1}, c_{i_2} + ... + c_{i_3-1}, ..., c_{i_l-1} + ... + c_{i_l-1})$$

is denoted by $(i_1 i_2 ... i_l)$, and the chain map by $[\![i_1 i_2 ... i_l]\!]$. For example we have that $(c_1 + c_2, c_3, c_4 + c_5) = (1346)$. For a proof of the following lemma see Johnson's paper [35, Lemma 1].

Lemma 3.3. *If $C_j = T_{c_j}$, then C_j commutes with $[\![i_1 i_2 ...]\!]$ if and only if $j, j+1$ are either both contained in or are disjoint from the i-s. If $j = i_m$ but $j+1 \neq i_{m+1}$, then*

$$C_{i_m} * [\![i_1 i_2 ...]\!] = [\![i_1 ... i_{m-1}, i_m + 1, i_{m+1} ...]\!].$$

If $j+1 = i_m$ but $j \neq i_{m-1}$, then

$$C_{i_m-1}^{-1} * [\![i_1 i_2 ...]\!] = [\![i_1 ... i_{m-1}, i_m - 1, i_{m+1}, ...]\!].$$

We set $b_1 + c_4 = \beta$. If $B = T_{b_1}$, then $B * [\![4 i_1 i_2 ...]\!] = [\![\beta i_1 i_2 ...]\!]$. The odd-chains maps of the form $[\![\beta i_1 i_2 ...]\!]$ are called *β-chains* and the odd-chain maps of the form $[i_1 i_2 ...]$ are called *straight-chains.* Johnson proved that all β-chains and all straight-chains generate $\mathcal{I}(\Sigma_g^b)$ where $b \leq 1$ [35]. He also proved that $\mathcal{I}(\Sigma_3)$ and $\mathcal{I}(\Sigma_3^1)$ are generated by 35 and 42 elements respectively (the maximal straight chain maps become trivial in $\mathcal{I}(\Sigma_g)$). More particularly, he proved that $\mathcal{I}(\Sigma_3)$ is generated by all 3-chains, that is $[\![i_1 i_2 i_3 i_4]\!]$, and $\mathcal{I}(\Sigma_3^1)$ is generated by all 3-chains, by $[\![\beta 567]\!]$, and by all 5-chains except $[\![123456]\!]$ [35, Section 5].

3.3.2 Cubic generating set

Now we are ready to describe a set of bounding pair maps, which we later prove that is the set generating $\mathcal{I}(\Sigma_g)$.

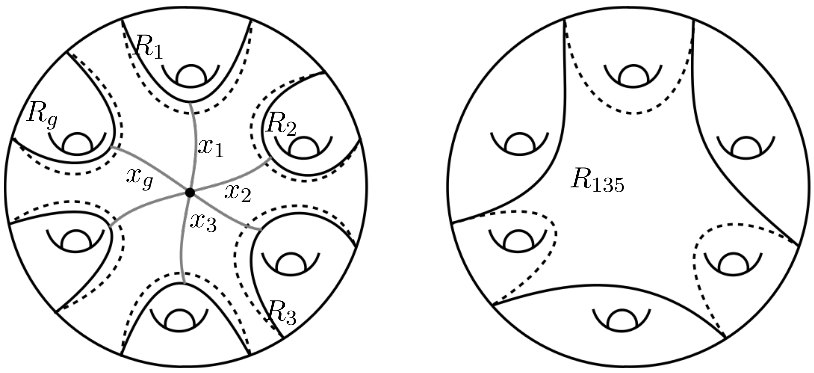


Figure 3.12: An example of R_{ijk} inside Σ_g.

For a surface Σ_g, we denote the g handles by R_i as in Figure 3.12. Consider the arcs x_i as depicted on the left hand side of the Figure 3.12. For each $\{i, j, k\} \subseteq \{1, 2, 3, 4, ..., g\}$, we define the subsurface $R_{i,j,k}$ to be a regular neighborhood of $x_i \cup x_j \cup x_k \cup R_i \cup R_j \cup R_k$. The choice of a regular neighborhood is not unique but all of the choices are isotopic. Furthermore, each R_{ijk} is homeomorphic to Σ_3^1. On the right hand side of the Figure 3.12 we illustrate an example of R_{235}. Note that $R_{ijk} = R_{jki} = R_{kij}$.

Church-Putman proved that every bounding pair map in $\mathcal{I}(\Sigma_g)$ belongs to the group, generated by $\bigcup_{1\le i<j\le k\le g} \mathcal{I}(R_{ijk})$ [14, 54]. In the next section we follow the strategy of Putman [54] to explicitly factor certain elements of $\mathcal{I}(\Sigma_g)$ into elements of $\bigcup_{1\le i<j\le k\le g} \mathcal{I}(R_{ijk})$. More particularly, we show that if $f \in \mathrm{Mod}(\Sigma_g)$ and $h \in \bigcup_{1\le i<j\le k\le g} \mathcal{I}(R_{ijk})$, then $fhf^{-1} \in \bigcup_{1\le i<j\le k\le g} \mathcal{I}(R_{ijk})$. This method leads to a different proof from Church-Putman's proof, since $\mathcal{I}(\Sigma_g)$ is normally generated by bounding pair maps. We note here that the cardinality of the generating set coming from

$\bigcup_{1\le i<j\le k\le g}\mathcal{I}(R_{ijk})$ is equal to $42\binom{g}{3}$.

3.3.3 Factorization algorithm

Consider a surface Σ_g, $g\ge 4$, and let $C_7 = T_{c_7}$ be as in Figure 3.4. In this section we explain how to factorize an element of $C_7^{\pm1} * \mathcal{I}(R_{123})$ into elements of $\bigcup_{1\le i<j<k\le 4}\mathcal{I}(R_{ijk})$, where the latter set is considered as a subset of $\bigcup_{1\le i<j<k\le g}\mathcal{I}(R_{ijk})$. We describe an algorithmic method and we apply it to $C_7^{-1} * [1267]$. By Section 3.3.1 we have that the bounding pair map $[\![1267]\!]$, indicated in Figure 3.13, is a generator of $\mathcal{I}(R_{123})$. The element $C_7^{-1} * [\![1267]\!]$ does not seem to lie on $\bigcup_{1\le i<j<k\le 4}\mathcal{I}(R_{ijk})$, but we show step by step how to factor it into maps lying on $\bigcup_{1\le i<j<k\le 4}\mathcal{I}(R_{ijk})$.

Step 1 Recall from Section 3.2.2 the inclusion $i : \Sigma_{g-1}^2 \to \Sigma_g$ induced by gluing the boundary components of Σ_{g-1}^2. Recall also the inverse map $i_*^{-1} : \mathcal{I}(\Sigma_g) \to \mathcal{I}(\Sigma_{g-1}^2)$. In this step we will show how to factorize an element $i_*^{-1}(f) \in \mathcal{I}(\Sigma_{g-1}^2)$ into elements of $K \rtimes \mathcal{I}(\Sigma_{g-1}^1)$, where $f \in \mathcal{I}(\Sigma_g)$, and $K \cong [\pi_1(\Sigma_{g-1}^1), \pi_1(\Sigma_{g-1}^1)]$.

Lemma 3.4. *Let $T_aT_{a'}^{-1}$ be a bounding pair map in $\mathcal{I}(\Sigma_g)$. Then there is a nonseparating simple closed curve b in R_1 (see Figure 3.12) such that the geometric intersection number of b and any of a, a' is zero.*

According to Lemma 3.4, we can find a simple closed curve $c \in R_1$ that is fixed by $T_aT_{a'}^{-1}$. Then, we cut the surface Σ_g along c. Denote the induced surface by Σ_{g-1}^2 and the boundaries by q_1, q_2. The induced bounding pair map $i_*^{-1}(T_aT_{a'}^{-1})$ depicted on the right hand side of the Figure 3.13 is denoted again by $T_aT_{a'}^{-1} \in \mathcal{I}(\Sigma_{g-1}^2)$. In this step we factorize $T_aT_{a'}^{-1}$ into terms of K and $\mathcal{I}(\Sigma_{g-1}^1)$.

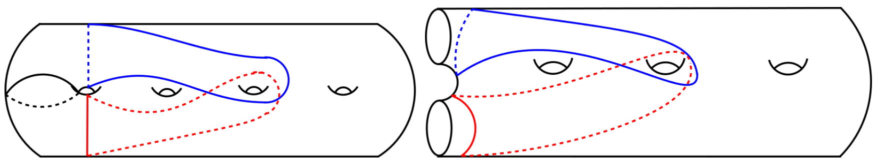


Figure 3.13: The bounding pair $[\![1267]\!]$ on the left lies on $\mathcal{I}(\Sigma_3^2)$ on the right.

1) First we glue a disc on the boundary q_1 of the surface Σ_{g-1}^2. The resulting bounding pair map now lies on Σ_{g-1}^1. In order to distinguish that map from $T_aT_{a'}^{-1}$, we denote it by $T_tT_{t'}^{-1}$. Then we glue a pair of pants on the boundary q_2 (see Figure 3.14), to obtain a new surface of genus $g-1$ with 2 boundary components.

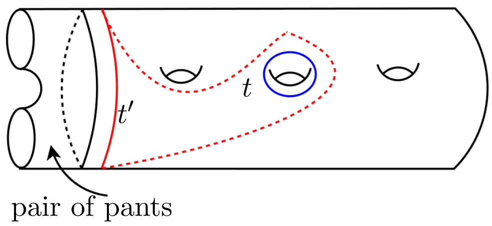


Figure 3.14: The bounding pair $T_t T_{t'}^{-1}$.

2) Returning to the original surface Σ_{g-1}^2, consider a separating curve μ such that q_1, q_2, μ bound a pair of pants as in Figure 3.14. The curves a, a' intersect with μ in 4 points p_1, p_2, p_3, p_4 and divide μ into 4 arcs $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$. Two points, say p_1, p_2, are in a, and the other two p_3, p_4 are in a'. Assume that the arc ϵ_1 has endpoints p_1, p_3. If we let the points p_1, p_3 move along the curves a, a', we have an arc like in Figure 3.15. The boundary of the regular neighborhood of $a \cup a' \cup \epsilon_1$ is a separating curve γ. In Figure 3.15 we show the curve γ when $T_a T_{a'}^{-1} = [1267]$.

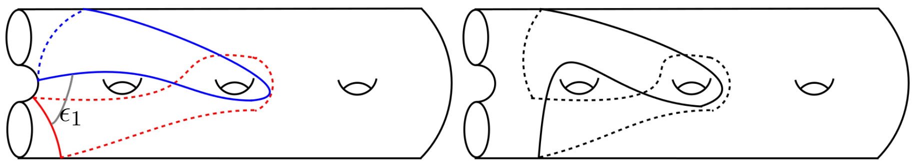


Figure 3.15: Obtaining a separating curve from two homologous non-separating curves.

3) Now we apply the lantern relation as follows. From the construction of γ we see that the curves a, a', γ bound a disc with two boundary components. Furthermore, since a is a regular neighborhood of t and q_1, we deduce that a', γ, t, q_1 form a disc with 3 boundary components. Since t' can be deduced from a' by gluing a disc to q_1, then we choose an appropriate arc between a' and q_1 such that their regular neighborhood is t'. Similarly, a regular neighborhood of a' and γ is a. Finally, we choose an arc between γ and q_1 to deduce a new curve namely $\overline{\gamma}$. Figure 3.16 shows an example for [1267].

Finally, using the lantern relation (see Figure 3.17) we deduce that

$$T_a T_{a'}^{-1} = ((T_{q_1} T_{\overline{\gamma}}^{-1}) T_\gamma)(T_t T_{t'}^{-1}) \in K \ltimes \mathcal{I}(\Sigma_{g-1}^1).$$

This finishes Step 1.

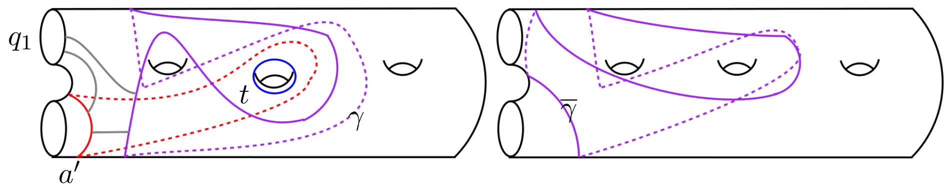


Figure 3.16: On the left the curves a', γ, q_1, t form a sphere with 4 boundary components. On the right the curve $\overline{\gamma}$ bounds the curves γ and q_1.

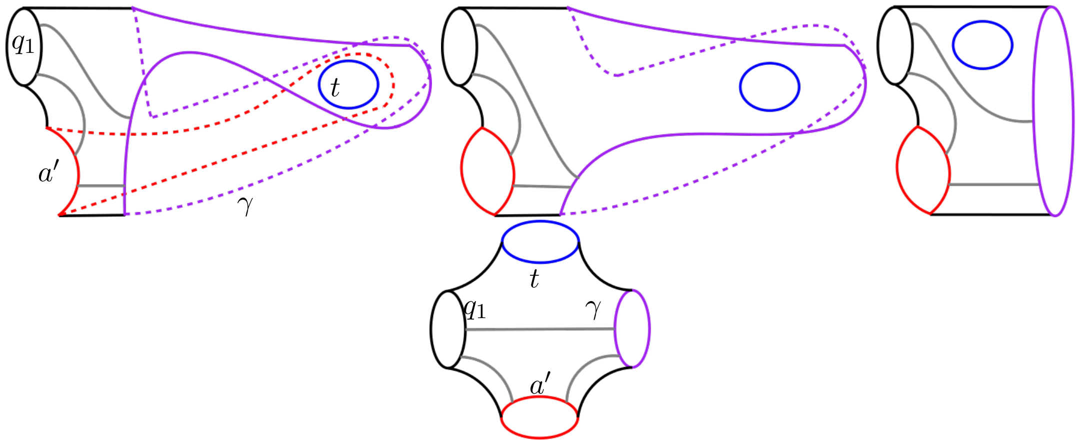


Figure 3.17: Cutting the surface Σ^2_{g-1} along a', γ, q_1, t to deduce a sphere with four boundaries.

Step 2 Now that we have a factorization for $T_a T_{a'}^{-1}$, we will conjugate it by C_7^{-1}, $C_7^{-1} * T_a T_{a'}^{-1} = (C_7^{-1} * ((T_{q_1} T_{\overline{\gamma}}^{-1}) T_\gamma))(C_7^{-1} * T_{t'} T_t^{-1})$. Consider the homomorphism $i_* : \mathrm{Mod}(\Sigma^2_{g-1}) \to \mathrm{Mod}(\Sigma_g)$ induced by gluing the boundaries of Σ^2_{g-1}. It is obvious that $i_*(C_7^{-1} * T_{t'} T_t^{-1})) \in \mathcal{I}(R_{234})$. But it is not obvious that $i_*(C_7^{-1} * ((T_{q_1} T_{\overline{\gamma}}^{-1}) T_\gamma))$ lies entirely in $\bigcup_{1 \le i<j<k \le 4} \mathcal{I}(R_{ijk})$. In this step we will show how to factorize the element $C_7^{-1} * ((T_{q_1} T_{\overline{\gamma}}^{-1}) T_\gamma)$.

Consider $[\![1267]\!] = T_a T_{a'}^{-1}$, and assume that $g = 4$. The curve $C_7^{-1}(\gamma) \in K$ depicted in Figure 3.18 is mapped into $C_7^{-1} * ((T_{q_1} T_{\overline{\gamma}}^{-1}) T_\gamma) \in K \ltimes \mathcal{I}(\Sigma^1_{g-1})$ under the pushing-disc map.

Consider the generators of the fundamental group shown in Figure 2.3. We set $\delta_k = \prod_k^{i=1} [a_i, b_i]$. We have

$$C_7^{-1}(\gamma) = b'_2 b_1^{-1} a_2 \delta_2^{-1} \delta_3 a_3^{-1} a_2^{-1} b_2'^{-1} b'_1 a_3.$$

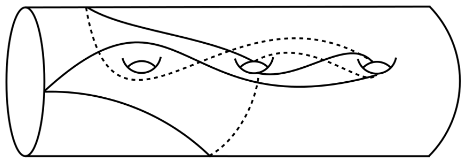


Figure 3.18: The curve $C_7^{-1}(\gamma) \in K$.

We would like to express $C_7^{-1}(\gamma)$ as a product of commutators. We have

$$C_7^{-1}(\gamma) = \delta_1[a_2^{-1}, b_1]^{a_2b_2}[a_2b_2, b_1^{-1}][a_3, b_3]^{b_1^{-1}a_2b_2}[a_2b_2, a_3^{-1}]^{b_1^{-1}}[b_1^{-1}, a_3^{-1}].$$

If f is any of the elements in the product above, except $[a_2b_2, a_3^{-1}]^{b_1^{-1}}$, and $[a_3, b_3]^{b_1^{-1}a_2b_2}$, then we have $i_*(f) \in \bigcup_{1\leq i<j<k\leq 4} \mathcal{I}(R_{ijk})$.

We want to find a homeomorphism $f_{b_1} \in \mathcal{I}(\Sigma_{g-1}^1)$ such that $f_{b_1}(a_i) = a_i^{b_1^{-1}}$ and $f_{b_1}(b_i) = b_i^{b_1^{-1}}$ for $i = 2$ or 3. This would imply that $f_{b_1}([a_2b_2, a_3^{-1}]) = [a_2b_2, a_3^{-1}]^{b_1^{-1}}$. The reason we need the homeomorphism f_{b_1} is the following. We set $\eta = [a_2b_2, a_3^{-1}]$. The image of $f_{b_1}(\eta)$ in $K \rtimes \mathcal{I}(\Sigma_{g-1}^1)$ is

$$(T_{q_1}T^{-1}_{f_{b_1}(\overline{\eta})})T_{f_{b_1}(\eta)} = f_{b_1}^{-1}(T_{c_1}T_{\overline{\eta}}^{-1})T_\eta f_{b_1}.$$

But $i_*(f_{b_1}) \in \mathcal{I}(R_{234})$ and $i_*(T_{c_1}T_{\overline{\eta}}^{-1})T_\eta) \in \mathcal{I}(R_{123})$, and this completes the factorization of $C_7^{-1}[1267]$ into elements of $\bigcup_{1\leq i<j<k\leq 4} \mathcal{I}(R_{ijk})$. If $g > 4$, the curve $C_7^{-1}(\gamma)$ admits the same factorization as above, but the elements $\{a_1, b_1, a_2, b_2, a_3, b_3\}$ are substituted by $\{a_{g-3}, b_{g-3}, a_{g-2}, b_{g-2}, a_{g-1}, b_{g-1}\}$, and $\delta_1, \delta_2, \delta_3$ by $\delta_{g-3}, \delta_{g-2}, \delta_{g-1}$.

Finding a homeomorphism f_w. We fix a base point x_0 in Σ_{g-1}^1 as in Figure 3.19. Let w be any of the elements a_{g-3}, b_{g-3} based on x_0, and let $[w]$ be its homology class. Consider a simple closed curve w' obtained from w by freely homotope the fixed point x_0. We denote the new fixed point by x_1 and we denote by ϵ the trace from x_0 to x_1. Then we glue a disc on the boundary of Σ_{g-1}^1, we push the curve w along ϵ, and then pass it over the disc to get a new curve w''. Then we remove that disc. We have that $[w] = [w'] = [w'']$. If we denote the boundary of Σ_{g-1}^1 by d, then we set

$$f_{a_{g-3}} = T_d(T_{a'_{g-3}}T^{-1}_{a''_{g-3}}),\ f_{b_{g-3}} = T_d^{-1}(T_{b''_{g-3}}T^{-1}_{b'_{g-3}}).$$

The homeomorphism f_w is in $\mathcal{I}(\Sigma_{g-1,1})$. Hence, $f_w^{-1}(a_i) = a_i^{w^{-1}}$, $f_w^{-1}(b_i) = b_i^{w^{-1}}$ and $f_w(a_i) = a_i^w$, $f_w(b_i) = b_i^w$ for $i = g-2$ or $g-1$.

If w is any of the elements a_{g-1}, b_{g-1} and $[w]$ its homology class then we follow the same process as before to find w' and w'', but this time set

$$f_{a_{g-1}} = T_{a'_{g-1}} T^{-1}_{a''_{g-1}},\ f_{b_{g-1}} = T_{b''_{g-1}} T^{-1}_{b'_{g-1}}.$$

Then for $i = g-2$ or $g-3$ and $z \in \{a_i, b_i\}$ we have

$$\begin{array}{rcl} f_{a_{g-1}}(z) & = & (\delta_{g-1}^{-1})^{a_{g-1}} z^{a_{g-1}} \delta_{g-1}^{a_{g-1}} \\ & = & \\ f^{-1}_{a_{g-1}}(z) & = & \delta_{g-1}^{-1} z^{a^{-1}_{g-1}} \delta_{g-1} \\ & = & \\ f_{b_{g-1}}(z) & = & \delta_{g-1}^{-1} z^{b_{g-1}} \delta_{g-1} \\ & = & \\ f^{-1}_{b_{g-1}}(z) & = & (\delta_{g-1}^{-1})^{b^{-1}_{g-1}} z^{b^{-1}_{g-1}} \delta_{g-1}^{b^{-1}_{g-1}} \end{array}$$

where $\delta_k = \prod_{j=1}^{k} [a_j, b_j]$. We note that if for example we want to factorize $[a_{g-2}, b_{g-3}]^{b_{g-1}}$, we do the following

$$[a_{g-2}, b_{g-3}]^{b_{g-1}} = \delta_{g-1} f_{b_{g-1}}([a_{g-2}, b_{g-3}]) \delta_{g-1}^{-1}.$$

This finishes Step 2.

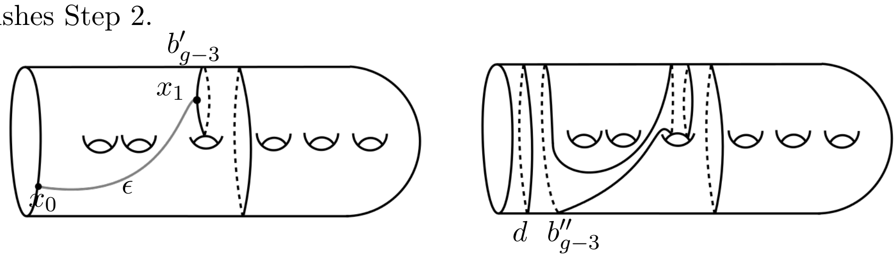


Figure 3.19: Finding the homeomorphism f_w.

3.3.4 Geometric proof to the generation of the Torelli group

In this section we prove that $\mathcal{I}(\Sigma_g)$ is generated by $\bigcup_{1\le i<j<k\le g} \mathcal{I}(R_{ijk})$. Let J_g be the group generated by $\bigcup_{1\le i<j<k\le g} \mathcal{I}(R_{ijk})$. Our aim is to prove that if we conjugate a generator of $\mathcal{I}(R_{ijk})$ by a generator of $\mathrm{Mod}(\Sigma_g)$, then the result lies in J_g. From now on when we say that $k \in \mathrm{Mod}(\Sigma_g)$ normalizes $h \in J_g$, we mean that $khk^{-1} \in J_g$. Consider the generators $T_{c_i} = C_i, T_{b_j} = B_j$ of $\mathrm{Mod}(\Sigma_g)$, depicted in Figure 3.4. It is obvious that $C_1^{\pm}, C_{2i}^{\pm}, B_j^{\pm}$ normalize J_g. It remains to check that $C_{2i+1}^{\pm 1}$ normalize J_g.

The first step of the proof is to show that $C_7^{\pm 1}$ normalize $\mathcal{I}(R_{123})$. Then we fix a set of generators for all $\mathcal{I}(R_{i_1 i_2 i_3})$, $i_1, i_2, i_3 \in \{1, 2, 3, ..., g\}$. In order to show that C_{2j+1} normalizes $\mathcal{I}(R_{i_1 i_2 i_3})$ for arbitrary $i_1 < i_2 < i_3$, we do the following: if $|i_k - j| > 1$ for all

$i_k \in \{i_1, i_2, i_3\}$, then C_{2j+1} commutes with every element of $\mathcal{I}(R_{i_1 i_2 i_3})$. Assume that for a fixed $i_k \in \{i_1, i_2, i_3\}$, we have $|i_k - j| = 1$. Then c_{2j+1} lies inside the regular neighborhood of $R_j \cup R_{i_k} \cup x_j \cup x_{i_k}$ (see Figure 3.12). Then for $g \in \mathcal{I}(R_{i_1 i_2 i_3})$ the element $C_{2g+1} * g$ lies inside $\mathcal{I}(S)$, where S is a regular neighborhood of $R_j \cup R_{i_1} \cup R_{i_2} \cup R_{i_3} \cup x_j \cup x_{i_1} \cup x_{i_2} \cup x_{i_3}$. The subsurface S is homeomoprhic to Σ_4^1. Our aim is to find a homeomorphism $h \in \mathrm{Mod}(\Sigma_g)$ satisfying the following:

1. The homeomorphisms $h^{\pm 1}$ normalize the elements of $\bigcup_{l_1, l_2, l_3 \in \{j, i_1, i_2, i_3\}} \mathcal{I}(R_{l_1 l_2 l_3})$ and $\bigcup_{1 \le l_1 \le l_2 \le l_3 \le 4} \mathcal{I}(R_{l_1 l_2 l_3})$.
2. Further, $h * C_{2g+1} = C_7$, and $h * g \in \mathcal{I}(R_{123})$.

Then we conjugate $C_{2g+1} * g$ by h to get $hC_{2g+1} * gh^{-1} = C_7 * hgh^{-1}$. But since $hgh^{-1} \in \mathcal{I}(R_{123})$, we have that $C_7 * hgh^{-1} \in \bigcup_{1 \le l_1 \le l_2 \le l_3 \le 4} \mathcal{I}(R_{l_1 l_2 l_3})$. Finally, since h^{-1} normalizes $\bigcup_{1 \le i_1 < l_2 < l_3 \le 4} \mathcal{I}(R_{l_1 l_2 l_3})$, we apply h^{-1} to get

$$C_{2g+1} * g \in \bigcup_{l_1, l_2, l_3 \in \{j, i_1, i_2, i_3\}} \mathcal{I}(R_{l_1 l_2 l_3}) \subset J_g.$$

We describe three homeomorphisms:

1. Let s be the involution which swaps the handles R_i, R_{g-i+1} for all $i \in \{1, 2, ..., g\}$. It is easy to see that s normalizes $\mathcal{I}(R_{ijk})$ if $|k - i| \le 3$ and $i < j < k$.
2. Let h be the homeomorphism, which moves the handle R_g as in Figure 3.20. The homeomorphism h normalizes J_g. Also, $h^2(c_{2g-1}) = c_3$, $h(c_{2g}) = c_2$, and $h(c_i) = c_{i+2}$ if $i \le 2g - 2$.
3. Let $H_{i,j}$ be a homeomorphism, which takes the handle R_i and places it between the handles R_{j-1} and R_j as in Figure 3.21. If $i \notin \{i_1, i_2, i_3\}$, then $H_{i,j}$ normalizes $\mathcal{I}(R_{i_1 i_2 i_3})$.

In order to show that C_{2j+1} normalizes $f \in \mathcal{I}(R_{i_1 i_2 i_3})$, we use an appropriate composition of homeomorphisms $s, h, H_{i,j}$. For example, in $\mathcal{I}(\Sigma_5)$, if $g \in \mathcal{I}(R_{134})$ and $j = 1$, then $shH_{2,1} * (C_3 * g) = C_7 * (shH_{2,1} * g)$, where $shH_{2,1} * g \in \mathcal{I}(R_{123})$. Hence, we only need to prove the following lemma.

Lemma 3.5. *The generators $C_7^{\pm 1}$ normalize $\mathcal{I}(R_{123})$.*

Proof. We have the relation $w(C_7 * w^{-1}) = (C_7^{-1} * w)w^{-1}$, where w is a straight chain [35, Lemma 7]. Thus we only need to check that C_7 normalizes $\mathcal{I}(R_{123})$. We want to

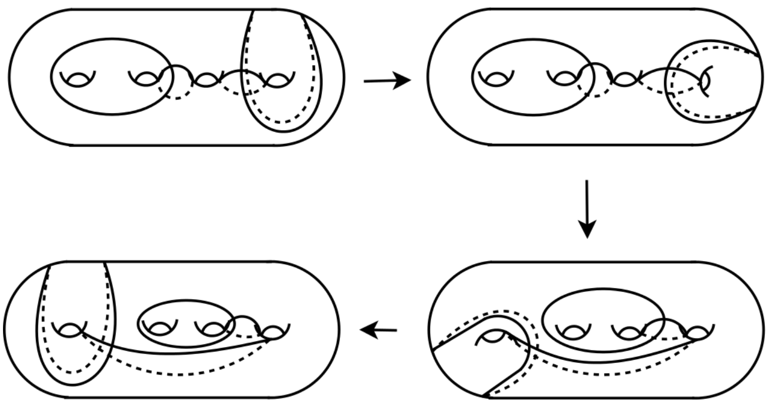


Figure 3.20: The homeomorphism h.

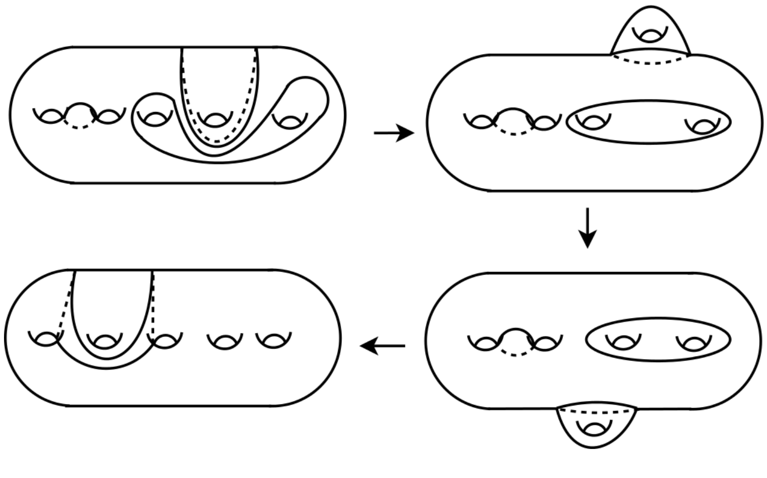


Figure 3.21: The homeomorphism $H_{i,j}$.

prove that $C_7 * [\![i_1 i_2 i_3 ... i_l]\!] \in J_4$ where $1 \leq i_1 < i_2 < i_3 < ... < i_l \leq 7$. If $i_l \leq 6$, then $C_7 * [\![i_1 i_2 i_3 ... i_l]\!] \in \mathcal{I}(R_{123})$. It remains to prove that $C_7 * [\![i_1 i_2 i_3 ... 7]\!] \in J_4$. If $k \in \mathrm{Mod}(\Sigma_4)$ normalizes $\mathcal{I}(R_{123})$ and commutes with C_7, then $C_7 * w \in J_4$ is equivalent to $kC_7 * w \in J_4$, where $w \in J_4$. We call that the *Johnson trick*. Since C_1, C_2, C_4, C_6, B normalize J_4 and commute with C_7 we only need to check that $C_7^{-1} * [\![1267]\!]$, $C_7^{-1} * [\![1247]\!]$, $C_7^{-1} * [\![3457]\!]$, $C_7 * [\![3467]\!]$, $C_7^{-1} * [\![4567]\!]$, $C_7^{-1} * [\![1237]\!]$, and $C_7^{-1} * [\![i_1 i_2 i_3 i_4 i_5 7]\!]$ lie on J_4 by the Johnson trick.

We have already seen in the previous section that $C_7^{-1} * [\![1267]\!] \in J_4$. We apply the algorithm described in the previous section for $C_7^{-1} * [\![1247]\!]$, $C_7^{-1} * [\![3457]\!]$, and $C_7 * [\![3467]\!]$. The elements $C_7^{-1} * [\![4567]\!]$, and $C_7^{-1} * [\![1237]\!]$ obviously lie in $\mathcal{I}(R_{234})$.

We cut the surface Σ_g along the curve c_1 depicted in Figure 3.4 to get a genus $g-1$ surface with 2 boundary components. We denote the resulting surface by $\Sigma_{g-1,2}$. Recall the inclusion $i : \Sigma_{g-1,2} \hookrightarrow \Sigma_g$ from Section 3.2.3, and the induced homomorphism $i_* : \mathrm{Mod}(\Sigma^2_{g-1}) \to \mathrm{Mod}(\Sigma_g, c_1) < \mathrm{Mod}(\Sigma_g)$; where $\mathrm{Mod}(\Sigma_g, c_1)$ stands for the stabilizer subgroup of c_1. The following bounding pair maps lie entirely in $\mathcal{I}(\Sigma^2_{g-1})$:

$$i_*^{-1}(C_7^{-1} * [\![1247]\!]), i_*^{-1}(C_7^{-1} * [\![3457]\!]), i_*^{-1}(C_7 * [\![3467]\!])$$

By Step 1 of the main algorithm we have the factorizations

$$i_*^{-1}(C_7^{-1} * [\![1247]\!]) = ((T_c T_{\overline{\gamma}_1}^{-1}) T_{\gamma_1}, T_{t_1} T_{t'_1}^{-1}),$$

$$i_*^{-1}(C_7^{-1} * [\![3457]\!]) = ((T_c T_{\overline{\gamma}_2}^{-1}) T_{\gamma_2}, T_{t_2} T_{t'_2}^{-1}),$$

$$i_*^{-1}(C_7 * [\![3467]\!]) = ((T_c T_{\overline{\gamma}_3}^{-1}) T_{\gamma_3}, T_{t_3} T_{t'_3}^{-1}).$$

In Section 3.2.3 we described the disc-pushing map $K \to K \rtimes \mathcal{I}(\Sigma^1_{g-1})$ $\eta_i \mapsto (T_c T_{\overline{\gamma}_i}^{-1}) T_{\gamma_i}$, $i = \{1, 2, 3\}$ where K is isomorphic to $[\pi_1(\Sigma^1_{g-1}, x_0), \pi_1(\Sigma^1_{g-1}, x_0)]$. We set $\delta_k = \prod_{i=1}^k [a_i, b_i]$. If $g-1 = 3$ we have

$$\begin{aligned}
\eta_1 &= b'_2 b_1^{-1} a_2 b_2 a_3 b_3^{-1} a_3^{-1} b_2^{-1} a_2^{-1} b_1 b_2'^{-1} b_3 \\
&= \delta_2 [b_2, b_1^{-1}] f_{b_1}^{-1}([a_2 b_2, b_3^{-1}]^{b_2} [b_2, b_3^{-1}][b_3, a_3]^{b_3^{-1} b_2 a_2 b_2}) [b_1^{-1}, b_3^{-1}] \\
&\quad \delta_3^{b_3^{-1}} f_{b_3}^{-1}([b_1^{-1}, b_2])(\delta_3^{-1})^{b_3^{-1}} (\delta_2^{-1})^{b_3^{-1}},
\end{aligned}$$

$$\begin{aligned}
\eta_2 &= b_2^{-1} a_2^{-1} b_1 b_2'^{-1} \delta_3 a_3^{-1} b_2 b_1^{-1} a_2 b_2 a_3 \\
&= [b_2^{-1} a_2^{-1}, b_1 b_2^{-1}] f_{b_1}([a_3, b_3]^{b_2^{-1} a_2^{-1}} [b_2^{-1} a_2^{-1}, a_3^{-1}]^{b_2^{-1}} [b_2^{-1}, a_3^{-1}]) \\
&\quad [a_3^{-1}, b_1^{-1}]^{b_1} \delta_3^{-1} f_{a_3}^{-1}([b_1 b_2^{-1}, b_2^{-1} a_2^{-1}]) \delta_3,
\end{aligned}$$

$$\begin{aligned}
\eta_3 &= b_1^{-1} \delta_3^{-1} \delta_2 b_2 a_2^{-1} b_1^{-1} \delta_1^{-1} \delta_3 b_3 a^{-1} b_2^{-1} \delta_2^{-1} \delta_1 b_1 a_2 a_3 \\
&= [b_3, a_3]^{b_3^{-1}} \delta_3^{b_3^{-1}} f_{b_3}^{-1}([b_2 a_2^{-1}, b_1^{-1}])(\delta_3^{-1})^{b_3^{-1}} [b_3^{-1}, b_1^{-1}] f_{b_1}^{-1}([b_3^{-1}, b_2 a_2^{-1}]) \\
&\quad [b_1^{-1}, b_2 a_2^{-1}][b_2, a_2^{-1} b_1] f_{b_1}^{-1}(([a_2, b_2][a_3, b_3])^{a_2^{-1} b_2 b_3^{-1}} [a_3, b_2^{-1}]^{a_2^{-1} b_2}) \\
&\quad f_{b_1}^{-1}([b_2, a_2]^{a_2^{-1} a_3^{-1}}) f_{b_1}([a_2^{-1}, a_3^{-1}])[b_1^{-1}, a_3^{-1}] \delta_3^{-1} f_{a_3}^{-1}([b_1^{-1}, a_2^{-1}]) \delta_3.
\end{aligned}$$

If $g-1 \geq 3$, then the curves η_i admit the same factorization but the elements $\{a_1, b_1, a_2, b_2, a_3, b_3\}$ are replaced by $\{a_{g-3}, b_{g-3}, a_{g-2}, b_{g-2}, a_{g-1}, b_{g-1}\}$.

It remains to prove that $C_7^{-1} * [\![i_1 i_2 i_3 i_4 i_5 7]\!]$ lies in J_g. We only need to check the elements $C_7 * [\![234567]\!]$, $C_7 * [\![134567]\!]$, $C_7 * [\![124567]\!]$ because the rest lie in $\mathcal{I}(R_{234})$. Consider the curves depicted in Figure 3.22. These curves form the lantern relation $C_2 C_4 C_6 T_d = T_b T_a T_e$. We reflect the curves with respect to the page. The resulting curves are denoted by d', e', a', b' and they form the relation $C_2 C_4 C_6 T_{d'} = T_{e'} T_{a'} T_{b'}$.

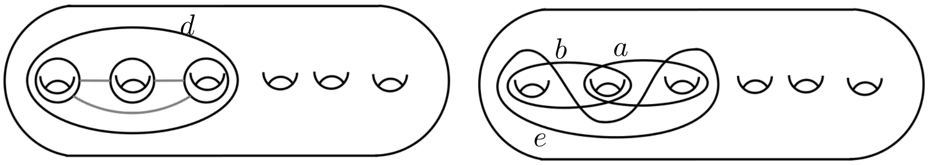


Figure 3.22: Curves that form a lantern relation.

Inverting the second relation and multiplying it by the first, we deduce that

$$[\![234567]\!] = [\![2345]\!][\![4567]\!]T_e T_{e'}^{-1}.$$

We conjugate the above relation first by C_7^{-1}, then by C_1^{-1}, and finally by C_2^{-1}. Those conjugations give the desired result. $\square$

By Lemma 3.5, we have that if $f \in \mathcal{I}(R_{123})$ then $C_7^{\pm 1} * f \in \bigcup_{1\le i<j<k\le 4} \mathcal{I}(R_{ijk})$. Using the argument given before Lemma 3.5 with the three families of homeomorphisms $H_{i,j}, s, h$ we obtain the following corollary.

Theorem 3.6 (Church-Putman)**.** *The group $\mathcal{I}(\Sigma_g)$ is generated by $\bigcup_{1\le i<j<k\le g} \mathcal{I}(R_{ijk})$.*

We finish this chapter by finding generators for $\mathcal{I}(\Sigma_g^1)$.

Theorem 3.7 (Church-Putman)**.** *The group $\mathcal{I}(\Sigma_g^1)$ is generated by $\bigcup_{1\le i<j<k\le g} \mathcal{I}(R_{ijk})$.*

Proof. Consider the Birman exact sequence

$$1 \to \pi_1(U\Sigma_g) \to \mathcal{I}(\Sigma_g^1) \to \mathcal{I}(\Sigma_g) \to 1,$$

where $U\Sigma_g$ stands for the unit tangent bundle of Σ_g [52, Theorem 1.2]. Let Γ_g be the subgroup of $\mathcal{I}(\Sigma_g^1)$ generated by $\bigcup_{1\le i<j<k\le g} \mathcal{I}(R_{ijk})$. By Corollary 3.6 we only need to prove that $\pi_1(U\Sigma_g)$ injects into Γ_g. We prove the theorem by induction on $g \geq 4$.

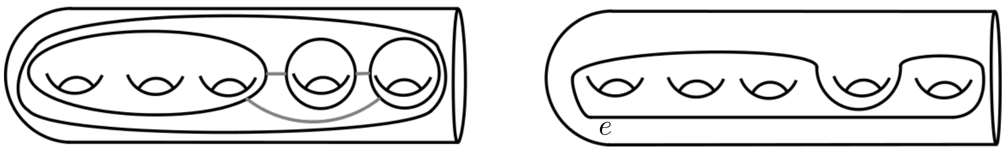


Figure 3.23: Curves that form a lantern relation.

Johnson proved that $\pi_1(U\Sigma_g)$ is generated by the maximal odd chains maps $[\![i_1 i_2 ... i_{2g-1}]\!]$ plus $B^{-1} * [\![234...2g+1]\!]$, where B is the Dehn twist about b_1 as in Figure 3.4, [35, Lemma

7]. We need to generalize the lantern of Figure 3.22. The curves indicated on the left hand side of the Figure 3.23 bound a sphere with 4 boundary components. By using the same strategy like in the proof of Lemma 3.5 we obtain the following relation:

$$[\![234...2g-3]\!][\![2345...2g+1]\!] = [\![234...2g-1]\!][\![2g-2, 2g-1, 2g, 2g+1]\!]T_e T_{e'}^{-1}.$$

We prove the theorem by induction on g. If $g = 4$, we note that we already have $[\![12345 i_1 i_2 i_3 i_4]\!] \in \mathcal{I}(R_{234})$. The relation above shows that $[\![23456789]\!] \in \Gamma_4$. We conjugate the latter relation by B^{-1} and we have that $B^{-1} * [\![23456789]\!] \in \Gamma_4$. We complete the proof in the case $g = 4$ by conjugating the above relation by $C_1^{-1}, C_2^{-1}, C_3^{-1}$, and C_4^{-1}. If $g \geq 5$, we use the same relation we constructed above and the theorem follows by the inductive argument. $\square$

Johnson proved that $\mathrm{H}_1(\mathcal{I}(\Sigma_g);\mathbb{Z})$ (resp. $\mathrm{H}_1(\mathcal{I}(\Sigma_g^1);\mathbb{Z})$) has rank $(4g^3+5g+3)/3$ (resp. $(4g^3-g)/3$) [37]. These give large lower bounds on the size of generating sets for $\mathcal{I}(\Sigma_g)$ and $\mathcal{I}(\Sigma_g^1)$. Unfortunately, the cardinality of the generating set in Theorems 3.6 and 3.7 is $42\binom{g}{3}$, which is much larger compared to the lower bound. Potentially, it would be interesting to see whether we can use the algorithm of Section 3.3.3 to find relations between generators of the Torelli group and then reduce the cardinality of the generating set.

Part II

Factor groups of braid groups, and the hyperelliptic mapping class group

Chapter 4

Braid groups

In this chapter we define braid groups, and pure braid groups. Braid groups are closely related to mapping class groups. Let $\Sigma_{g,n}^b$ be an n-punctured surface of genus g with b boundary components. We show that the mapping class group of a punctured disc $\Sigma_{0,n}^1$ has the structure of a braid group. Then we define a proper subgroup of the mapping class group of Σ_g^b, namely the hyperelliptic mapping class group $\mathrm{SMod}(\Sigma_g^b)$, and we show that it is closely related to braid group.

4.1 Several definitions of braid groups

Braid groups were introduced by Emil Artin in 1925. There are several definitions of braid groups, given, for example, in terms of fundamental groups of configurations spaces, mapping class groups, and subgroups of automorphism groups. In this section we present the above definitions and we provide generators, and relations.

4.1.1 Geometric definition

Consider the space $[0,1] \times \mathbb{R}^2$ with n collinear points lying in $\{0\} \times \mathbb{R}^2$ in positions $(0,1,0),(0,2,0),...,(0,n,0)$. Consider also n collinear points in $\{1\} \times \mathbb{R}^2$ in positions $(1,1,0),(1,2,0),...,(1,n,0)$. For $1 \leq i \leq n$, define the injective continuous functions $a_i : [0,1] \to [0,1] \times \mathbb{R}^2$ such that $a_i(0) = (0,i,0)$ and $a_i(1) = (1,i,0)$. The functions a_i are simple curves in $[0,1] \times \mathbb{R}^2$. Furthermore, for $i \neq j$ and $t_0 \in [0,1]$, we have that $a_i(t_0) \neq a_j(t_0)$. A multicurve of the form $a(t) = (a_1(t), a_2(t), ..., a_n(t))$ is called a *geometric braid* on n strands.

Let $a(t) = (a_1(t), a_2(t), ..., a_n(t))$ and $b(t) = (b_1(t), b_2(t), ..., b_n(t))$ be two braids. If there exists an isotopy $F : [0,1] \times [0,1] \to [0,1] \times \mathbb{R}^2$ such that $F(t,0) = a(t)$ and

$F(t,1) = b(t)$, then these two geometric braids will be called isotopic. We will denote the isotopy classes of braids by $[a]$. Denote by B_n, the set of the isotopy classes of geometric braids with n strands. For an illustration consult Figure 4.1. The elements of B_n are called *braids*.

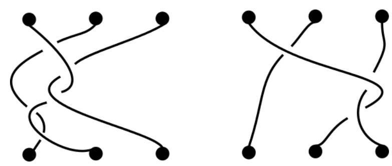


Figure 4.1: Two isotopic braids.

Next we define an operation between braids. Let $[a],[b] \in B_n$. Consider two representatives a, b of $[a],[b]$ respectively. By definition we have $a, b : [0,1] \to [0,1] \times \mathbb{R}^2$. Rescale b to obtain $b' : [1,2] \to [1,2] \times \mathbb{R}^2$. By noting that $a(1) = b'(1)$, we define the map $a \circ b : [0,2] \to [0,2] \times \mathbb{R}^2$ by

$$\begin{cases} a : [0,1] \to [0,1] \times \mathbb{R}^2 \\ b' : (1,2] \to [0,1] \times \mathbb{R}^2. \end{cases}$$

Further, rescaling $a \circ b$ we obtain the geometric braid $a * b : [0,1] \to [0,1] \times \mathbb{R}^2$. Define the operation between the isotopy classes of braids by $[a] * [b] = [a * b]$. This operation is well defined. Indeed, let a, b, c, d be four geometric braids, and for $i \in \{1,2\}$, let $F_i : [0,1] \times [0,1] \to [0,1] \times \mathbb{R}^2$ be two isotopies such that

$$F_1(t,0) = a,\ F_1(t,1) = c,$$

$$F_2(t,0) = b,\ F_2(t,1) = d.$$

We want to show that $[a*b] = [c*d]$. But this is easy if we think of the following isotopy:

$$F(t,x) = \begin{cases} F_1(t,2x) & \text{if } 0 \leq x < 1/2, \\ F_2(t,2x-1) & \text{if } 1/2 \leq x \leq 1. \end{cases}$$

The set B_n together with $*$ defines a group. Indeed, the operation $*$ is closed on B_n and associative. The identity element is the braid, whose strands are perpendicular to the plane $\{0\} \times \mathbb{R}^2$. The inverse of an isotopy class of the braid $[a]$, is the braid a^{-1} obtained by reflecting its strands with respect to the plane $\{1/2\} \times \mathbb{R}^2$. See for example Figure 4.2.

The group $(B_n, *)$ is called the *braid group on n strands*. In the rest of the paper we use the notation B_n instead of $(B_n, *)$, a instead of $[a]$, and if $a, b \in B_n$, we use the

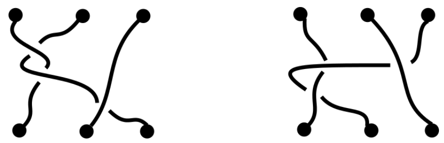


Figure 4.2: A braid with its inverse.

notation ab instead of $a * b$.

Next we generators of the braid group. Consider $i = 1, 2, ..., n-1$ and denote by σ_i the braid depicted in Figure 4.3.

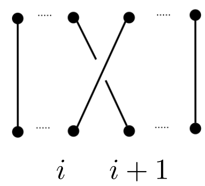


Figure 4.3: The generator σ_i.

Theorem 4.1 (Artin). *The group B_n is generated by the elements σ_i.*

Before we prove the theorem we need a definition. Consider the braids depicted in Figure 4.4. These braids show three forbidden positions.

A braid diagram is a braid b projected on $[0,1] \times \mathbb{R}$. On the left hand side of the Figure 4.4 three strands intersect at a single point. In the middle of Figure 4.4 two crossings are depicted in the same height. Finally, the right hand side of the Figure 4.4, one strand is tangent to another strand. These three position are called *forbidden positions* for a braid. A braid diagram a is said to be in *general position* if for every subset $[x, y]$ of $[0,1]$, the restriction $a : [x, y] \to [x, y] \times \mathbb{R}^2$ is not in a forbidden position.

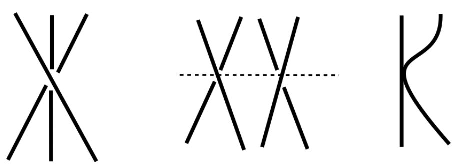


Figure 4.4: Forbidden positions for a braid.

Proof. (of Theorem 4.1) Consider a braid in B_n. Project this braid in $[0,1] \times \mathbb{R}$. We can deform the braid such that each crossing contains only two braids. If there is $t \in [0,1]$ such that there are two or more crossings, we deform the braid in such a way that there is only one crossing for distinct values of $t \in [0,1]$. We apply these deformation from the bottom to the top of the braid. Then the braid is in general position. Then it is easy to see that it will always be a product of $\sigma_i^{\pm 1}$, $1 \leq i \leq n-1$. Thus, B_n is generated by σ_i. □

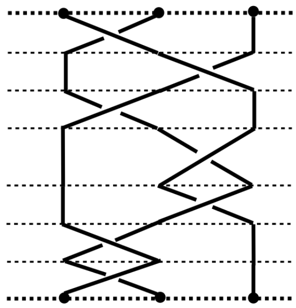


Figure 4.5: A braid in general position.

For example, the braid in Figure 4.5 is $\sigma_1\sigma_1^{-1}\sigma_2^2\sigma_1\sigma_2^{-1}\sigma_1^{-1}$. The generators σ_i satisfy two relations.

1. We have that $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for all $i < n-1$.

2. If $|i-j| > 1$, then $\sigma_i\sigma_j = \sigma_j\sigma_i$.

In 1925 Emil Artin proved that B_n admits a presentation with generators σ_i and the relations above [5].

We denote by S_n the symmetric group with generators the transposition $s_i = (i, i+1)$; consider the surjective homomorphism $B_n \to S_n$. This homomorphism associates to a generator σ_i the permutation s_i. The kernel is the *pure braid group* denoted by PB_n. Intuitively, a pure braid consists of strings with the same endpoints. Let $1 \leq i < j \leq n$; denote by $a_{i,j}$ the element $\sigma_{j-1}...\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}...\sigma_{j-1}^{-1}$ (see Figure 4.6).

Theorem 4.2 (Artin)**.** *The group PB_n is generated by the set $\{a_{i,j} \mid 1 \leq i < j \leq n\}$.*

Proof. We consider B_{n-1} as a subgroup of B_n by adding one string perpendicular to the plane $\mathbb{R}^2$ to each braid in B_{n-1}. Then, PB_{n-1} is a subgroup of PB_n. We prove the theorem by induction on the number of strings. When $n = 2$ the statement is obviously

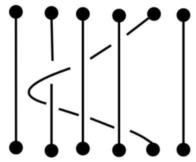


Figure 4.6: The braid $a_{i,j}$.

true. Let $a \in PB_n$ and delete the string connecting the points p_n. Denote by b the resulting braid. The braid b lies in PB_{n-1}. By the inductive hypothesis, b is a word on $\{a_{i,j}\}$. But we also have that $b \in PB_n$. Then ab^{-1} is the braid whose strings are vertical except the last one. See for example Figure 4.7 on the left. But then we can express ab^{-1} as a product of $\{a_{i,j}\}$ like in Figure 4.7 on the right. Since b and ab^{-1} are product of $a_{i,j}$-s, the same is true for a.

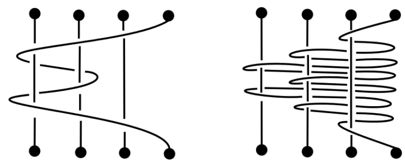


Figure 4.7: The braid $a * b^{-1}$.

□

We finish this subsection by providing a presentation for PB_n. Consider the relations:

P1. $a_{r,s}^{-1}a_{i,j}a_{r,s} = a_{i,j}$, $1 \leq r < s < i < j \leq n$ or $1 \leq i < r < s < j \leq n$,

P2. $a_{r,s}^{-1}a_{i,j}a_{r,s} = a_{r,j}a_{i,j}a_{r,j}^{-1}$, $1 \leq r < s = i < j \leq n$,

P3. $a_{r,s}^{-1}a_{i,j}a_{r,s} = (a_{i,j}a_{s,j})a_{i,j}(a_{i,j}a_{s,j})^{-1}$, $1 \leq r = i < s < j \leq n$,

P4. $a_{r,s}^{-1}a_{i,j}a_{r,s} = (a_{r,j}a_{s,j}a_{r,j}^{-1}a_{s,j}^{-1})a_{i,j}(a_{r,j}a_{s,j}a_{r,j}^{-1}a_{s,j}^{-1})^{-1}$, $1 \leq r < i < s < j \leq n$.

It turns out that the pure braid group PB_n is generated by $\{a_{i,j}\}$, for $1 \leq i < j \leq n$ with relations $P1, P2, P3, P4$ [9, Lemma 1.8.2].

4.1.2 Fundamental group of configuration spaces

There is another topological definition of braid groups. The *configuration space* of n points of the complex plane $\mathbb{C}$ is defined to be:

$$\mathcal{C}(n) = \{(z_1, ..., z_n) \in \mathbb{C}^n \mid z_i \neq z_j \text{ when } i \neq j\}.$$

An element of $\mathcal{C}(n)$ is denoted by $\vec{z} = (z_1, ..., z_n)$. The space $\mathcal{C}(n)$ is called the *configuration space of n ordered points* of the complex plane, and it turns out that it is a manifold of dimension $2n$. The symmetric group S_n acts freely on $\mathcal{C}(n)$ by permuting the coordinates of $\vec{z} \in \mathcal{C}(n)$. The quotient space $\mathcal{C}(n)/S_n$ is called the *configuration space of n unordered points* of the complex plane. We have the projection $\tau : \mathcal{C}(n) \to \mathcal{C}(n)/S_n$. Fix a point $\vec{p} \in \mathcal{C}(n)$. We define:

$$B_n := \pi_1(\mathcal{C}(n)/S_n, \tau(\vec{p})),$$

$$PB_n := \pi_1(\mathcal{C}(n), \vec{p}).$$

By definition the groups $\pi_1(\mathcal{C}(n), \vec{p})$ and $\pi_1(\mathcal{C}(n)/S_n, \tau(\vec{p}))$ consist of closed curves on $\mathcal{C}(n)$ and $\mathcal{C}(n)/S_n$, based on $\vec{p}$ and $\tau(\vec{p})$ respectively.

We explain how elements of $\pi_1(\mathcal{C}(n), \vec{p})$ can be considered as braids. Firstly, since for any $\vec{z} = (z_1, ..., z_n) \in \mathcal{C}(n)$, we have that $z_i \neq z_j$; we can think of $\vec{z}$ as a set of n distinct points on $\mathbb{C}$. A closed curve in $\mathcal{C}(n)$ is a continuous map $g : [0, 1] \to \mathcal{C}(n)$ such that $g(t) = (g_1(t), ..., g_n(t))$, for $g_i : [0, 1] \to \mathbb{C}$, and $g(0) = g(1)$. Furthermore, for each $t_0 \in [0, 1]$ we have that $g_i(t_0) \neq g_j(t_0)$. Denote by $g'(t)$, the multicurve obtained from $g(t)$ by projecting $g(t)$ onto $\mathbb{C}$ for all $t \in [0, 1]$. Then the element $(t, g'(t)) \in [0, 1] \times \mathbb{C}$ represents an element of PB_n.

Consider $s \in S_n$ and denote the action of the symmetric group on $\mathcal{C}(n)$ by $s(z) \in \mathcal{C}(n)$, for $z \in \mathcal{C}(n)$. A closed curve in $\mathcal{C}(n)/S_n$ is a continuous map $h[0, 1] \to \mathcal{C}(n)$ such that $h(t) = (h_1(t), ..., h_n(t))$, for $h_i : [0, 1] \to \mathbb{C}/S_n$, and $h(1) = s(h(0))$. Furthermore, for each $t_0 \in [0, 1]$ we have that $h_i(t_0) \neq h_j(t_0)$. Denote by $h'(t)$, the multicurve obtained from $h(t)$ by projecting $h(t)$ onto $\mathbb{C}/S_n$ for all $t \in [0, 1]$. Then the element $(t, h'(t)) \in [0, 1] \times \mathbb{C}$ represents an element of B_n. For a detailed discussion of the representations above, see, for example, Birman's book [9, Definitions 1.1].

We can think of the map $\tau : \mathcal{C}(n) \to \mathcal{C}(n)/S_n$ as a covering space, and of S_n as the group of deck transformations. Then we have a short exact sequence:

$$1 \to \pi_1(\mathcal{C}(n), \vec{p}) \to \pi_1(\mathcal{C}(n)/S_n, \tau(\vec{p})) \to S_n \to 1.$$

In other words we have obtained the same short exact sequence of the previous subsection:

$$1 \to PB_n \to B_n \to S_n \to 1. \tag{4.1}$$

4.1.3 Subgroup of automorphism of free groups

Let F_n be the free group generated by $x_1, x_2, ..., x_n$. Let $\mathrm{Aut}(F_n)$ be the automorphism group of F_n. Consider the subgroup A_n of $\mathrm{Aut}(F_n)$ generated by maps $\sigma_i : F_n \to F_n$, $1 \leq i \leq n-1$ of the form

$$\sigma_i(x_j) = \begin{cases} x_i x_{i+1} x_i^{-1} & \text{if } i = j, \\ x_i & \text{if } j = i+1, \\ x_j & \text{otherwise.} \end{cases}$$

Direct calculations show that the generators σ_i satisfy the braid relations. For example, $\sigma_i \sigma_{i+1} \sigma_i(x_i) = x_i x_{i+1} x_{i+2} x_{i+1}^{-1} x_i^{-1} = \sigma_{i+1} \sigma_i \sigma_{i+1}(x_i)$. It turns out that A_n is isomorphic to B_n [9, Theorem 1.9].

4.1.4 Braid groups as mapping class groups

We recall that $\mathrm{Mod}(\Sigma_{g,n}^b) = \pi_0(\mathrm{Diff}^+(\Sigma_{g,n}^b))$, where $\mathrm{Diff}^+(\Sigma_{g,n}^b)$ is the group of orientation preserving diffeomorphisms of $\Sigma_{g,n}^b$ fixing the boundary pointwise. Let P be the set containing the marked points of $\Sigma_{g,n}^b$. The subgroup of $\mathrm{Mod}(\Sigma_{g,n}^b)$, which contains elements fixing the marked points of the surface $\Sigma_{g,n}^b$, is called the *pure mapping class group*, and it is denoted by $\mathrm{PMod}(\Sigma) = \pi_0(\mathrm{Diff}^+(\Sigma, P))$.

Let $D_n = \Sigma_{0,n}^1$ be the disc containing n marked points on its interior. The purpose of this section is to present a proof of the following theorem.

Theorem 4.3. *The group* $\mathrm{PMod}(D_n)$ *is isomorphic to* PB_n*, and the group* $\mathrm{Mod}(D_n)$ *is isomorphic to* B_n*.*

Before we prove the theorem we would like to describe how a diffeomorphism can be considered as a braid and vice versa. Let D be the disc without marked points and also let the inclusion $i : \mathrm{Diff}^+(D_n) \to \mathrm{Diff}^+(D)$. Consider any element $f \in \mathrm{Diff}^+(D_n)$; then $i(f)$ is isotopic to the identity in $\mathrm{Diff}^+(D)$, since the latter group is isomorphic to the trivial group. Let F_t, for $t \in [0,1]$, be the isotopy transforming f into the identity element. Under this transformation the points are moving around the disc D tracing n paths. We can consider these paths as strings in $[0,1] \times D$. This process defines a geometric braid and its equivalence class is the image of the equivalence class of f in the braid group B_n.

Consider now a braid inside the cylinder $[0,1]\times D_n$. The strings of the braid connect the n points of $\{0\}\times D_n$ with the n points of $\{1\}\times D_n$. The cylinder $[0,1]\times D_n$ deformation retracts to D_n. This retraction is described by an isotopy F_t, for $t\in[0,1]$. Hence, F_1 is the desired homeomorphism. Now we can prove Theorem 4.3.

Proof. Our aim is to prove that $\mathrm{PMod}(D_n)\cong\pi_1(\mathcal{C}(n),\vec{p})$ and $\mathrm{Mod}(D_n)\cong\pi_1(\mathcal{C}(n)/S_n,\tau(\vec{p}))$. Consider the disc D as a subspace of $\mathbb{C}$. Recall that $\mathrm{Diff}^+(D_n,P)$ is a subgroup of $\mathrm{Diff}^+(D)$. Recall also that we can represent any element of $\mathcal{C}(n)$ by n distinct points on $\mathbb{C}$. It is convenient to us to represent elements of $\mathcal{C}(n)$ by n distinct points on D.

Let $\mathcal{E}:\mathrm{Diff}^+(D)\to\mathcal{C}(n)$ be the continuous map defined by $\mathcal{E}(f)=(f(z_1),...,f(z_n))$. Observe that if $f\in\mathrm{Diff}^+(D_n,P)$, then $(f(z_1),...,f(z_n))=(z_1,...,z_n)$. Furthermore, if $f_1,f_2\in\mathrm{Diff}^+(D)$ such that $\mathcal{E}(f_1)=\mathcal{E}(f_2)$, then $f_2^{-1}f_1\in\mathrm{Diff}^+(D_n,P)$. In other words f_1,f_2 are contained in the same coset of $\mathrm{Diff}^+(D_n,P)$ in $\mathrm{Diff}^+(D)$. Thus the map $\mathcal{E}:\mathrm{Diff}^+(D)\to\mathcal{C}(n)$ is a fiber space map with fiber $\mathrm{Diff}^+(D_n,P)$. Then we have a long exact sequence:

$$...\to\pi_1(\mathrm{Diff}^+(D))\to\pi_1(\mathcal{C}(n))\to\pi_0(\mathrm{Diff}^+(D_n,P))\to\pi_0(\mathrm{Diff}^+(D))\to...$$

But $\pi_1(\mathrm{Diff}^+(D))=\pi_0(\mathrm{Diff}^+(D))=\{1\}$. Hence, $\pi_1(\mathcal{C}(n))$ and $\pi_0(\mathrm{Diff}^+(D_n,P))$ are isomorphic. Thus, we have proved that

$$PB_n\cong\mathrm{PMod}(D_n).$$

To complete the proof, consider the short exact sequence

$$1\to\mathrm{PMod}(D_n)\to\mathrm{Mod}(D_n)\to S_n\to 1$$

where S_n is the symmetric group of rank $n-1$. Comparing this exact sequence with (1) and using the Five Lemma, we deduce that

$$\mathrm{Mod}(D_n)\cong B_n.$$

□

We finish this section by introducing generating sets for $\mathrm{Mod}(D_n)$ and $\mathrm{PMod}(D_n)$. Let D_n be a disc with n punctures on its interior. Denote the punctures by $p_1,p_2,...,p_n$

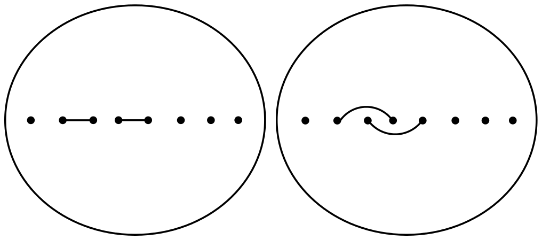


Figure 4.8: The action of σ_3 on D_8.

enumerating from left to right. Consider two arcs connecting the punctures p_{i-1} with p_i and p_{i+1} with p_{i+2} respectively (see Figure 4.8 on the left). Then for $i < n$ let σ_i be the homeomorphism which interchanges the puncture p_i with the puncture p_{i+1} by moving these two punctures by the counterclockwise direction (see Figure 4.8 on the right). The homeomorphism σ_i is called a half twist. In order to check that the σ_i are generators for $\mathrm{Mod}(D_n)$, fix a point $d \in \partial D_n$ and consider $\pi_1(D_n, d)$. But $\pi_1(D_n, d)$ is isomorphic to the free group of n generators F_n. Denote the generators of $\pi_1(D_n, d)$ by γ_i, when $1 \geq i \geq n$. The generators γ_i are loops starting at the point d, go around the puncture i and end up at the point d. The action of σ_i to γ_j is the same action of the automorphism σ_i defined in Subsection 4.1.3. Thus the half twists generate $\mathrm{Mod}(D_n)$.

Recall that the generators of PB_n are the elements $a_{i,j} = \sigma_{j-1}...\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}...\sigma_{j-1}^{-1}$. Consider a closed curve surrounding the points p_i and p_{i+1}. Denote that curve by $c_{i,j}$. One easily checks that $T_{c_{i,i+1}} = \sigma_i^2$ (where $T_{c_{i,i+1}}$ is the Dehn twist about $c_{i,i+1}$). Consider now the curve $c_{i,j}$ surrounding the punctures i and j. Then $a_{i,j} = T_{c_{i,j}}$.

4.2 Hyperelliptic mapping class group

Here we define a proper subgroup of $\mathrm{Mod}(\Sigma_g^b)$, namely, the hyperelliptic mapping class group. We divide the present section in two parts. In the first part we define the hyperelliptic mapping class group of Σ_g, and in the second part we define the hyperelliptic mapping class group of Σ_g^b where $b = 1, 2$.

Surfaces without boundary. We define the *hyperelliptic involution* $\iota \in \mathrm{Mod}(\Sigma_g)$ to be an order 2 element that acts on $\mathrm{H}_1(\Sigma_g, \mathbb{Z})$ as minus the identity. Alternatively, we can consider ι as the mapping class which rotates Σ_g by 180 degrees as indicated on the left hand side of Figure 4.9. We think of Σ_g as a branched cover of the sphere $\mathbb{S}^2$,

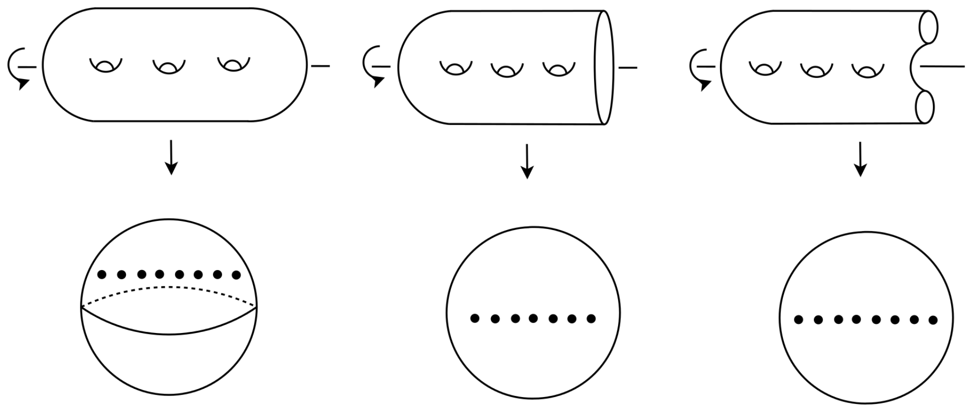


Figure 4.9: Two fold branched cover.

branched at $2g+2$ points

$$\Sigma_g \to \Sigma_g/\iota.$$

The quotient Σ_g/ι is an orbifold sphere with $2g+2$ cone points of order 2. In this thesis we do not need this geometric information about Σ_g/ι, and we consider it as a topological space $\Sigma_{0,2g+2}$, that is, a sphere with $2g+2$ marked points.

Recall the half twists $\sigma_i \in \mathrm{Mod}(\Sigma^1_{0,2g+2})$ described in Section 4.3.1. Consider the surjective homomorphism $\mathrm{Mod}(\Sigma^1_{0,2g+2}) \to \mathrm{Mod}(\Sigma_{0,2g+2})$. We denote by H_i the image of σ_i in $\mathrm{Mod}(\Sigma_{0,2g+2})$. For $1 \leq i \leq 2g+1$, the homeomorphisms H_i are called *half twists*. It is well known, [20, Section 5.1.3], that $\mathrm{Mod}(\Sigma_{0,2g+2})$ is generated by H_i for $1 \leq i \leq 2g+1$ with the following relations:

$$H_i H_{i+1} H_i = H_{i+1} H_i H_{i+1},$$

$$H_i H_j = H_j H_i, \text{ if } |i-j| > 1,$$

$$(H_1 H_2 ... H_{2g+1})^{2g+2} = 1,$$

and

$$H_1 H_2 ... H_{2g+1}^2 ... H_2 H_1 = 1.$$

We denote by $\mathrm{SMod}(\Sigma_g)$ the centralizer of ι in $\mathrm{Mod}(\Sigma_g)$. Birman-Hilden proved the following exact sequence, [10, Theorem 1].

$$1 \to \langle \iota \rangle \to \mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2}) \to 1$$

The group $\mathrm{SMod}(\Sigma_g)$ is called the *hyperelliptic mapping class group* of Σ_g. For $i \leq 2g+1$ let c_i be the curves in Figure 3.4. The map $\mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2})$ in the exact sequence above is defined by $T_{c_i} \mapsto H_i$. Then it is easy to see that $\mathrm{SMod}(\Sigma_g)$ is generated by $T_{c_1}, T_{c_2}, ..., T_{c_{2g+1}}$. Note that we have an expression for the hyperelliptic involution:

$$\iota = T_{c_1} ... T_{c_{2g+1}}^2 ... T_{c_1}.$$

Surfaces with boundary. Consider a hyperelliptic involution ι as described above. For $b = 1, 2$, ι acts on Σ_g^b. Since ι does not fix the boundary components of Σ_g^b pointwise, then $\iota \notin \mathrm{Mod}(\Sigma_g^b)$. As before we have a two fold branched cover $\Sigma_g^b \to \Sigma_g^b/\iota$. Topologically Σ_g^b/ι is homeomorphic to $\Sigma_{0,2g+b}^1$ (see Figure 4.9). We note that if q_1, q_2 denote the boundary components of Σ_g^2, then $\iota(q_1) = q_2$.

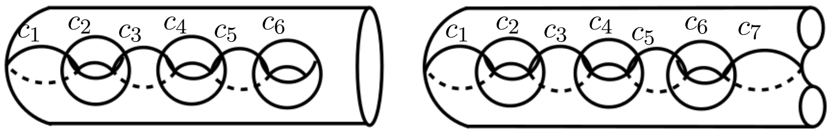


Figure 4.10: Generators of the hyperelliptic mapping class group.

Consider the curves c_i depicted in Figure 4.10, and let σ_i be the generators of B_{2g+b}. We define a map $\xi : B_{2g+b} \to \mathrm{Mod}(\Sigma_g^b)$ by $\xi(\sigma_i) = T_{c_i}$. Since the braid, and the disjointness relations are satisfied by σ_i, and T_{c_i} then ξ is a homomorphism. The image of ξ is called hyperelliptic mapping class group of Σ_g^b, and it is denoted by $\mathrm{SMod}(\Sigma_g^b)$. In fact we have $B_{2g+b} \cong \mathrm{SMod}(\Sigma_g^b)$ [50].

Chapter 5

Hecke algebra representations

In this chapter we define a quotient of the group algebra of the braid group, namely the Hecke algebra. Hecke algebras are important because, for example, we can classify their irreducible representations. Furthermore, we introduce representations of Hecke algebras $H(q,n)$. If q is not a root of unity, it is well known that the set of irreducible representations of $H(q,n)$ is in bijective correspondence with the set of irreducible representations of S_n [26, Theorem 8.1.7]. But irreducible representations of S_n are in bijective correspondence with the Young diagrams. In the first section we define Young diagrams, and we describe how a Young diagram is related to an irreducible representation of $H(q,n)$. The construction of the matrices of the representations is not easy. Wenzl has constructed representations for $H(q,n)$ in the case where q is not a root of unity [57]. As we see in Chapter 6, roots of unity are important, so Wenzl's construction is not sufficient for our purposes in here. In Section 5.2 we will give a different method to construct matrices of the Hecke algebra representations, which are well defined even when q is a root of unity. This method uses the notion of W-graphs introduced by Kazhdan-Lusztig [41]. We note here that if q is a root of unity, we do not always know whether the representations are irreducible or not. In Section 5.3 we relate the constructions of Section 5.2 with Young diagrams. Finally, in Section 5.4 we use Hecke algebra representations to define representations for braid groups.

5.1 Hecke algebras

Let $\mathbb{Z}[q^{\pm 1}]$ be the ring of Laurent polynomials over $\mathbb{Z}$, where q is an indeterminate. Let S_n be the symmetric group, and let S be the set of transpositions $s_i = (i, i+1)$ of S_n. The pair (S_n, S) is called *Coxeter system* of S_n. We denote by $H(q,n)$ the algebra over $\mathbb{Z}[q^{\pm 1}]$, generated by the set $\{T_{s_i} \mid s_i \in S\}$ with relations as follows:

(1) We have that $T_{s_i}T_{s_{i+1}}T_{s_i} = T_{s_{i+1}}T_{s_i}T_{s_{i+1}}$.

(2) If $|i-j|>1$, then $T_{s_i}T_{s_j} = T_{s_j}T_{s_i}$.

(3) For all $s_i \in S$, we have that $T_{s_i}^2 = 1 + (q - q^{-1})T_{s_i}$.

An algebra $H(q,n)$ of this form is called a *Hecke algebra.* Let (S_n, S) be a Coxeter system. Given $w \in S_n$, we can write $w = s_{j_1}s_{j_2} \ldots s_{j_p}$, where $s_{j_k} \in S$. If p is minimal, we say that this is a *reduced expression* for w; then $l(w) = p$ is called the *length of* w. If $l(w) = p$ then we define $T_w = T_{s_{j_1}}T_{s_{j_2}} \ldots T_{s_{j_p}}$. The element T_w is independent of the choice of the reduced expression for w. It turns out that the multiplication rule is the following [26, Lemma 4.4.3]:

$$T_{s_i}T_w = \begin{cases} T_{s_iw}, & \text{if } l(s_iw) > l(w), \\ T_{s_iw} + (q-q^{-1})T_w, & \text{if } l(s_iw) < l(w). \end{cases}$$

Furthermore, $H(q,n)$ admits a basis $\{T_w \mid w \in S_n\}$ [26, Theorem 4.4.6].

We can easily check that $T_{s_i}^{-1} = T_{s_1} - (q - q^{-1})$. The map $\psi : B_n \to H(q,n)$, defined by $\psi(\sigma_i) = T_{s_i}$, is a well defined homomorphism from B_n to the group of units of $H(q,n)$. Similarly, if $q = 1$ then we have a well defined homomorphism $\phi : S_n \to H(1,n)$ defined by $\phi(s_i) = T_{s_i}$. We can think of $H(q,n)$ as a quotient of the group algebra of B_n and $H(1,n)$ as the group algebra of S_n.

5.2 Young diagrams

A *Young diagram* $\lambda = [\mu_1, \mu_2, ..., \mu_k]$ is an array of n boxes with μ_i boxes in the i^{th} row, $\mu_i \geq \mu_{i+1}$, and $\sum \mu_i = n$. We denote by Λ_n the set of all Young diagrams with n boxes. Consider a Young diagram $\lambda \in \Lambda_n$. A *standard tableau* of λ is obtained by filling the boxes of λ with integers between 1 and n, such that the integers are strictly increasing from left to right and from top to bottom, and every box contains exactly one number. An example is given in Figure 5.1. We denote by Y_λ the set of all standard tableaux of λ. For each Y_λ, there is an irreducible representation of S_n. The dimension of the representation of the symmetric group S_n associated to $\lambda \in Y_\lambda$ is equal to the dimension of the representation of the Hecke algebra $H(q,n)$ [38, Section 4].

Let V_λ be a free $\mathbb{Z}[q^{\pm 1}]$-module with basis $\{u_t, \mid t \in Y_\lambda\}$. The irreducible representation associated to the Young diagram λ is denoted by $\pi_\lambda : H(q,n) \to \mathrm{End}(V_\lambda)$. We describe how such an irreducible representation decomposes when it is restricted to $H(q,n-1) \subset H(q,n)$. A *Young's lattice* is a diagram formed by Young diagrams, such

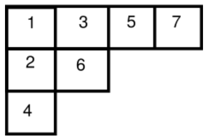


Figure 5.1: Example of a standard tableau.

that each Young diagram is connected by an edge to another one if they differ by one box. Consider, for example, the Young's lattice indicated in Figure 5.2.

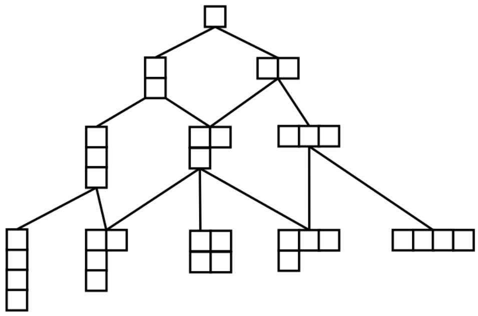


Figure 5.2: Young's lattice up to 4 boxes.

Let $\lambda \in \Lambda_n$ be a diagram which is connected by edges to diagrams $\lambda_1, ..., \lambda_m$ such that $\lambda_i \in \Lambda_{n-1}$ for $i = 1, 2, ..., m$. The restriction of the irreducible representation $\pi_\lambda : H(q, n) \to \mathrm{End}(V_\lambda)$ to $H(q, n-1)$ is as follows [38, Section 4]:

$$\bigoplus_{i=1}^{m} \pi_{\lambda_i} : H(q, n-1) \to \bigoplus_{i=1}^{m} \mathrm{End}(V_{\lambda_i}).$$

The restriction formula above is called the *branching rule*. The dimension of the representation of $H(q, n)$ associated to $\lambda \in \Lambda_n$ is equal to the number of the descending paths from $\square$ to λ, which is equal to the cardinality of Y_λ. In order to compute the cardinality of Y_λ we need the notion of the hook length [22, Theorem 1]. The *hook length*, denoted by $hook(x)$, of a box x in λ is the number of boxes that are in the same row to the right of it plus those boxes in the same column below it, plus one. For example consider the Young diagram of Figure 5.3, where in each box we have assigned its hook length. The cardinality of Y_λ is equal to

$$|Y_\lambda| = \frac{n!}{\prod\limits_{x \in \lambda} hook(x)}.$$

For the diagram λ of Figure 5.3, we have $|Y_\lambda| = 68640$.

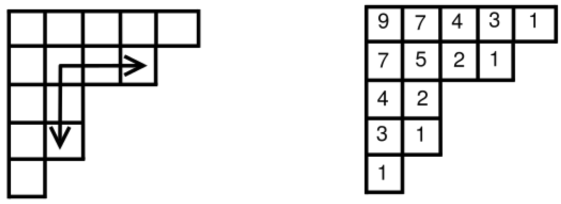


Figure 5.3: The hook length of every box in the Young diagram.

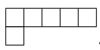
5.3 The Burau representation

We will give an example of a Hecke algebra irreducible representation, namely the reduced Burau representation. We will treat the Burau representation in detail in Chapter 7. For $n > 2$ the *reduced Burau representation* $\beta_t : B_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[t^{\pm 1}])$ is determined by the matrices

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

and for $1 < i < n-1$,

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

A direct calculation shows that $(-\beta_t(\sigma_i))^2 = (t-1)(-\beta_t(\sigma_i)) + t$. This relation was first observed by Jones [38, Note 5.7]. For $q^2 = t$, the matrices $(-q^{-1}\beta_{q^2}(\sigma_i))$ satisfy the quadratic relation of $H(q, n)$. Since the Burau representation is irreducible and satisfies the quadratic relation, one can check that $(-q^{-1}\beta_{q^2}(\sigma_i)) = \pi_\lambda(\sigma_i)$, where λ is the Young diagram .

5.4 Kazhdan-Lusztig's construction

In this section we provide a tool to explicitly construct matrices of representations of the Hecke algebra $H(q, n)$. In fact, we define a $\mathbb{Z}[q^{\pm 1}]$-module E and an action of $H(q, n)$ on E. A W-graph encodes the structure of a $\mathbb{Z}[q^{\pm 1}]$-module in the sense that its vertices correspond to a basis for E, and the edges provide all the information we need for the action of $H(q, n)$ on E. First we give a new basis for $H(q, n)$; as before each basis element is associated to an element of the symmetric group S_n. Then we define an equivalence relation on elements of S_n. The equivalence classes are called cells. Vertices of a W-graph correspond to elements of a fixed cell. We define an action of generators of $H(q,n)$ on the basis of E. This action extends to a representation $H(q,n) \to \mathrm{End}(E)$ [41].

Definition of W-graphs. Let (S_n, S) be the Coxeter system for the symmetric group introduced in the previous section. A *W-graph* is defined to be a set of vertices X and a set of edges Y together with the following data. For each vertex $x \in X$, we are given a subset $I_x \subset S$, and for each ordered pair of vertices (y,w) with $\{y,w\} \in Y$, we are given an integer $\mu(y,w)$, subject to the requirements in the following paragraph.

Let E be the free $\mathbb{Z}[q^{\pm 1}]$-module with basis associated to the vertex set X. Recall that s_i is the transposition $(i, i+1)$ in S_n. For any $s_i \in S$ and for any $w \in X$ (considering X as a basis for E) we define the map τ_{s_i} as follows:

$$\tau_{s_i} w = \begin{cases} -q^{-1} w, & \text{if } s_i \in I_w, \\ qw + \sum \mu(y,w) y, & \text{if } s_i \notin I_w, \end{cases}$$

where the sum is taken over all $y \in X, s_i \in I_y$ such that $\{y,w\} \in Y$. Extending linearly, we get an endomorphism of E. For $i < n-2$, we require that

$$\tau_{s_i} \tau_{s_{i+1}} \tau_{s_i} = \tau_{s_{i+1}} \tau_{s_i} \tau_{s_{i+1}}$$

and for $|i - j| > 1$

$$\tau_{s_i} \tau_{s_j} = \tau_{s_j} \tau_{s_i}.$$

In other words, we require that the endomorphisms τ_{s_i} satisfy the usual relations in the braid group. We note that Kazhdan-Lusztig defined W-graphs for any Coxeter system.

Example 1. We give an example of a W-graph for the group S_3 in Figure 5.4. We label the vertices of the W-graph by the elements of the set $X = \{s_1, s_2 s_1\}$. We let $I_{s_1} = \{s_1\}$, $I_{s_2 s_1} = \{s_2\}$ and the integers $\mu(s_1, s_2 s_1) = 1$, $\mu(s_2 s_1, s_1) = 0$. Furthermore, we have

$$\begin{array}{rcl} \tau_{s_1}(s_1) & = & -q^{-1} s_1, \\ \tau_{s_1}(s_2 s_1) & = & q s_2 s_1 + s_1, \\ \tau_{s_2}(s_1) & = & q s_1 + s_2 s_1, \\ \tau_{s_2}(s_2 s_1) & = & -q^{-1} s_2 s_1. \end{array}$$

The matrices of the representation are as follows:

$$T_{s_1} \mapsto \begin{pmatrix} -q^{-1} & 1 \\ 0 & q \end{pmatrix}, \quad T_{s_2} \mapsto \begin{pmatrix} q & 0 \\ 1 & -q^{-1} \end{pmatrix}.$$

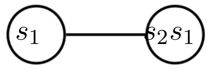


Figure 5.4: Example of a W-graph.

We note that in the literature the vertices of W-graphs are often labeled by I_w where $w \in S_n$.

The endomorphism τ_{s_i} satisfies the quadratic relation $(\tau_{s_i} + q^{-1})(\tau_{s_i} - q) = 0$. To see this consider $w \in S_n$ such that $s_i \in I_w$. Then we have:

$$(\tau_{s_i} + q^{-1})(\tau_{s_i} - q)(w) = (\tau_{s_i} + q^{-1})(-q^{-1}w - qw) = q^{-2}w + w - q^{-2}w - w = 0.$$

On the other hand, if $s_i \notin I_w$, then we have:

$$\begin{aligned}(\tau_{s_i} + q^{-1})(\tau_{s_i} - q)(w) &= (\tau_{s_i} + q^{-1})(qw + \sum \mu(y,w)y - qw) \\ &= \sum \mu(y,w)\tau_{s_i}(y) + q^{-1} \sum \mu(y,w)y \\ &= -q^{-1} \sum (y,w)y + q^{-1} \sum \mu(y,w)y \\ &= 0\end{aligned}$$

By the second condition of the definition of W-graphs and since the endomorphism τ_{s_i} satisfies the quadratic relation, the map $T_{s_i} \mapsto \tau_{s_i}$ extends to a representation of the Hecke algebra $H(q,n)$.

The Kazhdan-Lusztig basis. Let $a \to \overline{a}$ be the involution on the ring $\mathbb{Z}[q^{\pm 1}]$, defined by $\overline{q} = q^{-1}$. We extend this to an involution on $H(q,n)$ by the formula

$$\overline{\sum a_w T_w} = \sum \overline{a} T^{-1}_{w^{-1}}.$$

We consider the set of generators S of S_n, and the length function $l : S_n \to \mathbb{Z}$ described in Section 2. We denote by $\leqq$ the Bruhat order on the set of all words in the generating set S, that is, $y \leqq x$ if y is subword of x.

We have the following theorem of Kazhdan-Lusztig [41, Theorem 1] reformulated by Yin [58, Theorem 1.4]:

Theorem 5.1 (Kazhdan-Lusztig). *For any $w \in S_n$, there is a unique element $C_w \in H(q,n)$ such that $\overline{C_w} = C_w$, where*

$$C_w = \sum_{y \leqq w} (-q)^{l(w)-l(y)} \overline{P_{y,w}(q^2)} T_y$$

and $P_{y,w}$ is a polynomial of degree at most $\frac{1}{2}(l(w) - l(y) - 1)$ if $y < w$, and $P_{w,w} = 1$.

The polynomial $P_{y,w}$ is known as the *Kazhdan-Lusztig polynomial*, and Theorem 5.1 proves the existence and uniqueness of $P_{y,w}$. The Kazhdan-Lusztig polynomial is difficult to construct explicitly and we do not give details of the construction in here. A recursive formula for the computation of the Kazhdan-Lusztig polynomial can be found in the original paper [41, Equation 2.2c].

We show by induction on $l(w)$ that T_w can be expressed as a linear combination of elements of $\{C_x \mid x \in S_n\}$. We have that $C_1 = T_1$ and $C_{s_i} = T_{s_i} - qT_1$, where 1 stands for the trivial element of S_n, and s_i is the transposition $(i, i+1)$ in S. For an arbitrary $w \in S_n$ we have

$$C_w = (\sum_{y<w} (-q)^{l(w)-l(y)} \overline{P_{y,w}(q^2)} T_y) + T_w.$$

Since $l(y) < l(w)$, by the inductive hypothesis we have that T_y can be expressed as a linear combination of C_x, for elements $x \in S_n$ with $l(x) < l(w)$. Furthermore, since the cardinality of $\{C_x \mid x \in S_n\}$ is equal to the cardinality of $\{T_x \mid x \in S_n\}$, then the set $\{C_x \mid x \in S_n\}$ forms a basis for $H(q,n)$.

Construction of W-graphs. Consider $y, w \in S_n$. We say that $y \prec w$ if $y < w$, $(-1)^{l(y)} = -(-1)^{l(w)}$, and the Kazhdan-Lusztig polynomial $P_{y,w}$ has degree exactly $\frac{1}{2}(l(w) - l(y) - 1)$. We take $\mu(y,w)$ to be the coefficient of the highest power of q in $P_{y,w}$. Let Γ be the graph whose vertices X correspond to the $n!$ elements of S_n and whose edges are subsets of S_n of the form $\{y, w\}$ with $y \prec w$. We set $I_w = \{s_i \in S \mid s_i w < w\}$. We define a preorder relation $\leqq_\Gamma$ on the set of vertices of Γ as follows. Two vertices x, x' satisfy $x \leqq_\Gamma x'$ if there exist a sequence of vertices $x = x_0, x_1, ..., x_n = x'$ such that for each i, $(1 \leq i \leq n)$, $\{x_{i-1}, x_i\}$ is an edge and $I_{x_{i-1}} \nsubseteq I_{x_i}$. Define the equivalence relation $x \sim_\Gamma x'$ if $x \leqq_\Gamma x' \leqq_\Gamma x$. The equivalence classes of S_n under $\sim_\Gamma$, denoted by $[w]$, are called *cells*. We denote by $\Gamma_{[w]}$ the subgraph of Γ whose vertices correspond to elements of $[w]$. Now we can define the action of T_{s_i} on $\{C_w \mid w \in S_n\}$:

$$T_{s_i} C_w = qC_w + C_{s_i w} + \sum_{y \prec w, s_i y < y} \mu(y,w) C_y.$$

This action above is well defined [58, Theorem 2.5].

Let D_w be the $\mathbb{Z}[q^{\pm 1}]$-module spanned by the set $\{C_y \mid y \leqq_\Gamma w\}$, and let D'_w be the $\mathbb{Z}[q^{\pm 1}]$-module spanned by the set $\{C_y \mid y \leqq_\Gamma w, y \notin [w]\}$. It is obvious that D'_w is contained in D_w. We show that D_w and D'_w are left-ideals of $H(q,n)$. Recall the formula

$$T_{s_i}C_w = qC_w + C_{s_iw} + \sum_{y \prec w, s_iy<y} \mu(y,w)C_y.$$

The conditions $y \prec w, s_iy < y$ together with the existence of $\mu(y,w)$ show that $y \leqq_\Gamma w$. Furthermore $s_iw \leqq_\Gamma w$ since $w \prec s_iw$ (in particular, we have $P_{w,s_iw} = 1$ [41, Lemma 2.6 (iii)]), and $I_w \nsubseteq I_{s_iw}$. Hence, we can define the quotient D_w/D'_w. Thus, we have the following theorem [58, Theorem 2.6]:

Theorem 5.2. *The graph $\Gamma_{[w]}$ defined above is a W-graph whose associated $\mathbb{Z}[q^{\pm 1}]$-module is D_w/D'_w.*

By the theorem above we have a well defined representation

$$\rho : H(q,n) \to \mathrm{End}(D_w/D'_w),$$

where the elements in the basis of D_w/D'_w correspond to the elements of the cell $[w]$. Kazhdan-Lusztig proved that the representation of $H(q,n)$, arising from the action on cells is irreducible and that the isomorphism class of the W-graph depends only on ρ and not on $[w]$ [41, Theorem 1.4].

Example of Figure 5.4. We have already seen that $s_2s_1 \leqq_\Gamma s_1$. By denoting the trivial element of S_n by 1, we have that $1 \prec s_1$ with $s_1 \leqq_\Gamma 1$. Then we have $1 \prec s_1s_2s_1$ with $1 \leqq_\Gamma s_1s_2s_1$. Finally, $s_1s_2s_1 \leqq_\Gamma s_2s_1$. Hence, $s_1 \sim_\Gamma s_2s_1$; the vertex set $\{s_1, s_2s_1\}$ is labeled by $\mu(s_1, s_2s_1) = 1$ [41, Theorem 2.6].

5.5 Robinson-Schensted correspondence and dual Knuth equivalence

In this section we give an algorithm to find elements of a fixed cell. Unfortunately, the construction of cells given by Kazhdan-Lusztig [41] is not easy when n is large. Therefore, we provide a different strategy to obtain cells. We have two tools: the Robinson-Schensted correspondence (RS-correspondence) and the dual Knuth equivalence. Using the RS-correspondence, we are able to decide when two elements of S_n belong to the same cell. Also, we are able to calculate the cardinality of a cell, that is, the dimension of the representation associated to that cell. By the dual Knuth equivalence, given an element $w \in S_n$ we can obtain all elements of $[w]$. That is, by taking any $w \in S_n$, we find all $y \in S_n$ such that $w \sim_\Gamma y$.

Robinson-Schensted correspondence. Here we give an algorithm that associates elements of S_n with Young diagrams. More particularly, in this algorithm every element of S_n corresponds to two standard tableaux of the same shape.

For $w \in S_n$, let w_i denote the image of $w(i)$ under the mapping $w : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$. We identify w with the sequence $w_1 w_2 ... w_n$. Consider an arbitrary tableaux T. We denote the boxes of the ith row by $R_i(T)$. In the first step the row $R_1(T)$ contains a box filled by w_1. In the next steps if w_j is greater than every number in $R_i(T)$, then we add a box on the right of all other boxes filled by w_j. If w_j is not greater than every number of $R_i(T)$, we consider $k \in R_i(T)$ such that k is the smallest number for which $w_j < k$. We replace k by w_j. If $R_{i+1}(T)$ does not exist, we add a box in $R_{i+1}(T)$ filled by k. If not, we repeat the same process with k playing the role of w_j in the $R_{i+1}(T)$ row. The algorithm ends when we insert all w_j in the boxes of T. The algorithm we described is called the *row insertion algorithm.* The standard diagram we obtain is denoted by $P(w)$, and it is called the *P-symbol.* We define the *Q-symbol* to be $Q(w) = P(w^{-1})$. For example, in S_3 consider the element $s_1 s_2 = 231$, where $s_i \in S$ are transpositions. In Figure 5.5 we compute the P-symbol of $s_1 s_2$ step by step.

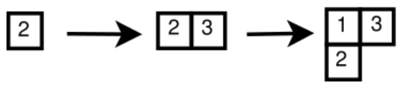


Figure 5.5: The P-symbol of $s_1 s_2$.

The pair $(P(w), Q(w))$ is called the *Robinson-Schensted correspondence.* There is a bijection between the elements of S_n and the pairs $(P(w), Q(w))$ for all $w \in S_n$. For the proof of Theorem 5.3, see [3, Theorem A].

Theorem 5.3. *For $y, w \in S_n$, we have $y \sim_\Gamma w$ if and only if $Q(y) = Q(w)$.*

As we have seen in the previous section, Kashdan-Luzstig proved that the action of $H(q, n)$ on cells induces irreducible representations. But there is no clear connection between cells and Young diagrams. The latter connection is summarized in the following theorem [8, Theorems 6.5.2, 6.5.3]. For a fixed $x \in S_n$, we denote the shape of $Q(x)$ by $S(Q(x))$.

Theorem 5.4. *An irreducible representation of $H(q, n)$ associated with the cell $[w]$, for a fixed $w \in S_n$, is labeled by a Young diagram λ, where $\lambda = S(Q(w))$.*

Dual Knuth equivalence. Here we provide an algorithm to find all elements of a cell. That is, starting with an element of S_n, we have a process that allows us to obtain elements of the cell associated with a given element of S_n.

For $x, y \in S_n$, we write $x \sim_{dK} y$ (x is dual Knuth equivalent to y) if x and y differ by transposition of two values i and $i+1$, and either $i-1$ or $i+2$ occurs in a position between those of i and $i+1$. For example,

$$215436 \sim_{dK} 315426 \sim_{dK} 415326 \sim_{dK} 425316$$

shows that $215436 \sim_{dK} 425316$. Thus, we have the following result [8, Fact A3.6.2].

Theorem 5.5. *For $x, y \in S_n$, we have that $Q(x) = Q(y)$ if and only if $x \sim_{dK} y$.*

The algorithm for construction of a cell is divided into 2 steps.

1. Fix an element w of S_n. By Theorem 5.4 we obtain the cardinality of $[w]$.
2. By the dual Knuth equivalence, we obtain all elements of $[w]$. For any $x \in [w]$ we deduce $I_x = \{s_i \in S \mid s_i x < x\}$.

5.6 Facts about the Hecke algebra representation

In the previous chapter we have seen that a Hecke algebra $H(q, n)$ is a quotient of the group algebra of B_n. Hence, every representation of $H(q, n)$ gives a representation of B_n. Our aim here is to define representations of B_n that factor through $H(q, n)$ and examine some of their properties.

We fix an element $w \in S_n$. Let $H(q, n) \to \mathrm{End}(V)$ be a Hecke algebra representation, where V is the $\mathbb{Z}[q^{\pm 1}]$-module spanned by C_x for all $x \in [w]$ as described in Section 5.2. Since $H(q, n)$ is a quotient of the group algebra of B_n, there is a well defined representation $\pi_\lambda : B_n \to \mathrm{End}(V)$. Furthermore, λ is the shape of the standard diagram of $Q(w)$.

Representations when the Young diagram is rectangular. We now focus on representations of B_{2g+2} when $g \geq 2$ and λ is a rectangular diagram. For $g \geq 2$ we want to construct a representation $\pi_\lambda : B_{2g+2} \to \mathrm{End}(V_\lambda)$ such that the matrices in the image of π_λ follow a pattern when the g increases. First we want to find cells that correspond to rectangular diagrams. Consider, for example, $w \in S_6$ such that $[w]$ is a cell associated to a rectangular diagram. Furthermore, w is an element of S_8. But by the RS-correspondence we can see that $[w]$ in S_8 does not always correspond to a rectangular diagram.

We can solve this problem by making appropriate choices for cells. Denote the generators of S_{2g+2} by the transpositions s_i, $i < 2g+2$, and consider the element $s_1 s_3 s_5 ... s_{2g+1} \in S_{2g+2}$. Recall from Section 3.3 that for $x \in S_n$, $Q(x)$ is the Q-symbol. By the RS-correspondence it is easy to check that the shape of $Q(s_1 s_3 s_5 ... s_{2g+1})$, denoted by λ_{2g+2}, is rectangle as indicated in Figure 5.6 for $g = 5$.

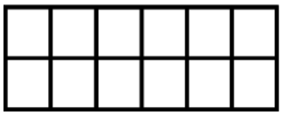


Figure 5.6: The Young diagram of the cell $[s_1 s_3 s_5 ... s_{11}]$.

For $g \geq 2$, we consider the cells $[s_1 s_3 s_5] = W_1$ and $[s_1 s_3 s_5 ... s_{2g+1}] = W_2$. The cell $[s_1 s_3 s_5]$ contains the elements

$$\{s_1 s_3 s_5, s_1 s_4 s_3 s_5, s_2 s_1 s_3 s_5, s_2 s_1 s_4 s_3 s_5, s_3 s_2 s_1 s_4 s_3 s_5\}.$$

For $g = 3$ the cell $[s_1 s_3 s_5 s_7]$ contains the elements

$$\{s_1 s_3 s_5 s_7, s_1 s_4 s_3 s_5 s_7, s_2 s_1 s_3 s_5 s_7, s_2 s_1 s_4 s_3 s_5 s_7, s_3 s_2 s_1 s_4 s_3 s_5 s_7,$$

$$s_1 s_3 s_6 s_5 s_7, s_1 s_5 s_4 s_3 s_6 s_5 s_7, s_2 s_1 s_4 s_3 s_6 s_5 s_7, s_2 s_1 s_5 s_4 s_3 s_6 s_5 s_7, , s_2 s_1 s_3 s_6 s_5 s_7$$

$$s_1 s_4 s_3 s_6 s_5 s_7, s_3 s_2 s_1 s_4 s_3 s_6 s_5 s_7, s_3 s_2 s_1 s_5 s_4 s_3 s_6 s_5 s_7, s_4 s_3 s_2 s_1 s_5 s_4 s_3 s_6 s_5 s_7\}.$$

The first five elements of $[s_1 s_3 s_5 s_7]$ above differ from the elements of $[s_1 s_3 s_5]$ by the generator s_7. For $g > 3$ the first five elements of $[s_1 s_3 s_5 ... s_{2g+1}]$ differ from $[s_1 s_3 s_5]$ by the word $s_7 s_9 ... s_{2g+1}$.

Recall from Section 2 the correspondence $\sigma_i \mapsto T_{s_i}$ where T_{s_i} is a generator of $H(q, n)$. We have the following theorem.

Theorem 5.6. *The map $C_w \mapsto C_{w s_7 s_9 ... s_{2g+1}}$ for $w \in W_1$ and $w s_7 s_9 ... s_{2g+1} \in W_2$ defines an embedding for $H(q, 6)$-modules $V_{\lambda_6} \hookrightarrow V_{\lambda_{2g+2}}|_{H(q,6)}$.*

In other words, we get a representation $B_{2g+2} \to \mathrm{End}(V_{\lambda_{2g+2}})$, such that

$$\sigma_i \mapsto \pi_{\lambda_{2g+2}}(\sigma_i) = \begin{pmatrix} \pi_{\lambda_6}(\sigma_i) & A \\ 0 & B \end{pmatrix},$$

where $\pi_{\lambda_6}(\sigma_i)$ is a 5×5 matrix, d is the dimension of $\pi_{\lambda_{2g+2}}(\sigma_i)$, A is a matrix of dimension $5 \times (d-5)$, and B is a matrix of dimension $(d-5) \times (d-5)$.

Proof. We denote the elements of W_1 by u_1, u_2, u_3, u_4, u_5. Then the first five elements of W_2 have the form $u_i s_7 s_9 ... s_{2g+1} = w_i$, where $i \leq 5$. Recall from Section 3.2 that the action of T_{s_j} on C_{w_i} is defined as follows:

$$T_{s_j} C_{w_i} = q C_{w_i} + C_{s_j w_i} + \sum_{y \prec w_i, s_j y < y} \mu(y, w_i) C_y.$$

We divide the proof into two steps. In the first step we show that the basis elements C_x, for $x \in W_2$ in the above sum are the same for any $g \geq 2$. In the second step we show that $\mu(y', w_i) = \mu(y, u_i)$ for $y' \prec w_i, s_j y' < y'$, $y \prec u_i$, $s_j y < y$, and y, y' differ by the word $s_7 s_9 \ ... \ s_{2g+1}$.

Step 1. By Theorem 5.2 if $s_j w_i < w_i$, then $T_{s_j} C_{w_i} = -q^{-1} C_{w_i}$; if $s_j w_i > w_i$ then the element $C_{s_j w_i}$ vanishes in $V_{\lambda_{2g+2}}$ (the $\mathbb{Z}[q^{\pm 1}]$-module spanned by C_x for all $x \in W_2$).

We show that if $y \prec w_i, s_j y < y$, then y is one of the first five elements in W_2. By considering a weaker restriction $y \leqq w_i$, we show that either $y \notin W_2$ or y is one of w_i. We can see that the argument of the first step is true for $g = 2$ and 3 (see the examples of cells above). If $g \geq 4$, we note that u_i differ from w_i by the word $s_7 s_9 ... s_{2g+1}$, and every u_i is a word in $\{s_j \mid j \leq 5\}$. Therefore, by the RS-correspondence for $y \in S_{2g+2}$ such that $y \leqq w_i$, we have that either $y \notin W_2$ or y is one of w_i.

Step 2. If $k = 1$ and $i = 5$ do not occur simultaneously, then $\mu(w_k, w_i) = \mu(u_k, u_i) = 1$ since $l(w_i) - l(w_k) \leq 2$ [41, Theorem 2.6], where $l : S_{2g+2} \to \mathbb{Z}$ is the length function defined in Section 2. It remains to prove that $\mu(w_1, w_5) = \mu(u_1, u_5) = 1$. We compute the polynomial P_{w_1,w_5}. We know that $\deg(P_{w_1,w_5}) = \frac{l(w_2) - l(w_1) - 1}{2} = 1$. Therefore, $P_{w_1,w_2} = \mu(w_1, w_2) q + 1$. By the recursive formula given by Kazhdan-Lusztig [41, 2.2c] we have that

$$P_{w_1,w_5} = P_{s_3 w_1, s_3 w_5} + q P_{w_1, s_3 w_5} - \sum \mu(z, s_3 w_5) q P_{w_1,z},$$

where the sum is over all z such that $w_1 \leqq z \prec s_3w_5$, $s_3z < z$. But since we have $P_{w_1,s_3w_5} = \mu(z, s_3w_5) = P_{w_1,z} = 1$, [41, theorem 2.6] we conclude

$$P_{w_1,w_5} = P_{s_3w_1,s_3w_5} + q - \sum q.$$

Furthermore, by the RS-correspondence we can easily check that the elements s_3w_1 and s_3w_5 are not equivalent, which implies that the degree of $P_{s_3w_1,s_3w_5}$ is strictly less than 1. Hence, $P_{s_3w_1,s_3w_5} = 1$. Finally, the Kazhdan-Lusztig polynomials have non-negative integer coefficients [19, Corollary 1.2]. Therefore $P_{w_1,w_5} = q + 1$, and we have deduced that $\mu(w_1, w_5) = \mu(u_1, u_5) = 1$. □

Theorem 5.6 gives a nice description of the modules W_2. It would be an interesting result for the future to identify the matrices A, B.

Chapter 6

Normal closures of powers of twists

In the previous chapter we studied the irreducible representations of braid groups that factor through the Hecke algebras and we examined some properties of these representations. In this chapter we use the Hecke algebra representations to construct representations for mapping class groups of punctured spheres and we examine the structure of the latter groups.

6.1 Constructed a representations of mapping class group of a punctured sphere

For $i = 1, 2, ..., 2g+1$, let σ_i be the generators of B_{2g+2}, and let H_i be the generators of $\mathrm{Mod}(\Sigma_{0,2g+2})$ as in Section 2. Since the homomorphism $B_{2g+2} \to \mathrm{Mod}(\Sigma_{0,2g+2})$ is surjective, it is reasonable to ask whether we can define a linear representation of $\mathrm{Mod}(\Sigma_{0,2g+2})$ via the Hecke algebra $H(q, 2g+2)$. An affirmative answer was given by Jones [38, Theorem 10.2]. Since we use a different definition of $H(q, n)$ than Jones, we reformulate his representation. But first we need to prove two lemmas. Those lemmas hold for the braid group B_n for any $n \geq 2$. After we prove the lemmas, we will concentrate in the case where $n = 2g+2$.

Let f_i be the image of σ_i in $\mathrm{End}(V)$, and for $q^2 \neq -1$ we set $e_i = (q - f_i)/(q + q^{-1})$. In this section we examine certain properties of the representation of the braid group $\pi_\lambda : B_n \to \mathrm{End}(V)$. Firstly, we calculate the image of the center of B_n under the map π_λ in Lemmas 6.1 and 6.2.

Lemma 6.1. *The element e_i satisfies $e_i^2 = e_i$ for all $i = 1, 2, ..., n-1$. The rank of the* *idempotent e_i is the number of descending paths from the diagram $\lambda_0 = \begin{smallmatrix}\square\\ \square\end{smallmatrix}$ to the diagram λ of Young's lattice described in Section 5.1.*

Proof. We can easily check that $e_i^2 = e_i$. Also, it is easy to check that the rank of an idempotent in $\mathrm{End}(V)$ is equal to its trace. Since all generators of B_n are conjugate in B_n, then all e_i have the same rank (trace). It suffices to calculate the rank of e_1. We have that $\pi_{\lambda_0}(\sigma_1) = -q^{-1}$. Thus, $\pi_{\lambda_0}(e_1) = 1$. We prove the lemma by induction. We restrict the representation of B_n to B_{n-1}. Then the image of σ_1 in $\mathrm{End}(V)$ is $\bigoplus \pi_{\lambda_i}(\sigma_1)$, where the sum is taken over all λ_i that are connected by an edge in the Young's lattice. By the induction argument the rank of $\pi_{\lambda_i}(\sigma_1)$ is the number of paths from λ_0 to λ_i. Since the rank of $\pi_\lambda(\sigma_1)$ is the sum of ranks of $\pi_{\lambda_i}(\sigma_1)$, we conclude that the rank is equal to the number of paths from the diagram λ_0 to the diagram λ. □

The center of the braid group B_n is generated by $(\sigma_1 ... \sigma_{n-1})^n$ [20, Section 9.2]. We use Lemma 6.2 to explicitly compute the image of the homomorphism π_λ for every Young diagram λ.

Lemma 6.2. *If* $\dim(\pi_\lambda) = d$ *and* $\mathrm{rank}(e_i) = r$*, then*

$$\pi_\lambda((\sigma_1\sigma_2 ... \sigma_{n-1})^n) = q^{n(n-1)\frac{d-2r}{d}} Id_{\pi_\lambda}.$$

Proof. The element $(\sigma_1\sigma_2 ... \sigma_{n-1})^n$ is in the center of B_n; thus, $\pi_\lambda((\sigma_1\sigma_2 ... \sigma_{n-1})^n)$ is a diagonal matrix whose entries are all equal. We can evaluate the determinant as follows:

$$\det(\pi_\lambda(\sigma_i)) = \det(f_i) = \det(q - qe_i - q^{-1}e_i) = \det(q)\det(1 - e_i - q^{-2}e_i) = (-1)^r q^{d-2r}.$$

It follows that $\det(\pi_\lambda((\sigma_1\sigma_2 ... \sigma_{n-1})^n)) = q^{n(n-1)(d-2r)}$. Hence,

$$\pi_\lambda((\sigma_1\sigma_2 ... \sigma_{n-1})^n) = \omega q^{n(n-1)\frac{d-2r}{d}}$$

for some d^{th} root of unity ω. But ω depends continuously on q, so if we put $q = 1$, then we obtain a representation for the symmetric group S_n. Since the center of S_n is trivial, we deduce that $\omega = Id_{\pi_\lambda}$. □

Remark. For a rectangular Young diagram λ_{2g+2} as in Theorem 5.6, the dimension of the associated representation is equal to

$$\binom{2g+2}{g+1}\frac{1}{g+2}.$$

Furthermore, according to Lemma 6.1 the rank of the idempotent e_i is equal to the number of the descending paths from $\begin{smallmatrix}\square\\\square\end{smallmatrix}$ to λ_{2g+2} of the Young's lattice. But the latter is equal to the number of the descending paths from $\square$ to λ_{2g}, which is equal to

$$\binom{2g}{g}\frac{1}{g+1}.$$

Below, we use Lemmas 6.1 and 6.2 to construct a representation for $\mathrm{Mod}(\Sigma_{0,2g+2})$.

Proposition 6.3. *Consider the representation $\pi_\lambda : B_{2g+2} \to \mathrm{End}(V_\lambda)$ associated to the Young diagram λ. We set $\pi'_\lambda(\sigma_i) = q^{(2r-d)/d}\pi_\lambda(\sigma_i)$. Then the map*

$$J : \mathrm{Mod}(\Sigma_{0,2g+2}) \to \mathrm{End}(V_\lambda)$$

defines a representation via $J(H_i) = \pi'_\lambda(\sigma_i)$ if and only if λ is rectangular.

We note that the homomorphism $J : \mathrm{Mod}(\Sigma_{0,2g+2}) \to \mathrm{End}(V_\lambda)$ of Proposition 6.3 is known as the *Jones representation.*

Proof. We show that the elements $\pi'_\lambda(\sigma_i)$ satisfy the relations of $\mathrm{Mod}(\Sigma_{0,2g+2})$ defined in Section 2. First, we assume that λ is rectangular. The braid relation and the disjointness relation are satisfied for $\pi'_\lambda(\sigma_i)$. By Lemma 6.2 we have that $\pi'_\lambda((\sigma_1\sigma_2...\sigma_{2g+1})^{2g+2})$ is trivial. We note that in the braid group we have the relation

$$\sigma_1\sigma_2...\sigma_{2g+1}^2\sigma_{2g}...\sigma_1 = (\sigma_1\sigma_2...\sigma_{2g+1})^{2g+2}(\sigma_2...\sigma_{2g+1})^{-(2g+1)}.$$

The condition $\pi'_\lambda(\sigma_1\sigma_2...\sigma_{2g+1}^2\sigma_{2g}...\sigma_1) = 1$ is equivalent to $\pi'_\lambda((\sigma_2...\sigma_{2g+1})^{2g+1}) = 1$, since we already have that $\pi'_\lambda((\sigma_1\sigma_2...\sigma_{2g+1})^{2g+2})$ is trivial. But the restriction $\pi'_\lambda|_{B_{2g+1}}$ when λ is rectangular, satisfies the relation $\pi'_\lambda(\sigma_2...\sigma_{2g+1})^{2g+1} = 1$. We note that by Young's lattice, the dimension d and the rank r after the restriction above do not change. This proves the 'if' part.

Now we prove the other direction. If λ is not rectangular then π'_λ restricted to B_{2g+1} reduces as the direct sum of representations π'_{λ_i}. For $i \leq k$ and each π'_{λ_i} we have the numbers r_i and d_i such that $d = \sum_{i=1}^k d_i$ and $r = \sum_{i=1}^k r_i$. The only way to have $\pi'_{\lambda_i}(\sigma_2...\sigma_{2g+1})^{2g+1} = 1$ for $(d_i - 2r_i)/d_i$ is to be $(d-2r)/d$ for all i. But this is impossible if $k > 1$. This completes the proof. $\square$

Precomposing the map of Proposition 6.3 with the surjective homomorphism

$$\mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2}),$$

we obtain the following corollary.

Corollary 6.4. *There is a well defined representation* $\mathrm{SMod}(\Sigma_g) \to \mathrm{End}(V_\lambda)$ *defined by* $T_{c_i} \mapsto q^{(2r-d)/d}\pi_\lambda(\sigma_i)$ *if and only if* λ *is rectangular.*

By using the formula given in the definition of W-graphs, the action of $H(q,6)$ on $[s_1s_3s_5]$ gives the following matrices for the generators of $\mathrm{Mod}(\Sigma_{0,6})$:

$$H_1 \mapsto q^{-1/5}\begin{pmatrix} -q^{-1} & 0 & 1 & 0 & 1 \\ 0 & -q^{-1} & 0 & 1 & 0 \\ 0 & 0 & q & 0 & 0 \\ 0 & 0 & 0 & q & 0 \\ 0 & 0 & 0 & 0 & q \end{pmatrix}, H_2 \mapsto q^{-1/5}\begin{pmatrix} q & 0 & 0 & 0 & 0 \\ 0 & q & 0 & 0 & 0 \\ 1 & 0 & -q^{-1} & 0 & 0 \\ 0 & 1 & 0 & -q^{-1} & 1 \\ 0 & 0 & 0 & 0 & q \end{pmatrix},$$

$$H_3 \mapsto q^{-1/5}\begin{pmatrix} -q^{-1} & 1 & 1 & 0 & 0 \\ 0 & q & 0 & 0 & 0 \\ 0 & 0 & q & 0 & 0 \\ 0 & 0 & 0 & q & 0 \\ 0 & 0 & 0 & 1 & -q^{-1} \end{pmatrix}, H_4 \mapsto q^{-1/5}\begin{pmatrix} q & 0 & 0 & 0 & 0 \\ 1 & -q^{-1} & 0 & 0 & 0 \\ 0 & 0 & q & 0 & 0 \\ 0 & 0 & 1 & -q^{-1} & 1 \\ 0 & 0 & 0 & 0 & q \end{pmatrix},$$

$$H_5 \mapsto q^{-1/5}\begin{pmatrix} -q^{-1} & 1 & 0 & 0 & 1 \\ 0 & q & 0 & 0 & 0 \\ 0 & 0 & -q^{-1} & 1 & 0 \\ 0 & 0 & 0 & q & 0 \\ 0 & 0 & 0 & 0 & q \end{pmatrix}.$$

6.2 The index of a normal closure of a power of a Dehn twist

Let $\mathcal{N}(h)$ denote the normal closure of an element h in $\mathrm{Mod}(\Sigma_{0,2g+2})$. In this section we use the Jones representation $J : \mathrm{Mod}(\Sigma_{0,2g+2}) \to \mathrm{End}(V_\lambda)$ to construct a linear representation for $\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n)$, for $n \geq 5$. Humphries constructed a linear representation for the group $\mathrm{Mod}(\Sigma_{0,6})/\mathcal{N}(H_i^n)$ and proved that $\mathrm{Mod}(\Sigma_{0,6})/\mathcal{N}(H_i^n)$ has infinite order if $n \geq 4$ [30, Theorem 4]. Our aim here is to extend Humphries' result for any $g \geq 2$.

Let λ be the Young diagram associated to the cell $[s_1s_3s_5...s_{2g+1}]$ as before. Consider the representation $\pi_\lambda : B_{2g+2} \to \mathrm{End}(V_\lambda)$. Recall from Section 4 that $\pi_\lambda(\sigma_i) = f_i$ and $e_i = (q - f_i)/(q + q^{-1})$ for $q^2 \neq -1$. Then we have $J(H_i) = q^{(2r-d)/d}(q - (q + q^{-1})e_i)$. We want to compute $J(H_i^n) = q^{n(2r-d)/d}(q - (q + q^{-1})e_i)^n$. Our aim is to modify the representation $J : \mathrm{Mod}(\Sigma_{0,2g+2}) \to \mathrm{End}(V_\lambda)$ such that the image of H_i^n trivial, and the relations of $\mathrm{Mod}(\Sigma_{0,2g+2})$ still hold. Then we will have a well defined linear representation for $\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n)$. Using the binomial theorem and the fact that $e_i^j = e_i$ for any $j \geq 2$, we can rewrite $(q-(q+q^{-1})e_i)^n$ as follows:

$$\begin{array}{rcl}(q-(q+q^{-1})e_i)^n & = & \sum_{j=0}^{n}(-1)^j\binom{n}{j}q^{n-j}(q+q^{-1})^j e_i^j \\ & = & q^n + \sum_{j=1}^{n}(-1)^j\binom{n}{j}q^{n-j}(q+q^{-1})^j e_i \\ & = & q^n + e_i(-q^n + e_i\sum_{j=0}^{n}(-1)^j\binom{n}{j}q^{n-j}(q+q^{-1})^j) \\ & = & q^n + e_i((q-q-q^{-1})^n - q^n) \\ & = & q^n + e_i((-1)^n q^{-n} - q^n)\end{array}$$

Hence, we have that

$$J(H_i^n) = q^{\frac{2nr}{d}} + e_i((-1)^n q^{2n\frac{r-d}{d}} - q^{\frac{2nr}{d}}). \tag{*}$$

Case n odd. It is convenient to change $q^{2/d}$ to t to obtain

$$J(H_i^n) = t^{nr} + e_i((-1)^n t^{n(r-d)} - t^{nr}).$$

We let $(-1)^n t^d$ be an n^{th} root of unity. Then we have $t^{nd} = -1$, and $t^n = (-1)^{1/d}$. If $J'(H_i) = (-1)^{-r/d}J(H_i)$, then $J'(H_i^n) = 1$. To see that the map

$$J' : \mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n) \to \mathrm{GL}_d(\mathbb{C}).$$

is a homomorphism, we only need to check that $J'(H_i)$ satisfy the relations of $\mathrm{Mod}(\Sigma_{0,2g+2})$. In fact we only need to check that $(2g+1)(2g+2)r/d$ is even. In that case we would have $(-1)^{(2g+1)(2g+2)r/d} = 1$ (see proof of Proposition 6.3). In the end of Section 3, we gave two formulas for d, r in terms of g. A direct calculation shows that

$$(2g+1)(2g+2)\frac{r}{d} = (g+1)(g+2).$$

The right hand side is an even number. This completes the case where n is odd.

Case n even. It is convenient to change $q^{1/d}$ to t to obtain

$$J(H_i^n) = t^{2nr} + e_i((-1)^n t^{2n(r-d)} - t^{2nr}).$$

We let t^d be an n^{th} root of unity. Then $t^{(d-2r)n}J(T_{c_i}^n) = 1$. In this case we denote $t^{(d-2r)n}J(H_i)$ by $J'(H_i)$. We want to show that the map

$$J' : \mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n) \to \mathrm{GL}_d(\mathbb{C})$$

is a well defined representation. By Lemma 6.2 the number $(d-2r)(2g+1)(2g+2)$ is an integer multiple of d. Therefore $n(d-2r)(2g+1)(2g+2)$ is a multiple of nd. Since t^d is a root of unity, then $J'(H_i)$ satisfy the relations of $\mathrm{Mod}(\Sigma_{0,2g+2})$ (see proof of Proposition 6.3).

We note here that the representations J' we constructed are not necessarily irreducible because the parameter t is a root of unity.

Theorem 6.5. *The group* $\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_{c_i}^n)$ *has infinite order if* $n \geq 5$.

Proof. Let $\Sigma_{0,2g+2}$ be a sphere with $2g+2$ marked points. We recall that $\mathrm{Mod}(\Sigma_{0,2g+2})$ is generated by the half-twists H_i for $i \leq 2g+1$. We will prove that the element $A = (H_1H_2)^6H_3(H_1H_2)^6H_3^{-1}$ has infinite order in $\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n)$. In fact we prove that $J'(A)$ has infinite order in $\mathrm{GL}_d(\mathbb{C})$ by showing that if μ is an eigenvalue of either $J'(A)$, then μ^n is not trivial for any $n \geq 4$. Consequently, $J'(A)^n$ is not the identity matrix for $n \geq 4$.

Case n odd. By construction we have that

$$J'(A) = (-1)^{\frac{-12r}{d}} t^{6(2r-d)} \pi(\sigma_1\sigma_2)^6\pi(\sigma_3)\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)^{-1}.$$

We denote by C the matrix $\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)^{-1}$. Again by Theorem 3.8 we have that the first 5×5 block of C are the same for any $g \geq 2$. We denote this 5×5 block by C'. The matrix C' has 3 eigenvalues (2 distinct and 1 repeated).

Let $(-1)^nt^d$ be an n^{th} root of unity. We set $t^d = \exp((3k\pi i)/n)$ where $n = (4k \pm 1)$ if k is odd, and $t^d = (-1)^{-n}\exp(((3k-1)\pi i)/n)$ where $n = (4k \pm 1)$ if k is even. In both cases if $k \to \infty$ then the absolute value of one of the eigenvalues of C' converges to 9.5521659 approximately, thus it has infinite order. This completes the proof when n odd.

Case n even. By the construction of the representation we have that

$$J'(A) = t^{\frac{12}{2}(2r-d)+(d-2r)n} \pi(\sigma_1\sigma_2)^6\pi(\sigma_3)\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)^{-1}.$$

We denote by C the matrix $\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)\pi(\sigma_1\sigma_2)^6\pi(\sigma_3)^{-1}$. We want to prove that C has infinite order. By Theorem 3.8 we have that the first 5×5 block of C are the same for any $g \geq 2$. Denote this 5×5 block by C'. We note that C' has 5 eigenvalues (2 distinct, and 1 repeated).

For $n = 6$, if $t^d = \exp(\pi i/3)$, then the absolute value of one of the eigenvalues of C' is equal to 9.8989795 approximately. Hence, it has infinite order. It follows that if n is even and it is divisible by 3 then the eigenvalue has infinite order. For $n = 2(3k \pm 1) > 6$, put $t^d = \exp((4\pi i k)/n)$. If $k \to \infty$ then the absolute value of the same eigenvalue converges to 9.8989795 approximately, thus, it has infinite order. This completes the proof when n is even. □

As a corollary we obtain a similar theorem for $\mathrm{SMod}(\Sigma_g)$. Consider the homomorphism $\mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2})$ defined by $T_{c_i} \mapsto H_i$ as described in Section 4.2, where c_i are symmetric curves of Figure 3.4. Then we have a surjective homomorphism $\mathrm{SMod}(\Sigma_g)/\mathcal{N}(T_c^n) \to \mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n)$. Therefore, we obtain the following corollary.

Corollary 6.6. *The group* $\mathrm{SMod}(\Sigma_g)/\mathcal{N}(T_c^n)$ *has infinite order if* $n \geq 5$ *and* $g \geq 2$.

Free nonabelian subgroups. Theorem 6.5 shows that $\mathcal{N}(H_{c_i}^n)$ is very small comparing to $\mathrm{Mod}(\Sigma_{0,2g+2})$ if $n \geq 5$, since $\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_{c_i}^n)$ has infinite order. In fact we can do even more than that. We can prove that $\mathcal{N}(H_{c_i}^n)$ is even much smaller than what Theorem 6.5 suggests.

Theorem 6.7. *The quotient of* $\mathrm{Mod}(\Sigma_{0,2g+2})$ *by the normal closure of the* m^{th} *power of a half-twist contains a free nonabelian subgroup, if* $g \geq 2$, *and* $m \notin \{1, 2, 3, 4, 6, 10\}$.

In the proof of Theorem 6.5 we found an element in $J'(\mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_{c_i}^n))$ (that is, in the image of the quotient of the Jones representation) and we computed its order. Theorem 6.7 was suggested by Funar.

Proof. Consider Equation (*). For n even, let $q^{2/d}$ be an n^{th} root of unity. Then we have that $J(H_i^n)$ is trivial. By denoting J by J' we have a well defined linear representation

$$J' : \mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n) \to \mathrm{GL}_d(\mathbb{C}).$$

For n odd, let $-q^2$ be an n^{th} root of unity. In this case $(-1)^{-r/d} J(H_i^n)$ is trivial (see proof of Theorem 6.5). We set $(-1)^{-r/d} J(H_i) = J'(H_i)$ and we have

$$J' : \mathrm{Mod}(\Sigma_{0,2g+2})/\mathcal{N}(H_i^n) \to \mathrm{GL}_d(\mathbb{C}).$$

Our aim is to prove that the group $J'(G)$ generated by the elements $J'(H_1^2)$ and $J'(H_2^2)$, contains a free nonabelian subgroup. By Young's lattice described in Section 5.1, if we restrict the Jones representation to the subgroup generated by H_1, H_2 then the representation J reduces into a direct sum of subrepresentations containing the representation labeled by $\lambda = \begin{smallmatrix}\square & \square \\ \square & \end{smallmatrix}$. Therefore, the elements $q^{(2r-d)/d}\pi_\lambda(\sigma_i) = \pi'_\lambda(\sigma_i)$ where $i = 1, 2$ are contained in the image of J. In Section 5.1 we saw that the map π_λ is the Burau representation. If q^2 is not a primitive root of unity of order in the set $\{1, 2, 3, 4, 6, 10\}$, then $\pi_\lambda(PB_3)$ contains a free nonabelian subgroups [24, Lemma 3.9].

Case n even. If $q^{2/d}$ is an n^{th} nonprimitive root of unity such that $n \notin \{2, 4, 6, 10\}$, then $\pi'_\lambda(PB_3) < J'(G)$ contains a free nonabelian subgroups, since scalar multiplication of elements of a free group, give a free group as well.

Case n odd. If we consider $-q^2$ to be an n^{th} nonprimitive root of unity such that $n \notin \{1, 3\}$, then $\pi'_\lambda(PB_3) < J'(G)$ contains a free nonabelian subgroups, since scalar multiplication of elements of a free group, give a free group as well. $\square$

By the Birman-Hilden homomorphism $\mathrm{SMod}(\Sigma_g) \to \mathrm{Mod}(\Sigma_{0,2g+2})$ sends every Dehn twist about symmetric curve into a half twist in $\mathrm{Mod}(\Sigma_{0,2g+2})$. Therefore, the result of Theorem 6.7 shows that the quotient of $\mathrm{SMod}(\Sigma_g)$ by the normal closure of the m^{th} power of a Dehn twist about a symmetric curve contains a nonabelian free subgroup if $m \notin \{1, 2, 3, 4, 6, 10\}$.

Factor groups of braid groups. The symmetric group S_n is a finite group that can be considered as a quotient group of the braid group B_n over the relation $\sigma_1^2 = 1$ where σ_1 is a generator of B_n. If we generalize this relation to σ_1^m such that m is any integer greater than 2, then the quotient group is not always finite. In fact, Coxeter proved that the group $B_n / < \sigma_1^m >$ is finite if and only if $(n-2)(m-2) < 4$ [16, Section 10]. We will reprove Coxeter's theorem for $n \geq 5$, and $m \geq 5$ using the proof Theorem 6.5.

Theorem 6.8. *The normal closure of σ_i^m in B_n has infinite index in B_n, if $m \geq 5$, and $n \geq 4$.*

Proof. We want to prove that if $\mathcal{N}(\sigma_i^m)$ is the normal closure of σ_i^m in B_n, then $B_n/\mathcal{N}(\sigma_i^m)$ has infinite order when $m \geq 5$, and $n \geq 4$.

Recall the representations $J' : S\mathrm{Mod}(\Sigma_g)/\mathcal{N}(T_{c_i}^m) \to \mathrm{GL}_d(\mathbb{C})$, when m is even, and $J' : S\mathrm{Mod}(\Sigma_g)/\mathcal{N}(T_{c_i}^m) \to \mathrm{GL}_d(\mathbb{C})$ when m is odd. By the surjective homomorphism $B_{2g+2} \twoheadrightarrow \mathrm{SMod}(\Sigma_g)$ defined by $\sigma_i \mapsto T_{c_i}$ we have

$$B_{2g+2}/\mathcal{N}(\sigma_i^m) \twoheadrightarrow \mathrm{SMod}(\Sigma_g)/\mathcal{N}(T_{c_i}^m) \to \mathrm{GL}_d(\mathbb{C})$$

when m is even, and

$$B_{2g+2}/\mathcal{N}(\sigma_i^m) \twoheadrightarrow \mathrm{SMod}(\Sigma_g)/\mathcal{N}(T_{c_i}^m) \to \mathrm{GL}_d(\mathbb{C})$$

when m is odd.

Case n is even. In this case the theorem follows by the surjectivity of

$$B_{2g+2}/\mathcal{N}(\sigma_i^m) \twoheadrightarrow \mathrm{SMod}(\Sigma_g)/\mathcal{N}(T_{c_i}^m).$$

Case n is odd. We want to prove that $B_{2g+1}/\mathcal{N}(\sigma_i^m)$ has infinite order. If we restrict the above representations to B_{2g+1} we get

$$B_{2g+1}/\mathcal{N}(\sigma_i^m) \to \mathrm{GL}_d(\mathbb{C})$$

when m is even, and

$$B_{2g+1}/\mathcal{N}(\sigma_i^m) \to \mathrm{GL}_d(\mathbb{C})$$

when m is odd. These representations above are well defined, by the restriction formula described in Section 5.1. By the proof of Theorem 6.5, the elements $(\sigma_1\sigma_2)^6\sigma_3(\sigma_1\sigma_2)^6(\sigma_3)^{-1}$ and $(\sigma_1\sigma_2)^6\sigma_3(\sigma_1\sigma_2)^6$ have infinite order in $B_{2g+1}/\mathcal{N}(\sigma_i^m)$.

To complete the proof, we denote by $\mathcal{N}'(\sigma_i^n)$ the normal closure of σ_i^m in B_4, and we denote by $\mathcal{N}(\sigma_i^m)$ the normal closure of σ_i^n in B_5.

We have that $B_4/(\mathcal{N}(\sigma_i^n)\cap B_4) < B_5/\mathcal{N}(\sigma_i^m)$, and $(\mathcal{N}(\sigma_i^m)\cap B_4)/\mathcal{N}'(\sigma_i^m)\lhd B_4/\mathcal{N}'(\sigma_i^m)$. By the third isomorphism theorem we get a surjective homomorphism

$$B_4/\mathcal{N}'(\sigma_i^m) \to B_4/(\mathcal{N}(\sigma_i^m)\cap B_4) < B_5/\mathcal{N}(\sigma_i^m).$$

But again the elements $(\sigma_1\sigma_2)^6\sigma_3(\sigma_1\sigma_2)^6$ and $(\sigma_1\sigma_2)^6\sigma_3(\sigma_1\sigma_2)^6(\sigma_3)^{-1}$ are in B_4. Hence, $B_4/\mathcal{N}'(\sigma_i^m)$ has infinite order. $\square$

Chapter 7

Symplectic representations of braid groups

In this chapter we construct representations of braid groups whose images are symplectic. For the definition of the symplectic group see Section 2.4. In Section 7.1 we give two constructions for the symplectic representation of braid groups. The first uses monodromy actions on hyperelliptic curves, while the second uses the symplectic representation of the mapping class group. In Section 7.2 we give a topological definition of the Burau representation of braid groups. The Burau representation is defined over a ring of polynomials $\mathbb{Z}[t^{\pm 1}]$, where t is considered as any complex number. If we evaluate $t = -1$, then we explain how the image of the Burau representation becomes symplectic.

7.1 Symplectic representation

In this section we give two constructions of the symplectic representation

$$\rho : B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}) & \text{if } b = 1 \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

where $(\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$ stands for the stabilizer subgroup of $\mathrm{Sp}_{2g+2}(\mathbb{Z})$ of one particular vector as described in Section 2.4.

7.1.1 Representation via monodromy

In the following construction follow A'Campo [2, Introduction]. Consider the universal cover $F : \mathbb{C}^2 \times \mathbb{C}^{n-1} \to \mathbb{C} \times \mathbb{C}^{n-1}$ defined by

$$F(x, y, a_1, ..., a_{n-1}) = (x^n - y^2 + \sum_{i=1}^{n-1} a_i x^{i-1}, a_1, ..., a_{n-1}).$$

Consider also the space $X = \{(x, y, a_1, ..., a_{n-1}) \mid F(x, y, a_1, ..., a_{n-1}) = (0, a_1, ..., a_{n-1})\}$ Obviously X is a subset of $\mathbb{C}^2 \times \mathbb{C}^{n-1}$. We define the fibration map $\pi : X \to \mathbb{C}^{n-1}$. We denote by $[x]$ the greatest integer y of x such that $y < x$. For $\vec{a} = (a_1, ..., a_{n-1})$, the fiber $\pi^{-1}(\vec{a}) = X_{\vec{a}}$ is a hyperelliptic curve of genus $[(n-1)/2]$ in $\mathbb{C}^2$. The fiber $X_{\vec{a}}$ is smooth if and only if $x^n + \sum_{i=1}^{n-1} a_i x^{i-1}$ has simple roots. We define the set

$$\Delta = \{(a_1, ...a_{n-1}) = \vec{a} \mid \text{when } X_{\vec{a}} \text{ is not smooth}\}$$

and we obtain a fibration

$$\phi : X \setminus \pi^{-1}(\Delta) \to \mathbb{C}^{n-1} \setminus \Delta.$$

The fiber with respect to ϕ is diffeomorphic to a surface of genus $[(n-1)/2]$ with $r = gcd(n, 2)$ punctures, that is $\Sigma_{g,r}$ when $g = [(n-1)/2]$.

The alternating bilinear form $\hat{\imath} : \mathrm{H}_1(\Sigma_{g,r}, \mathbb{Z}) \wedge \mathrm{H}_1(\Sigma_{g,r}, \mathbb{Z}) \to \mathbb{Z}$ is the algebraic intersection number of curves in $\Sigma_{g,r}$. If $r = 1$, then $\hat{\imath}$ is symplectic.

Odd case. We have that $\mathrm{Aut}(\mathrm{H}_1(\Sigma_{g,1}, \mathbb{Z})) = \mathrm{Sp}_{2g}(\mathbb{Z})$. Fix a point $\hat{p} \in \mathbb{C}^{n-1} \setminus \Delta$. The action of $\pi_1(\mathbb{C}^{n-1} \setminus \Delta, \hat{p})$ on $\Sigma_{g,1}$ defines a representation

$$\rho : \pi_1(\mathrm{C}^{n-1} \setminus \Delta, \hat{p}) \to \mathrm{Sp}_{2g}(\mathbb{Z}).$$

But $\pi_1(\mathbb{C}^{n-1} \setminus \Delta, \hat{p})$ is isomorphic to the braid group B_n. Thus, we have

$$\rho : B_n \to \mathrm{Sp}_{2g}(\mathbb{Z}).$$

Even case. If $n = 2g + 2$ then $r = 2$. Consider $\mathrm{H}_1(\Sigma_{g,2}, Q, \mathbb{Z})$, where Q is the set containing the two punctures. Then we have a representation

$$\rho : B_n \to \mathrm{Aut}(\mathrm{H}_1(\Sigma_{g,2}, Q, \mathbb{Z})).$$

Recall the partitioned homology $\mathrm{H}_1^P(\Sigma_g^2) \cong \mathrm{H}_1(\Sigma_g^2, Q, \mathbb{Z})/\langle P \rangle$, where P is the set that contains the boundary components of Σ_g^2 (see Section 2.3). Recall also from Section 2.4 that $\mathrm{Aut}(\mathrm{H}_1^P(\Sigma_g^2)) = (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$. Consider the inclusion $\Sigma_g^2 \hookrightarrow \Sigma_{g,2}$ induced by gluing a disc with puncture in each boundary of Σ_g^2. Then we have a surjective homomorphism $\mathrm{H}_1^P(\Sigma_g^2) \to \mathrm{H}_1(\Sigma_{g,2}, Q, \mathbb{Z})$. But the abelian groups $\mathrm{H}_1^P(\Sigma_g^2), \mathrm{H}_1(\Sigma_{g,2}, Q, \mathbb{Z})$ have the same rank. Thus, we get $\mathrm{H}_1^P(\Sigma_g^2) \cong \mathrm{H}_1(\Sigma_{g,2}, Q, \mathbb{Z})$ and we obtain a representation

$$\rho : B_n \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}.$$

7.1.2 Representation via hyperelliptic mapping class group

Consider the surface Σ_g^b of genus g with $1 \leq b \leq 2$ boundary components. Recall that the mapping class group $\mathrm{Mod}(\Sigma_g^b)$ is the group of self-homeomorphisms of Σ_g^b fixing the boundary pointwise modulo isotopies that fix the boundary pointwise. Let ι be the hyperelliptic involution that acts on Σ_g^b as described in Section 4.2. We recall from Section 4.2 that the hyperelliptic mapping class group $\mathrm{SMod}(\Sigma_g^b)$ consists of elements of $\mathrm{Mod}(\Sigma_g^b)$ that commute with a fixed hyperelliptic involution ι. The group $\mathrm{SMod}(\Sigma_g^b)$ is generated by Dehn twists T_{c_i} about curves c_i as indicated in Figure 4.10.

For $i \leq 2g+b-1$ and $b = 1, 2$, let σ_i be the generators of the braid group B_{2g+b}. In the end of Section 4.2 we defined a homomorphism

$$\rho : B_{2g+b} \to \begin{cases} \mathrm{SMod}(\Sigma_g^1) & \text{if } b = 1, \\ \mathrm{SMod}(\Sigma_g^2) & \text{if } b = 2 \end{cases}$$

by $\sigma_i \mapsto T_{c_i}$. The action of $\mathrm{SMod}(\Sigma_g^1)$ on $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ gives a representation

$$B_{2g+1} \to \mathrm{SMod}(\Sigma_g^1) \to \mathrm{Sp}_{2g}(\mathbb{Z}).$$

Furthermore, the action of $\mathrm{SMod}(\Sigma_g^2)$ on $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ gives a representation

$$B_{2g+2} \to \mathrm{SMod}(\Sigma_g^2) \to (\mathrm{Sp}_{2g}(\mathbb{Z}))_{y_{g+1}}.$$

7.1.3 Matrices of symplectic representation

At this stage we can compute the matrices of the symplectic representation. Recall that B_{2g+b} is generated by σ_i where $i < 2g+b$ and $b = 1, 2$. The map $B_{2g+b} \to \mathrm{SMod}(\Sigma_g^b)$ is given by $\sigma_i \mapsto T_{c_i}$. Denote by $T_{[c_i]}$ the transvection associated to the homology class $[c_i]$ of c_i. We recall that a transvection $T_{[c_i]}$ acts on $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ (respectively $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$) by $T_{[c_i]}(u) = u + \hat{i}(u, [c_i])[c_i]$ for all $u \in \mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ (respectively $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$).

Consider the generators y_i, x_i of $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ (respectively $\mathrm{H}_1^P(\Sigma_g^2)$) as indicated in Figure 7.1, with the algebraic intersection number as follows: $\hat{i}(x_i, x_j) = \hat{i}(y_i, y_j) = 0$ and $\hat{i}(y_i, x_i) = 1$. We also set $y_1 = (1, 0, 0, ..., 0)$, $x_1 = (0, 1, 0, ..., 0)$,...,$y_g = (0, 0, 0, ..., 1, 0)$, $x_g = (0, 0, 0, ..., 1)$. Furthermore, for $i \geq 1$ we have that $[c_{2i-1}] = y_i - y_{i+1}$.

For $b = 1$ we have the representation $\rho : B_{2g+1} \to \mathrm{Sp}_{2\mathrm{g}}(\mathbb{Z})$ determined by

$$\rho(\sigma_1) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \oplus I_{2g-2}.$$

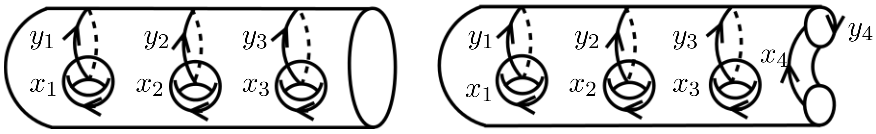


Figure 7.1: Standard generators for $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$, and $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$.

If i is even, then

$$\rho(\sigma_i) = I_{i-2} \oplus \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \oplus I_{2g-i}.$$

If $i \neq 1$ is odd, then

$$\rho(\sigma_i) = I_{i-3} \oplus \begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \oplus I_{2g-i-1}.$$

For $b = 2$ we have the representation $\rho : B_{2g+2} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$ determined by

$$\rho(\sigma_1) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \oplus I_{2g-1}$$

If i is even, then

$$\rho(\sigma_i) = I_{i-2} \oplus \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \oplus I_{2g+1-i}.$$

If i is odd but $i \neq 1, 2g+1$, then

$$\rho(\sigma_i) = I_{i-3} \oplus \begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \oplus I_{2g-i}.$$

The transvection $T_{[c_{2g+1}]}$ is slightly more complicated. We can easily verify that the following matrix satisfies the braid relations with the other matrices above.

$$\rho(\sigma_{2g+1}) = I_{2g-2} \oplus \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

7.2 Burau representation

In Section 5.2 we defined the Burau representation in terms of matrices and we showed that the Burau representation is a Hecke algebra representation. In this section we define the Burau representation from a homological point of view. The section is organized as follows. First, we define the reducible representation in terms of matrices, that is $\tilde{b}_t : B_n \to \mathrm{GL}(n, \mathbb{Z}[t^{\pm 1}])$, where t is indeterminate, and then we give a homological interpretation of the latter representation. The representation $\tilde{b}_t$ is reducible. We show how to reduce $\tilde{b}_t$ as a direct sum of one-dimensional irreducible representation and an $(n-1)$-dimensional irreducible representation (which is denoted by b_t). In the end we will state the theorem that relates the image of the symplectic representation ρ from the previous section with the image of b_{-1}.

7.2.1 The reducible Burau representation

Let $\Lambda = \mathbb{Z}[t^{\pm 1}]$ be the ring of Laurent polynomials with integer coefficients. Define the matrices of $\mathrm{GL}(n, \Lambda)$ as follows:

$$U_i = I_{i-1} \oplus \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \oplus I_{n-i-1},$$

where $i = 1, 2, ..., n-1$.

Proposition 7.1. *The map $\tilde{b}_t : B_n \to \mathrm{GL}(n, \Lambda)$ defined by $\tilde{b}_t(\sigma_i) = U_i$ is a homomorphism.*

Proof. We have to prove that the relations for σ_i also hold for U_i. Note that

$$U_i^{-1} = I_{i-1} \oplus \begin{pmatrix} 0 & 1 \\ t^{-1} & 1-t^{-1} \end{pmatrix} \oplus I_{n-i-1}.$$

The block form of the matrices implies that $U_iU_j = U_jU_i$ for $|i-j| \geq 2$. To see that $U_iU_{i+1}U_i = U_{i+1}U_iU_{i+1}$, it suffices to check that the next equality holds.

$$\begin{pmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -t+1 & -t^2+t & t^2 \\ -t+1 & t & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} -t+1 & -t^2+t & t^2 \\ -t+1 & t & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

This is a straightforward calculation.

□

7.2.2 Homological interpretation

Recall from Chapter 4 that if D_n is an n-punctured disc, then $B_n \cong \mathrm{Mod}(D_n)$. So it is convenient here to identify braids by homeomorphisms on the punctured disc D_n. We set $\eta : B_n \to \mathrm{Mod}(D_n)$. Fix a point $d \in \partial D_n$. Define the homomorpshism $\epsilon : \pi_1(D_n, d) \to \mathbb{Z} = \langle t \rangle$ by

$$\gamma \to t^{w(\gamma)},$$

where $\gamma \in \pi_1(D_n, d)$ and $w : \pi_1(D_n, d) \to \mathbb{Z}$ is the sum of the winding numbers of a loop in $\pi_1(D_n, d)$ around the punctures. The kernel of ϵ defines a covering $\tilde{D}_n \to D_n$ and the group of deck transformations is $\langle t \rangle = \mathbb{Z}$.

Fix a point $\tilde{d}$ in the fiber of d and consider the relative homology group $\tilde{H} = \mathrm{H}_1(\tilde{D}_n, \mathbb{Z}\tilde{d}, \mathbb{Z})$, where $\mathbb{Z}\tilde{d}$ is the $\mathbb{Z}$-orbit of $\tilde{d}$. The elements t^k for $k \in \mathbb{Z}$ act on $\tilde{D}_n$ as deck transformations and this action induces an action on $\tilde{H}$ making the latter group a Λ-module. To compute the rank of $\tilde{H}$, we note that D_n deformation retracts onto a union of n circles whose intersection is d. The lifts of these circles are arcs $t^k X_i$ connecting the points $t^k\tilde{d}$ and $t^{k+1}\tilde{d}$ (the points $t^k\tilde{d}$ and $t^{k+1}\tilde{d}$ are in the fiber of d). The module $\tilde{H}$ has rank n, and it is generated by $[X_i]$ for $i = 1, 2, ..., n$ [43, Section 1].

Consider a homeomorphism $f \in \mathrm{Mod}(D_n)$. By definition, f fixes the boundary of D_n; thus, f fixes the point $d \in \partial D_n$. The induced automorphism $f_\sharp : \pi_1(D_n, d) \to \pi_1(D_n, d)$ fixes the winding number of the elements of $\pi_1(D_n, d)$. The unique lift of f denoted by $\tilde{f} : \tilde{D}_n \to \tilde{D}_n$ commutes with the action of $\langle t \rangle$ on $\tilde{D}_n$. Consequently $\tilde{f}(t^k\tilde{d}) = t^k\tilde{d}$. Let $f_* : \tilde{H} \to \tilde{H}$ be the induced map of $\tilde{f}$. Define the representation $\tilde{b}'_t : \mathrm{Mod}(D_n) \to \mathrm{Aut}(\tilde{H})$ by $\tilde{b}'_t(f) = f_*$.

The next theorem shows that the homological representation constructed above coincides with the Burau representation defined in Section 7.2.1.

Theorem 7.2. *The following diagram commutes.*

$$\begin{tikzcd} B_n \arrow[r, "\eta"] \arrow[d, "\tilde{b}_t"] & \mathrm{Mod}(D_n) \arrow[d, "\tilde{b}'_t"] \\ \mathrm{GL}(n, \Lambda) \arrow[r, "\mu"] & \mathrm{Aut}(\tilde{H}), \end{tikzcd}$$

where $\mu : \mathrm{GL}(n, \Lambda) \to \mathrm{Aut}(\tilde{H})$ *is an isomorphism.*

Proof. Recall that $\mathrm{Aut}(\tilde{H})$ is freely generated by X_i, for $i = 1, 2, ..., n$. Define the map μ as $\mu(U) = (U^T)^{-1}$, where U^T is the transpose of U. We want to prove that for $\beta \in B_n$, the following holds:

$$\tilde{b}'_t\eta(\beta) = \mu\tilde{b}_t(\beta).$$

We prove the above statement for the generators $\sigma_1^{-1}, \sigma_2^{-1}, ..., \sigma_{n-1}^{-1}$.

Enumerate the punctures of the disc D_n from left to right. Let $\gamma_i \in D_n$ be the representatives of the generators of the fundamental group $\pi_1(D_n, d)$ (that is, loops around the punctures with starting and ending point in d). The homeomorphism $\eta(\sigma_i^{-1})$ is a half-twist interchanging the punctures i and $i+1$. The homeomorphism $\eta(\sigma_i^{-1})$ fixes γ_k for $k \neq i, i+1$, transforms γ_i into $\gamma_i\gamma_{i+1}\gamma_i^{-1}$ and transforms γ_{i+1} into γ_i. When we lift the homeomorphism $\eta(\sigma_i^{-1})$ into $\tilde{D}_n$, then this lift fixes X_k for $k \neq i, i+1$, transforms X_{i+1} into X_i and stretches X_i into the path $X_i(tX_{i+1})(tX_i)^{-1}$. Thus, $\tilde{b}_t'\eta(\sigma_i^{-1})$ acts on $\tilde{H}$ as follows:

$$\begin{array}{lll} [X_i] & \to & (1-t)[X_i] + tX_{i+1}, \\ [X_{i+1}] & \to & [X_i], \\ [X_k] & \to & [X_k]. \end{array}$$

for $k \neq i, i+1$. But the matrix defined by this action is precisely $\mu\tilde{b}_t(\sigma_i^{-1})$. This concludes the proof.

□

7.2.3 The reduced Burau representation

The Burau representation defined in the previous subsection is reducible. In fact it reduces into a one-dimensional representation and an $(n-1)$-dimensional representation. We call the latter representation as reduced Burau representation. In this section we compute the *reduced Burau representation*. For $n > 2$ define the $(n-1)$-dimensional square matrices

$$V_1 = \begin{pmatrix} -t & 0 \\ 1 & 1 \end{pmatrix} \oplus I_{n-3}$$

$$V_2 = I_{n-3} \oplus \begin{pmatrix} 1 & t \\ 0 & -t \end{pmatrix}$$

and for $1 < i < n-1$,

$$V_i = I_{i-2} \oplus \begin{pmatrix} 1 & t & 0 \\ 0 & -t & 0 \\ 0 & 1 & 1 \end{pmatrix} \oplus I_{n-i-2}.$$

Let C be the upper triangular matrix with all nonzero entries equal to 1:

$$C = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Proposition 7.3. *We have*

$$C^{-1}U_iC = \begin{pmatrix} V_i & 0 \\ X_i & 1 \end{pmatrix}$$

where U_i are the matrices defined in the begining of Section 7.2.1; the row vector X_i has length $n-1$, and $X_i = (0, ..., 0)$ if $i \neq n-1$ and $X_{n-1} = (0, ..., 0, 1)$.

Proof. Let

$$W_i = \begin{pmatrix} V_i & 0 \\ X_i & 1 \end{pmatrix}$$

It suffices to prove that $U_iC = CW_i$. But both matrices are equal to a matrix obtained from C replacing the $(i,i)^{th}$ entry by $1-t$ and the $(i+1,i)^{th}$ entry by 1. □

Since U_i satisfy the braid relation, the same is true for W_i. Furthermore, since $\det(W_i) = \det(V_i)$, the matrices V_i are invertible. Also, the fact that the last column of W_i is nonzero in the last entry implies that V_i satisfy the braid relations. So we can define

$$b_t : B_n \to \mathrm{Aut}(\Lambda^{n-1})$$

by $b_t(\sigma_i) = V_i$. The representation b_t is the reduced Burau representation.

7.2.4 Homological interpretation and the symplectic representation

In this section we give a homological interpretation of the reduced Burau representation similar to Section 7.2.2. Then we describe the relation of the Burau representation with the symplectic representation.

Let D_n be an n-punctured disc and let d be a fixed point in ∂D_n. Recall from Section 7.2.2 the homomoprhism $\epsilon : \pi_1(D_n, d) \to \mathbb{Z} = \langle t \rangle$, determined by $\gamma \mapsto t^{w(\gamma)}$ where $w(\gamma)$ stands for the sum of the winding numbers of γ around the punctures of D_n. The kernel of ϵ defines a covering space map $\tilde{D}_n \to D_n$ with $\mathrm{Aut}(D_n) = \mathbb{Z}$. Every homotopy class of homeomorphisms $f : D_n \to D_n$ fixing ∂D_n lifts uniquely to $f_* : \tilde{D}_n \to \tilde{D}_n$.

Here we define chain complexes of D_n as $\mathbb{Z}[t^{\pm 1}]$ modules. The face of D_n lifts to a face of $\tilde{D}_n$ and as a $\mathbb{Z}[t^{\pm 1}]$ module generates the trivial group. The disc D_n deformation retracts to the wedge sum of circles X_i, $i \leq n$ with common point d. We choose lifts $\tilde{X}_i$ of X_i in $\tilde{D}_n$. As $\mathbb{Z}[t^{\pm 1}]$ modules the cycles $\tilde{X}_i$ generate a chain complex C_1. The $\mathbb{Z}[t^{\pm 1}]$ module $\mathrm{H}_1(\tilde{D}_n, \mathbb{Z}[t^{\pm 1}])$ contains cycles such that the sum of the coordinates in the basis of C_1 is zero. Then $\mathrm{H}_1(\tilde{D}_n, \mathbb{Z}[t^{\pm 1}])$ is spanned by

$$\begin{aligned} u_1 &= \tilde{X}_1 - \tilde{X}_2, \\ u_2 &= \tilde{X}_2 - \tilde{X}_3, \\ &\vdots \\ u_{n-1} &= \tilde{X}_{n-1} - \tilde{X}_n. \end{aligned}$$

The induced action of f_* on $\mathrm{H}_1(\tilde{D}_n, \mathbb{Z}[t^{\pm 1}])$ is the reduced Burau representation [8, Section 4.4].

If we set $t = -1$, then $\langle t \rangle \cong \mathbb{Z}/2$, and the covering space map $\tilde{D}_n \to D_n$ becomes a two fold branched cover. Then the image of the symplectic representation

$$\rho : B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

is conjugate to the image of the Burau representation $b_{-1} : B_n \to \mathrm{Aut}(\mathrm{H}_1(\tilde{D}_n, \mathbb{Z}[t^{\pm 1}]))$ [25, Proposition 2.1].

Chapter 8

Congruence subgroups of braid groups

In this chapter we study congruence subgroups of braid groups B_n. More precisely, in Theorem 6.8 we proved that for $m \geq 5$ then $B_n/\mathcal{N}(\sigma_i^m)$ is infinite when $n \geq 4$. In order to obtain a finite quotient group of B_n we need more relations. In Section 8.1 we recall basic facts for congruence subgroups of the symplectic group. In Section 8.2 we examine the kernels of the symplectic representation (over $\mathbb{Z}$ and $\mathbb{Z}/m$, where $m = 2, 4$) of B_n, and we explain the isomorphism between the level 2 congruence subgroup of B_n and the pure braid group PB_n. In the end of Section 8.2 we characterize the level p congruence subgroups of B_n, when p is a prime number. In Section 8.3 we use the results of Sections 8.1 and 8.2 to find relations between PB_n and the level m congruence subgroups of B_n, when $m = 2p_1p_2...p_k$, and $m = 4p_1p_2...p_k$, and $p_i \geq 3$ are prime numbers. In the end of Section 8.3 we give generators for the level $2p$ congruence subgroups of B_n, where p is a prime number. In the last section of this chapter, we study symmetric quotients of the level p congruence subgroups of B_n.

8.1 Congruence subgroups of symplectic groups

We recall the definition of $\mathrm{Sp}_{2n}(\mathbb{Z})$ from Chapter 2. Let J be the $2n \times 2n$ matrix

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

The symplectic group with integer coefficients is defined to be

$$\mathrm{Sp}_{2n}(\mathbb{Z}) = \{A \in \mathrm{GL}(2n, \mathbb{Z}) \mid A^T J A = J\}.$$

We also define the symplectic group with coefficients in $\mathbb{Z}/m$ to be

$$\mathrm{Sp}_{2n}(\mathbb{Z}/m) = \{A \in \mathrm{GL}(2n, \mathbb{Z}) \mid A^T J A \equiv J \bmod(m)\}$$

where $m \in \mathbb{N}$. For a fixed $u \in \mathbb{Z}^{2n}$, we also recall

$$(\mathrm{Sp}_{2n}(\mathbb{Z}))_u = \{t \in \mathrm{Sp}_{2n}(\mathbb{Z}) \mid t(u) = u\}.$$

General linear Lie algebra. A Lie algebra $\mathfrak{g}$ is a vector space over a field $\mathbb{F}$ together with a bilinear form

$$\{\cdot,\cdot\} : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

which is skew symmetric and satisfies the Jacobi identity. That is, for $x, y, z \in \mathfrak{g}$, then

$$\{x, \{y, z\}\} + \{y, \{z, x\}\} + \{z, \{x, y\}\} = 0.$$

Let V be a vector space. then $\mathrm{End}(V)$ forms an associative algebra under function composition. The Lie bracket is the commutator, that is, $[x, y] = xy - yx$. The Lie algebra $\mathrm{End}(V)$ is denoted by $\mathfrak{gl}_{2n}(V)$ and it is called *general linear Lie algebra.*

The symplectic Lie algebra $\mathfrak{sp}_{2n}(\mathbb{Z})$ consists of those elements $A \in \mathfrak{gl}_{2n}(\mathbb{Z})$ which satisfy $A^T J + JA = 0$. We define also

$$\mathrm{Ann}(u) = \{m \in \mathfrak{sp}_{2n}(\mathbb{Z}) \mid m(u) = 0\},$$

where $\mathrm{Ann}(u)$ stands for the annihilator of the vector u.

Congruence subgroups and generators. The projection $\mathbb{Z} \to \mathbb{Z}/m$ induces a surjective homomorphism $\mathrm{Sp}_{2n}(\mathbb{Z}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/m)$, whose kernel is the *principal level m congruence subgroup* of $\mathrm{Sp}_{2n}(\mathbb{Z})$ denoted by $\mathrm{Sp}_{2n}(\mathbb{Z})[m]$. The group $\mathrm{Sp}_{2n}(\mathbb{Z})[m]$ consists of all matrices of the form $I_{2n} + mA$; where $A \in \mathrm{Sp}_{2n}(\mathbb{Z})$. Furthermore, if m is a multiple of l then $\mathrm{Sp}_{2n}(\mathbb{Z})[m] \lhd \mathrm{Sp}_{2n}(\mathbb{Z})[l]$.

Next we give generators for $\mathrm{Sp}_{2n}(\mathbb{Z})[p]$ when p is any prime number. Let $r \in \mathbb{Z}$. We define $\epsilon_{i,j}(r)$ to be the $n \times n$ matrix with $(i,j)^{th}$ entry equal to r and 0 otherwise. Let $\beta_i(r)$ be the $n \times n$ matrix with $(i,i)^{th}$ and $(i,i+1)^{th}$ entries equal to r, $(i+1,i+1)^{th}$ and $(i+1,i)^{th}$ entries equal to $-r$ and 0 otherwise. Define also $s\epsilon_{i,j}(r)$ to be the $n \times n$ matrix with $(i,j)^{th}$ and $(j,i)^{th}$ entries equal to r and 0 otherwise. For $1 \leq i \leq j \leq n$ we define:

$$\mathcal{X}_{i,j}(r) = I_{2n} + \begin{pmatrix} 0 & 0 \\ s\epsilon_{i,j}(r) & 0 \end{pmatrix}, \quad \mathcal{Y}_{i,j}(r) = I_{2n} + \begin{pmatrix} 0 & s\epsilon_{i,j}(r) \\ 0 & 0 \end{pmatrix}.$$

For $1 \leq i, j \leq n$ with $i \neq j$ we define:

$$\mathcal{Z}_{i,j}(r) = I_{2n} + \begin{pmatrix} \epsilon_{i,j}(r) & 0 \\ 0 & -\epsilon_{i,j}(r) \end{pmatrix}.$$

For $1 \leq i < n$

$$\mathcal{W}_i(r) = I_{2n} + \begin{pmatrix} \beta_i(r) & 0 \\ 0 & -\beta_i(r) \end{pmatrix}.$$

Finally,

$$\mathcal{U}_1(r) = I_{2n} + \begin{pmatrix} \epsilon_{1,1}(r) & \epsilon_{1,1}(r) \\ -\epsilon_{1,1}(r) & -\epsilon_{1,1}(r) \end{pmatrix}.$$

The following theorem gives a nice description of $\mathrm{Sp}_{2n}(\mathbb{Z})[p]$ as a group generated by the matrices above [15, Lemma 5.4].

Theorem 8.1 (Church-Putman)**.** *For $n \geq 2$ and for a prime number $p \geq 2$ the congruence subgroup $\mathrm{Sp}_{2n}(\mathbb{Z})[p]$ is generated by the set*

$$\mathcal{S} = \{\mathcal{X}_{i,j}(p), \mathcal{Y}_{i,j}(p), \mathcal{Z}_{i,j}(p), \mathcal{W}_i(p), \mathcal{U}_1(p)\}$$

where i, j are indices defined as above.

We prove the lemma below, since no concise proof was found. In Particular, we use the generators of Theorem 8.1 to prove that $\mathrm{Sp}_{2n}(\mathbb{Z}/b)$ can be expressed as a quotient of some congruence subgroup of $\mathrm{Sp}_{2n}(\mathbb{Z})$ when b is a prime number.

Lemma 8.2. *Let a and b two distinct prime numbers. Then the following sequence is exact.*

$$1 \to \mathrm{Sp}_{2n}(\mathbb{Z})[ab] \to \mathrm{Sp}_{2n}(\mathbb{Z})[a] \to \mathrm{Sp}_{2n}(\mathbb{Z}/b) \to 1.$$

Proof. The map $\mathrm{Sp}_{2n}(\mathbb{Z})[a] \to \mathrm{Sp}_{2n}(\mathbb{Z}/b)$ sends every matrix $A \in \mathrm{Sp}_{2n}(\mathbb{Z})[a]$ into its $\mathrm{mod}(b)$ reduction. First, we prove the surjectivity of the latter map. The generators of $\mathrm{Sp}_{2n}(\mathbb{Z}/b)$ are $\mathcal{X}_{i,j}(1) \bmod(b)$ and $\mathcal{Y}_{i,j}(1) \bmod(b)$ where $1 \leq i < j \leq n$. Define n to be the solution of the equation $an \equiv 1 \bmod(b)$. Then, $\mathcal{X}_{i,j}(a)^n \equiv \mathcal{X}_{i,j}(1) \bmod(b)$ and $\mathcal{Y}_{i,j}(a)^n \equiv \mathcal{Y}_{i,j}(1) \bmod(b)$. This proves the surjectivity of the reduction map. The kernel of this reduction map contains matrices which satisfy $I_{2n} + aA \equiv I_{2n} \bmod(b)$. But since a and b are relatively primes, the latter equivalence holds if and only if $A = bB$ when B is a symplectic matrix. □

The following proposition gives a useful decomposition of $\mathrm{Sp}_{2n}(\mathbb{Z}/m)$ [48, Theorem 5].

Proposition 8.3 (Newman-Smart)**.** *Let $m \in \mathbb{N}$ and write $m = p_1^{k_1} p_2^{k_2} ... p_l^{k_l}$, where $p_i^{k_i}$ are powers of prime numbers. Then*

$$\mathrm{Sp}_{2n}(\mathbb{Z}/m) = \bigoplus_{i=1}^{l} \mathrm{Sp}_{2n}(\mathbb{Z}/p_i^{k_i}).$$

Newman-Smart also proved that the abelian group $\mathfrak{sp}_{2n}(\mathbb{Z}/l)$ can be expressed as a quotient of congruence subgroups of $\mathrm{Sp}_{2n}(\mathbb{Z})$, [48, Theorem 7].

Proposition 8.4 (Newman-Smart)**.** *Let $l, m \geq 2$ such that l divides m. Then we have the following isomorphism.*

$$\mathrm{Sp}_{2n}(\mathbb{Z})[m]/\mathrm{Sp}_{2n}(\mathbb{Z})[ml] \cong \mathfrak{sp}_{2n}(\mathbb{Z}/l).$$

Lemma 8.2 and Propositions 8.3 and 8.4 play crucial role in the rest of this chapter, in which we explore the structure of congruence subgroups of braid groups.

8.2 Kernel of the symplectic representation and certain congruence subgroups

In this section we study the kernel of the homomorphism

$$B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/m) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} & \text{if } b = 2, \end{cases}$$

where m is a positive integer, and g is an integer greater or equal to 1. We denote by $B_{2g+b}[m]$ the kernel of the homomorphisms above. Precisely, we study the kernel of this homomorphism, where m is a prime or $m = 1, 4$. The main purpose of this Section is Theorem 8.9.

8.2.1 Hyperelliptic Torelli

Consider the map

$$\rho : B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} & \text{if } b = 2, \end{cases}$$

defined in Section 7.2. The kernel of ρ is denoted by $\mathcal{BI}_{2g+b}$, where the notation stands for *braid Torelli* group. If we identify B_{2g+b} with $\mathrm{Mod}(\Sigma_{0,2g+b})$ (the mapping class group of a disc with $2g+b$ punctures), then we have that $\mathcal{BI}_{2g+b}$ is generated by squares of

Dehn twists around curves surrounding an odd number of punctures [13, Theorem A].

We recall from Section 3.2 that $\mathcal{I}(\Sigma_g^b)$ is the subgroup of $\mathrm{Mod}(\Sigma_g^b)$ acting trivially on $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$, when $b = 0, 1$, and $\mathcal{I}(\Sigma_g^2)$ is the subgroup of $\mathrm{Mod}(\Sigma_g^2)$ acting trivially on $\mathrm{H}_1^P(\Sigma_g^2)$. We also recall from Section 4.2 that $\mathrm{SMod}(\Sigma_g^b) < \mathrm{Mod}(\Sigma_g^b)$ consists of mapping classes that commute with a hyperelliptic involution. We define the hyperelliptic Torelli to be $\mathcal{SI}(\Sigma_g^b) = \mathrm{SMod}(\Sigma_g^b) \cap \mathcal{I}(\Sigma_g^b)$ where $b = 0, 1, 2$. Since $\mathcal{SI}(\Sigma_g^b) < \mathcal{I}(\Sigma_g^b)$ the hyperelliptic Torelli acts trivially on $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z})$ if $b = 0, 1$ and $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$ if $b = 2$. The next theorem was proved by Brendle-Margalit-Putman [13, Theorem A].

Theorem 8.5 (Brendle-Margalit-Putman)**.** *For $g \geq 0$ the group $\mathcal{SI}(\Sigma_g)$ is generated by Dehn twists about separating symmetric (fixed under the action of the hyperelliptic involution ι) simple closed curves in Σ_g.*

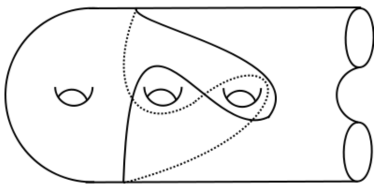


Figure 8.1: The element T_γ is a generator of $\mathcal{SI}(\Sigma_3^2)$.

For $b = 1, 2$, recall the isomorphism $B_{2g+b} = \mathrm{Mod}(\Sigma^1_{0,2g+b}) \to \mathrm{SMod}(\Sigma_g^b)$ defined by $\sigma_i \mapsto T_{c_i}$, where σ_i is a half-twist of the disc $\Sigma^1_{0,2g+b}$, and T_{c_i} is a Dehn Twist about curves depicted in Figure 4.10. Consider a curve $c \in \Sigma^1_{0,2g+b}$, surrounding an odd number of punctures. Then T_c^2 is mapped into a Dehn twist about a symmetric separating simple closed curve in Σ_g^b. By Theorem 8.5 we deduce that $\mathcal{SI}(\Sigma_g^b)$ is also generated by Dehn twists about symmetric separating simple closed curves.

8.2.2 Level 2 and 4 braid congruence subgroups

Here we describe the level 2 and 4 congruence subgroups of braid groups, namely $B_{2g+1}[m] = \ker(B_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z}/m))$, and $B_{2g+2}[m] = \ker(B_{2g+2} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}})$, where $m = 2, 4$. Recall that $(\mathrm{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}}$ denotes the stabilizer subgroup of the vector y_{g+1} (see Figure 8.2). If $m = 2$ we show that $B_{2g+b}[2] \cong PB_{2g+b}$, and if $m = 4$ we show that $B_{2g+b}[4] \cong PB^2_{2g+b}$, where $PB^2_{2g+b} = \{a^2 \mid a \in PB_{2g+b}\}$.

The level 2 braid congruence subgroups. Here we prove that $B_n[2] = PB_n$. The following construction was introduced by Arnol'd [4]. Consider the two-fold branched

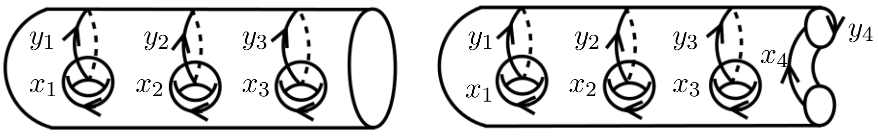


Figure 8.2: Standard generators for $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$, and $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$.

cover $\phi : \Sigma_g^b \to \Sigma_{0,2g+b}$ where $g \geq 1$, $b = 1, 2$. We denote by B the branched points of Σ_g^b, and by $\phi(B)$ the branched points of $\Sigma_{0,2g+b}$. We fix the following notation:

$$\begin{array}{lll} \Sigma & := & \Sigma_g^b, \\ D & := & \Sigma_{0,2g+b}, \\ \Sigma' & := & \Sigma_g^b \setminus B, \\ D' & := & \Sigma_{0,2g+b} \setminus \phi(B). \end{array}$$

Our aim is to define a monomorphism $\Phi : \mathrm{H}_1(\Sigma, \mathbb{Z}/2) \hookrightarrow \mathrm{H}_1(D', \mathbb{Z}/2)$. We need Φ is because we want to define a representation

$$B_{2g+b} \to \mathrm{Aut}(\mathrm{H}_1(\Sigma, \mathbb{Z}/2)) \hookrightarrow \mathrm{Aut}(\mathrm{H}_1(D', \mathbb{Z}/2)).$$

The map ϕ induces a map $\phi' : \Sigma_g^b \setminus B \to \Sigma_{0,2g+b} \setminus \phi(B)$. We have the following exact diagram

$$\begin{tikzcd} \mathrm{H}_2(\Sigma/\Sigma', \mathbb{Z}/2) \arrow[r, "\partial"] \arrow[d, "0"] & \mathrm{H}_1(\Sigma', \mathbb{Z}/2) \arrow[r, "i_*"] \arrow[d, "\phi'_*"] & \mathrm{H}_1(\Sigma, \mathbb{Z}/2) \arrow[r] \arrow[d, "\phi_*"] \arrow[dl, "\Phi"] & \mathrm{H}_1(\Sigma/\Sigma', \mathbb{Z}/2) \\ \mathrm{H}_2(D \setminus D', \mathbb{Z}/2) \arrow[r, "\partial"] & \mathrm{H}_1(D', \mathbb{Z}/2) \arrow[r] & \mathrm{H}_1(D, \mathbb{Z}/2). & \end{tikzcd}$$

The groups $\mathrm{H}_1(D, \mathbb{Z}/2)$ and $\mathrm{H}_1(\Sigma/\Sigma', \mathbb{Z}/2)$ are trivial because D/D' and Σ/Σ' are bundles of 2-spheres, and hence i_* is surjective. Also, the map $\mathrm{H}_2(\Sigma \setminus \Sigma', \mathbb{Z}/2) \to \mathrm{H}_2(D \setminus D', \mathbb{Z}/2)$ is induced by a degree 2 map, hence is a trivial mod(2) map [4, Lemma 1]. Now consider Φ. Every mod(2) cycle γ in $\mathrm{H}_1(\Sigma, \mathbb{Z}/2)$ can be modified by a homotopy so that it avoids intersections with points in B. But since i_* is surjective, there exists a $\beta \in \mathrm{H}_1(\Sigma', \mathbb{Z}/2)$ such that $i_*(\beta) = \gamma$, and $\phi'_*(\beta) \in \mathrm{H}_1(D', \mathbb{Z}/2)$. We define $\Phi(\gamma) = \phi'_*(i_*^{-1}(\gamma))$. The map Φ is well defined, since for every $k \in \mathrm{Ker}(i_*)$, there exists an $l \in \mathrm{H}_2(\Sigma \setminus \Sigma', \mathbb{Z}/2)$ such that $\partial(l) = k$, and since the left square diagram is commutative we get $\phi'_*(k) = \phi'_*(\partial(l)) = \partial(0(l)) = 0$.

Let μ_i be loops in D', such that, $\mu_i \neq \mu_j$ for $i \neq j$, and each μ_i surrounds a single point in $\phi(B)$. The group $\mathrm{H}_1(D', \mathbb{Z}/2)$ is generated by μ_i with relations $2\mu_i = \sum_{i=1}^{2g+b} \mu_i = 0$.

Consider the generators y_i, x_i of $\mathrm{H}_1(\Sigma, \mathbb{Z}/2)$ as indicated in Figure 8.2. We deduce $\Phi(x_i) = \mu_{2i+1} + \mu_{2i}$, $\Phi(y_i) = \sum_{j=1}^{2i+2} \mu_j$. Then the map Φ is injective. Thus, we get a representation

$$B_{2g+b} \to \mathrm{Aut}(\mathrm{H}_1(D', \mathbb{Z}/2)),$$

where the image of B_{2g+b} is the symmetric group S_{2g+b} [4, Lemma 2]. Therefore, the kernel of the latter representation is just the pure braid group PB_{2g+b}, and we have $PB_{2g+b} = B_{2g+b}[2]$.

The level 4 braid congruence subgroup. This paragraph is based on Brendle-Margalit's paper [12, Sections 2,3,4]. Consider the representation

$$\rho_4 : B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/4) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

We want to characterize the kernel $B_{2g+b}[4]$ of ρ_4. Since 4 is a multiple of 2 we have that $B_{2g+b}[4] < B_{2g+b}[2] = PB_{2g+b}$. The following maps are surjective [12, Theorem 3.3, Lemma 3.4]

$$\rho' : PB_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z})[2] \to \mathfrak{sp}_{2g}(\mathbb{Z}/2) & \text{if } b = 1 \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z})[2])_{y_{g+1}} \to \mathrm{Ann}(y_{g+1}) & \text{if } b = 2. \end{cases}$$

It follows that the kernel of ρ' is $B_{2g+b}[4] = PB^2_{2g+b}$ [12, Theorem 3.1]. We also note that PB^2_{2g+b} is the kernel of the map $PB_{2g+b} \to \mathrm{H}_1(PB_{2g+b}, \mathbb{Z}/2)$.

We recall from Chapter 4 that $\mathrm{Mod}(\Sigma^1_{0,2g+b}, \phi(B)) = PB_{2g+b}$. For every simple closed curve c in $\Sigma^1_{0,2g+b}$ we denote by T_c a Dehn twist about c. We set

$$\mathcal{T}(m) = \{T_c^m \mid T_c \in \mathrm{Mod}(\Sigma^1_{0,2g+b})\}.$$

We have that $\mathcal{T}(2) = B_{2g+b}[4]$ [12, Proposition 4.1]. Therefore, we get the following equalities:

$$\mathcal{T}(2) = B_{2g+b}[4] = PB^2_{2g+b}.$$

8.2.3 Level p congruence subgroups

The purpose of this section is the characterization of the group $B_{2g+b}[p]$ when p is prime. Since $B_{2g+b} \cong \mathrm{SMod}(\Sigma^b_g)$, it is convenient to study the kernel of the map

$$\mathrm{SMod}(\Sigma^b_g) \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/p) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

and we denote the map again by ρ_p. Also, we denote the kernel of ρ_p by $B_{2g+b}[p]$.

A'Campo proved that the homomorphism ρ_p is surjective, by using techniques of algebraic geometry [2, Theorem 1 (1)]. Later Assion gave a presentation for $\mathrm{Sp}_{2g}(\mathbb{Z}/3)$ and $(\mathrm{Sp}_{2g+2}(\mathbb{Z}/3))_{y_{g+1}}$ as quotients of braid groups [6]. Wajnryb improved the result of Assion and generalized it for any prime number greater than 2 [56, Theorem 1]. We begin with the theorem of Wajnryb.

Theorem 8.6 (Wajnryb)**.** *Consider the curves c_i depicted in Figure 4.10. Let G_{2g+b} be a group with generators $T_{c_1}, ..., T_{c_{2g+b-1}}$ and relations $R1$ to $R6$ as follows.*

R1. $T_{c_i}T_{c_{i+1}}T_{c_i} = T_{c_{i+1}}T_{c_i}T_{c_{i+1}}$,

R2. $[T_{c_i}, T_{c_j}] = 1, \quad \text{for } |i-j| > 1$,

R3. $T_{c_1}^p = 1$,

R4. $(T_{c_1}T_{c_2})^6 = 1, \quad \text{for } p > 3$,

R5. $T_{c_1}^{(p-1)/2}T_{c_2}^4T_{c_1}^{-(p-1)/2} = T_{c_2}^2T_{c_1}T_{c_2}^{-2}, \quad \text{for } p > 3$,

R6. $(T_{c_1}T_{c_2}T_{c_3})^4 = AT_{c_1}^2A^{-1}$, for $n > 4$, where $A = T_{c_4}T_{c_3}^2T_{c_4}T_{c_2}^{(p-1)/2}T_{c_3}^{-1}T_{c_2}$.

Then G_{2g+1} is isomorphic to $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$, and G_{2g+2} is isomorphic to $(\mathrm{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{n+1}}$.

As a consequence of Theorem 8.6 we obtain elements of $\mathrm{SMod}(\Sigma_g^b)$ which normally generate $B_{2g+b}[p]$. In the rest of the section we examine the relations $R3, R4, R5, R6$ of Theorem 8.6 in order to give a better description for the generators of $B_{2g+b}[p]$. We note that relations $R1$ and $R2$ are the defining relations in the presentation of the braid group.

We denote by $[c_i]$ the homology class of c_i, and by $T_{[c_i]}$ the transvection associated to the Dehn twist T_{c_i} under the map

$$\mathrm{SMod}(\Sigma_g^b) \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/p) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

By definition, the action of a transvection $T_{[c]}^m$ on an element $u \in \mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ (respectively $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z})$) is defined to be $T_{[c]}^m(u) = [u] + m\hat{i}(u, [c])[c]$, where $\hat{i}$ stands for the algebraic intersection number.

R3: Powers of Dehn twists. The p^{th} powers of Dehn twists about symmetric non-separating simple closed curves are easy to check by looking at their image in the symplectic group. The symplectic representation sends $T_{c_1}^p$ into the following matrix:

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \oplus I,$$

where I stands for the identity matrix of dimension depending on g and b (see Section 7.1.3). The mod(p) reduction of the matrix above is the identity. Moreover, every Dehn twist about a non-separating curve is conjugate to T_{c_1}. As a consequence, every Dehn twist in $\mathrm{SMod}(\Sigma_g^b)$ raised to the power of p lies in $B_n[p]$.

R4: Symmetric separating Dehn twists. By the chain relation the element $(T_{c_1}T_{c_2})^6$ can be represented by a Dehn twist T_γ, where γ is the symmetric separating curve bounding the genus 1 subsurface of Σ_g^b as indicated in Figure 8.3 [20, Proposition 4.12]. We have that $T_\gamma \in \mathcal{SI}(\Sigma_g^b) \subset B_{2g+b}[p]$. We can generalize the relation R4 by considering a symmetric separating curve δ of a genus k subsurface of Σ_g^b. By the chain relation there is a maximal chain of curves $a_1, ..., a_{2k}$ in the subsurface of genus k with boundary δ such that $(T_{a_1}...T_{a_{2k}})^{4k+2} = T_\delta$. Since for every symmetric separating curve δ in Σ_g^b and $T_\delta \in B_{2g+b}[p]$ we have that $(T_{a_1}...T_{a_{2k}})^{4k+2} \in B_{2g+b}[p]$.

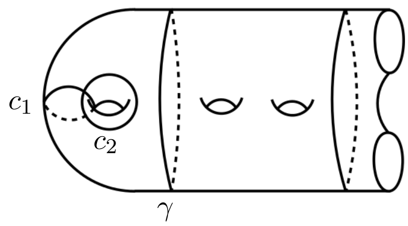


Figure 8.3: The curve γ that bound a surface of genus 1.

R5: Even-chain maps. Relation R5 of Theorem 8.6 does not seem to have a nice topological description. Our aim here is to find such a nice topological interpretation. In Lemma 8.7 we use the Tietze transformations in order to insert the relation $(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = (T_{c_1}T_{c_2})^3$ into R5 of Theorem 8.6. Then we explain why $(T_{c_1}T_{c_2})^3(T_{c_1}^{(p+1)/2}T_{c_2}^4)^{-2}$ lies in $B_{2g+b}[p]$.

Lemma 8.7. *The relation* $T_{c_1}^{(p-1)/2}T_{c_2}^4T_{c_1}^{-(p-1)/2} = T_{c_2}^2T_{c_1}T_{c_2}^{-2}$ *is equivalent to the relation* $(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = (T_{c_1}T_{c_2})^3$ *in* $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$ *(respectively* $(\mathrm{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}}$*).*

Proof. We have that $(T_{c_1}T_{c_2})^3 = T_{c_1}T_{c_2}^2T_{c_1}T_{c_2}^2$. Then

$$T_{c_1}^{(p-1)/2}T_{c_2}^4T_{c_1}^{-(p-1)/2} = T_{c_1}^{-1}(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2T_{c_2}^{-4} = T_{c_2}^2T_{c_1}T_{c_2}^{-2}.$$

On the other hand

$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = T_{c_1}T_{c_1}^{(p-1)/2}T_{c_2}^4T_{c_1}^{-(p-1)/2}T_{c_2}^4 = T_{c_1}T_{c_2}^2T_{c_1}T_{c_2}^2.$$

□

Now we examine the relation $(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = (T_{c_1}T_{c_2})^3$. For $i = 1, 2$ we have that $(T_{c_1}T_{c_2})^3([c_i]) = -[c_i]$, where $[c_i]$ stands for the homology class of c_i. Thus, the homeomorphism $(T_{c_1}T_{c_2})^3$ acts as the hyperelliptic involution on the subsurface bounded by the boundary of the chain $ch(c_1, c_2)$ (see Figure 8.3). We can see that $(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2$ acts as the hyperelliptic involution mod(p) in the subspace of $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z}/p)$, (resp $\mathrm{H}_1^P(\Sigma_g^2, \mathbb{Z}/p)$) spanned by the homology classes $[c_1], [c_2]$. Indeed, we have

$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2([c_1]) = -8p[c_2] + (4p^2 + 2p - 1)[c_1] \equiv -[c_1] \bmod(p),$$
$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2([c_2]) = 2p\frac{p+1}{2}[c_1] - (2p + 1)[c_2] \equiv -[c_2] \bmod(p)$$

We generalize Relation 5. For k even, consider any chain $ch(a_1, a_2, ..., a_k)$ such that $T_{a_i} \in \mathrm{SMod}(\Sigma_{g,b})$ for all $i \leq k$. Choose an $f \in \mathrm{SMod}(\Sigma_g^b)$ such that $f([a_i]) = -[a_i]$. Then $(T_{a_1}...T_{a_k})^{k+1}f^{-1} \in B_{2g+b}[p]$. We call this type of element an *even-chain map.*

R6: odd-chain maps. We describe a generalized version of $(T_{c_1}T_{c_2}T_{c_3})^4(AT_{c_1}^{-2}A^{-1})$. Let A_1 be the trivial homeomorphism in $\mathrm{SMod}(\Sigma_g^b)$. For k odd, and $k \geq 3$, define

$$A_k = T_{c_{k+1}}T_{c_k}^2T_{c_{k+1}}T_{c_{k-1}}^{(p-1)/2}T_{c_k}^{-1}T_{c_{k-1}}A_{k-2}.$$

First, we deal with the case $b = 1$. (For $b = 2$ the process is exactly the same.) Consider the symplectic bases $\{y_i, x_i\}$ for $\mathrm{H}_1(\Sigma_g^1, \mathbb{Z})$ depicted on Figure 8.2.

Lemma 8.8. *For k odd, we have that $A_kT_{[c_1]}A_k^{-1} = T_{[y_{(k+1)/2}]}$ in $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$.*

Note that if $k = 3$, then $T_{[y_2]} = T_{[d_3]}$.

Proof. We need to prove that $A_k([c_1]) \equiv [c_1] + [c_3] + ... + [c_k] \in \mathrm{Sp}_{2g}(\mathbb{Z}/p)$. A direct calculation shows that $A_3([c_1]) = [c_1] + p[c_2] + [c_3] \equiv [c_1] + [c_3] \bmod(p)$. Assume that the theorem is true for $k - 2$, that is $A_{k-2}([c_1]) = [c_1] + [c_3] + ... + [c_{k-2}]$. Then $T_{c_{k+1}}T_{c_k}^2T_{c_{k+1}}T_{c_{k-1}}^{(p-1)/2}T_{c_k}^{-1}T_{c_{k-1}}([c_{k-2}]) = [c_{k-2}] + [c_k]$. The proof of the lemma follows. □

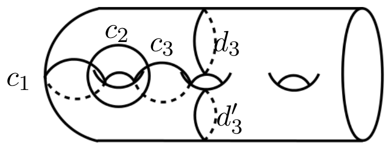


Figure 8.4: The chain relation of $R6$.

Let k be an odd integer, and consider also the odd chain $ch(c_1, c_2, ..., c_k)$. By the chain relation we have that $(T_{c_1}...T_{c_k})^{k+1} = T_{d_k}T_{d_k'}$, where $d_k = y_{(k+1)/2}$, and $[d_k] = [d_k'] = [y_{(k+)/2}]$ (see, for example, Figure 8.4). Thus, $(T_{[c_1]}...T_{[c_k]})^{k+1} = T^2_{[y_{(k+1)/2}]} \in \mathrm{Sp}_{2g}(\mathbb{Z}/p)$. On the other hand, according to Lemma 8.8 we have that $A_kT^2_{[c_1]}A_k^{-1} = T^2_{[y_{(k+1)/2}]} \in \mathrm{Sp}_{2g}(\mathbb{Z}/p)$. Hence, $(T_{c_1}...T_{c_k})^{k+1}A_kT_{c_1}^{-2}A_k^{-1} \in B_{2g+b}[p]$. Note that if $k = 3$, the element $(T_{c_1}...T_{c_k})^{k+1}A_kT_{c_1}^{-2}A_k^{-1}$ is the same one as in the relation 6 of Theorem 8.6.

We can describe a generalized version of $(T_{c_1}...T_{c_k})^{k+1}A_kT_{c_1}^{-2}A_k^{-1}$. Consider any odd chain $ch(a_1, a_2, ..., a_k)$, such that $T_{a_i} \in \mathrm{SMod}(\Sigma_g^1)$ for all $i \leq k$. Choose a homeomorphism $h \in \mathrm{SMod}(\Sigma_g^1)$ such that $h([a_1]) = [a_1] + [a_3] + ... + [a_k] \in \mathrm{Sp}_{2g}(\Sigma_g^1)$. Then we have that $(T_{a_1}...T_{a_k})^{k+1}hT_{a_1}^{-2}h^{-1} \in B_{2g+1}[p]$. If we consider $(T_{a_1}...T_{a_k})^{k+1}$ as the center of the subgroup K of $\mathrm{SMod}(\Sigma_g^b)$ generated by $T_{a_1}...T_{a_k}$, then $hT_{a_1}^{-2}h^{-1}$ is the center $\bmod (p)$ of the same group. Note that the choice of h is not unique. We call this type of element an *odd-chain map.*

Theorem 8.9. *If $p = 3$, then $B_{2g+b}[3]$ is generated by Dehn twists raised to the power of 3, and for $2g + b > 4$ by odd-chain maps. For $p > 3$ the subgroup $B_{2g+b}[p]$ of $\mathrm{SMod}(\Sigma_g^b)$ is generated by Dehn twists raised to the power of p, by symmetric separating curves, by even-chain maps, and for $2g + b > 4$ by odd-chain maps.*

The generating set in Theorem 8.9 is infinite. When $p = 3$ and $g = 1$ we can find a finite set of generators.

Theorem 8.10. *The group $B_3[3]$ is generated by four elements.*

Proof. Set $S = \{T_{c_1}^3, T_{c_2}^3, T_{c_2}T_{c_1}^3T_{c_2}^{-1}, T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}\}$. We denote by Γ the subgroup of $B_3[3]$ generated by S. We prove that if we conjugate elements of S by T_{c_1} or T_{c_2}, then the resulting elements lie in Γ. Since $B_3[3]$ is normally generated by S and since S generates a normal subgroup of B_3, then $\Gamma = B_3[3]$.

In the braid group we have the relation

$$T_{c_j}T_{c_{j-1}}...T_{c_i}^3...T_{c_{j-1}}^{-1}T_{c_j}^{-1} = T_{c_i}^{-1}T_{c_{i+1}}^{-1}...T_{c_j}^3...T_{ci+1}T_{c_i}$$

We prove the theorem in three steps.

Step 1: Conjugates of $T_{c_1}^3, T_{c_2}^3$:

$$\begin{aligned} T_{c_2}^{-1}T_{c_1}^3T_{c_2} = T_{c_2}^{-3}T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}T_{c_2}^3 \in \Gamma \\ T_{c_1}^{-1}T_2^3T_{c_1} = T_2T_{c_1}^3T_2^{-1} \in \Gamma \\ T_{c_1}T_{c_2}^3T_{c_1}^{-1} = T_{c_2}^{-1}T_{c_1}^3T_{c_2} = T_{c_2}^{-3}T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}T_{c_2}^3 \in \Gamma. \end{aligned}$$

Step 2: Conjugates of $T_{c_2}T_{c_1}^3T_{c_2}^{-1}$:

$$\begin{aligned} T_{c_1}T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1}^{-1} = T_{c_2}^3 \in \Gamma \\ T_{c_1}^{-1}T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1} = T_{c_1}^{-2}T_{c_2}^3T_{c_1}^2 = T_{c_1}^{-3}(T_{c_1}T_{c_2}^3T_{c_1}^{-1})T_{c_1}^3. \end{aligned}$$

The latter is in Γ by step 1.

Step 3: Conjugates of $T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}$:

$$\begin{aligned} T_{c_1}^{-1}T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}T_{c_1} = T_{c_1}^{-1}T_{c_2}^3T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_2}^{-3}T_{c_1} = \\ (T_{c_1}^{-1}T_{c_2}^3T_{c_1})(T_{c_1}^{-1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1})(T_1^{-1}T_{c_2}^{-3}T_{c_1}) \end{aligned}$$

The elements $(T_{c_1}^{-1}T_{c_2}^3T_{c_1}), (T_{c_1}^{-1}T_{c_2}^{-3}T_{c_1})$ are in Γ by step 1.

$$T_{c_1}^{-1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1} = T_{c_2}^3$$

Finally, since $T_{c_2}^2T_{c_1}^3T_{c_2}^{-2} = T_{c_2}^3T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_2}^{-3}$, it suffices to check that $T_{c_1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1}^{-1}$ is in Γ. But we have that

$$T_{c_1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1}^{-1} = T_{c_1}^2T_{c_2}^3T_{c_1}^{-2} = T_{c_1}^3T_{c_1}^{-1}T_2^3T_{c_1}T_{c_1}^{-3} = T_{c_1}^3T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1}^{-3} \in \Gamma.$$

This proves the theorem. □

It is well known that every finite index subgroup of a finitely generated group, is finitely generated [44, Corollary 2.7.1]. In Theorem 8.10 we found a finite generating set. This result enables us to seek for finite generating sets for $B_n[3]$, when $n > 3$.

8.3 Level m congruence subgroups

For $i \in \mathbb{N}$, let p_i denote a prime number greater than 2. In this section we characterize $B_{2g+b}[m]$, where $m = 2p_1p_2...p_k$ and $m = 4p_1p_2...p_k$. Our strategy is to find a presentation for $PB_{2g+b}/B_{2g+b}[m]$. We recall that $\mathrm{H}_1(PB_{2g+b}, \mathbb{Z}/2)$ is $\mathfrak{sp}_{2g}(\mathbb{Z}/2)$, if $b = 1$ and

$\mathrm{Ann}(y_{g+1})$ if $b = 2$, where $\mathrm{Ann}(y_{g+1}) = \{h \in \mathfrak{sp}_{2g+2}(\mathbb{Z}/2) \mid h(y_{g+1}) = 0\}$ [12]. The generators of B_{2g+b} are denoted by σ_i and the generators of PB_{2g+b} are denoted by $a_{i,j}$ as in Chapter 4.

Lemma 8.11. *For $m = 2p_1p_2...p_k$, where $p_i \geq 3$ are prime numbers, we have*

$$PB_{2g+b}/B_{2g+b}[m] = \begin{cases} \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i) & \text{if } b = 1, \\ \bigoplus_{i=1}^{k} (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

Proof. For the first part of the lemma, we set $m = 2p_1p_2...p_k$. We have the map

$$\rho_m : B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/m) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

with kernel $B_{2g+b}[m]$. By Lemma 8.3 we know that

$$\mathrm{Sp}_{2g}(\mathbb{Z}/m) = \mathrm{Sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i).$$

If we restrict to the pure braid group, then the image of the map $PB_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z})$ is the group $\mathrm{Sp}_{2g}(\mathbb{Z})[2]$, (see [12, Theorem 3.3]). Furthermore, by Lemma 8.2 we have that the map $\mathrm{Sp}_{2g}(\mathbb{Z})[2] \to \mathrm{Sp}(\mathbb{Z}/p_i)$ is surjective. Thus, the image of the map

$$\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/m) = \mathrm{Sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i),$$

after we restrict to $\mathrm{Sp}_{2g}(\mathbb{Z})[2]$, is the group $\bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i)$. Hence, have a short exact sequence

$$1 \to B_{2g+1}[m] \to PB_{2g+1} \to \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i) \to 1.$$

Likewise, since the image of the map $PB_{2g+2} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$ is $(\mathrm{Sp}_{2g+2}(\mathbb{Z})[2])_{y_{g+1}}$ (see [12, Theorem 3.3]), and since $(\mathrm{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} < \mathrm{Sp}_{2g+2}(\mathbb{Z}/m)$, we can apply Lemma 8.3 and end up with the following exact sequence.

$$1 \to B_{2g+2}[m] \to PB_{2g+2} \to \bigoplus_{i=1}^{k} (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} \to 1.$$

This completes the proof. $\square$

In the following statement we slightly generalize Lemma 8.11.

Lemma 8.12. *For $m = 4p_1p_2...p_k$, where $p_i \geq 3$ are prime numbers , we have*

$$PB_{2g+b}/B_{2g+b}[m] = \begin{cases} \mathfrak{sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i) & \text{if } b = 1, \\ \mathrm{Ann}(e) \bigoplus_{i=1}^{k} (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

Proof. Consider now $m = 4p_1p_2...p_k$. By Lemma 8.3 we have that

$$\mathrm{Sp}_{2g}(\mathbb{Z}/m) = \mathrm{Sp}_{2g}(\mathbb{Z}/4) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i).$$

We want to characterize the image of the map

$$B_{2g+b} \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/4) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}} \bigoplus_{i=1}^{k} (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

For $b = 1$ we only need to characterize the image of the restriction of the map above to PB_{2g+b}. In particular, we want to compute the image of the map $PB_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z}/4)$. We know that the image of the map $PB_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z})$ is $\mathrm{Sp}_{2g}(\mathbb{Z})[2]$. Consider the inclusion

$$\mathrm{Sp}_{2g}(\mathbb{Z})[2] \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}).$$

We quotient the above inclusion by $\mathrm{Sp}_{2g}(\mathbb{Z})[4]$, and we get the following inclusion:

$$\mathfrak{sp}_{2g}(\mathbb{Z}/2) \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/4).$$

We finally have

$$PB_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z})[2] \to \mathfrak{sp}_{2g}(\mathbb{Z}/2) < \mathrm{Sp}_{2g}(\mathbb{Z}/4).$$

Hence, the image of the map $PB_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z}/4)$ is the abelian group $\mathfrak{sp}_{2g}(\mathbb{Z}/2)$. Thus, we have

$$PB_{2g+b}/B_{2g+b}[m] \cong \mathfrak{sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \mathrm{Sp}_{2g}(\mathbb{Z}/p_i).$$

For $b = 2$, the maps

$$PB_{2g+2} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z})[2])_{y_{g+1}} \to \mathrm{Ann}(y_{g+1})$$

are both surjective, [12, Lemma 3.5]. But $\mathrm{Ann}(y_{g+1}) < (\mathrm{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}}$, and thus, the image of the map

$$PB_{2g+2} \to (\mathrm{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}}$$

is the group $\mathrm{Ann}(y_{g+1})$. Thus, we get

$$PB_{2g+2}/B_{2g+2}[m] \cong \mathrm{Ann}(y_{g+1}) \bigoplus_{i=1}^{k} (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}}.$$

This completes the proof. $\square$

In order to find generators for $B_{2g+1}[m]$, it suffices to find a presentation for $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$ in terms of pure braids. In the next proposition we prove that $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$ admits a presentation as a quotient of the pure braid group over some relations. These new relations are the generators for $B_{2g+1}[2p]$.

Proposition 8.13. *Fix a prime number p, and put $p = 2k+1$. Let H_n be the group with generators $\{a_{i,j}\}$ with the defining relations*

PR1. $a^k_{i,i+1}a^k_{i+1,i+2}a^k_{i,i+1} = a^k_{i+1,i+2}a^k_{i,i+1}a^k_{i+1,i+2}$,

PR2. $a^p_{i,j} = 1$,

PR3. $(a^{k+1}_{1,2}a^{k+1}_{2,3})^6 = 1 \,\mathrm{for}\, p > 3$,

PR4. $a^{-1}_{r,s}a_{i,j}a_{r,s} = a_{i,j}$, $1 \le r < s < i < j \le n \,\mathrm{or}\, 1 \le i < r < s < j \le n$,

PR5. $a^{-1}_{r,s}a_{i,j}a_{r,s} = a_{r,j}a_{i,j}a^{-1}_{r,j}$, $1 \le r < s = i < j \le n$,

PR6. $a^{-1}_{r,s}a_{i,j}a_{r,s} = (a_{i,j}a_{s,j})a_{i,j}(a_{i,j}a_{s,j})^{-1}$, $1 \le r = i < s < j \le n$,

PR7. $a^{-1}_{r,s}a_{i,j}a_{r,s} = (a_{r,j}a_{s,j}a^{-1}_{r,j}a^{-1}_{s,j})a_{i,j}(a_{r,j}a_{s,j}a^{-1}_{r,j}a^{-1}_{s,j})^{-1}$, $1 \le r < i < s < j \le n$,

PR8. $a_{i,j} = a^{k+1}_{j-1,j}a^{k+1}_{j-2,j-1}...a_{i,i+1}a^k_{i+1,i+2}...a^k_{j-1,j}$, $1 < |i-j| \le n$,

PR9. $(a^{k+1}_{1,2}a^{k+1}_{2,3})^3 = (a^{2k^2}_{1,2}a^2_{2,3})^2 \,\mathrm{for}\, p > 3$,

PR10. $(a^{k+1}_{1,2}a^{k+1}_{2,3}a^{k+1}_{3,4})^4 = Ba_{1,2}B^{-1}$, where $B = a^{k+1}_{4,5}a_{3,4}a^{k+1}_{4,5}a^{2k^2}_{2,3}a^k_{3,4}a^{k+1}_{2,3}$, for $n > 4$.

If $n = 2g+1$ then H_n is isomorphic to $\mathrm{Sp}_{2g}(\mathbb{Z}/p)$. On the other hand if $n = 2g+2$, then H_n is isomorphic to $\mathrm{Sp}_{2g+2}(\mathbb{Z}/p)_{y_{g+1}}$.

Note that relations $PR4$, $PR5$, $PR6$, $PR7$ are relations in the presentation of the pure braid group given in Chapter 4. We begin with the group G_n defined in Theorem 8.6, and using Tietze transformations, we obtain the presentation of H_n.

Proof. By Theorem 8.6 the group G_n has the following presentation:

$$G_n = \langle \sigma_i |\, R1, R2, R3, R4, R5, R6 \rangle,$$

where $1 \le i < 2g+b$. Let $a_{i,j} = \sigma_{j-1}...\sigma_{i+1}\sigma_i^2\sigma^{-1}_{i+1}...\sigma^{-1}_{j-1}$ and denote this relation by $PR11$. Then include $PR11$ into the presentation of G_n and add the generator $a_{i,j}$ to obtain

$$\langle \sigma_i, a_{i,j} |\, R1, R2, R3, R4, R5, R6, PR11 \rangle.$$

Since PB_n is a subgroup of B_n, this means that $R1$ and $R2$ can be used to deduce the relations $PR4$, $PR5$, $PR6$, $PR7$.

$$\langle \sigma_i, a_{i,j} | \, R1, R2, R3, R4, R5, R6, PR4, PR5, PR6, PR7, PR11 \rangle.$$

The relation $R2$ can be deduced by $PR11$ and $R3$ and $PR4$

$$\langle \sigma_i, a_{i,j} | \, R1, R3, R4, R5, R6, PR2, PR4, PR5, PR6, PR7, PR11 \rangle.$$

We derive two more relations from $PR11$ and $R3$.

$$\sigma_i = a_{i,i+1}^{k+1}, \quad \sigma_i^{-1} = a_{i,i+1}^{k}.$$

Then $PR1$ is equivalent to $R1$, $PR2$ is equivalent to $R3$, $PR3$ is equivalent to $R4$, $PR9$ is equivalent to $R5$, $PR10$ is equivalent to $R6$, and $PR11$ is equivalent to $PR8$. In other words,

$$\langle \sigma_i, a_{i,j} | \, PR1, PR2, PR4, PR5, PR6, PR7, PR8, PR9, PR10, \sigma_i = a_{i,i+1}^{k+1}, \sigma_i^{-1} = a_{i,i+1}^{k} \rangle$$

Finally, for $1 \leq i < j \geq 2g+b$ we have that

$$\langle a_{i,j} | \, PR1, PR2, PR4, PR5, PR6, PR7, PR8, PR9, PR10 \rangle,$$

which is the presentation of H_n. □

As an application of Proposition 8.13, we can obtain generators for $B_{2g+b}[2p]$.

Corollary 8.14. *For $k = (p-1)/2$, the group $B_{2g+b}[2p]$ is normally generated by six types of elements:*

$$\begin{aligned}
a_{i,j}^{p}. \\
(a_{1,2}^{k+1} a_{2,3}^{k+1})^6. \\
(a_{1,2}^{2k^2} a_{2,3}^{2})^2 (a_{1,2}^{k+1} a_{2,3}^{k+1})^{-3}. \\
(a_{1,2}^{k+1} a_{2,3}^{k+1} a_{3,4}^{k+1})^4 B a_{1,2}^{-1} B^{-1} \\
a_{i,i+1}^{k} a_{i+1,i+2}^{k} a_{i,i+1}^{k} a_{i+1,i+2}^{-k} a_{i,i+1}^{-k} a_{i+1,i+2}^{-k}. \\
a_{j-1,j}^{k+1} a_{j-2,j-1}^{k+1} \ldots a_{i,i+1} a_{i+1,i+2}^{k} \ldots a_{j-1,j}^{k} a_{i,j}^{-1}.
\end{aligned}$$

Actually we can use Proposition 8.13 to find normal generators for any $B_n[m]$, where m is either $2p_1 \ldots p_k$ or $4p_1 \ldots p_k$ and $p_i \geq 3$ are prime numbers.

8.4 Symmetric quotients of congruence subgroups

If m is a multiple of k, then $B_n[m] \lhd B_n[k]$. In this Section we investigate some quotients $B_n[k]/B_n[m]$ for particular values of k, m. From Section 8.2.2 we know that $B_n[2] \cong PB_n$ and $B_n/B_n[2] \cong S_n$. The purpose of this section is to prove the following theorem.

Theorem 8.15. *The quotient $B_n[p]/B_n[2p]$ is isomorphic to S_n.*

Before we proceed to the proof of Theorem 8.15, we prove the following lemma.

Lemma 8.16. *The groups $B_n[2p]$ and $B_n[2] \cap B_n[p]$ are isomorphic.*

Proof. It is obvious that $B_n[2p] < B_n[2] \cap B_n[p]$. By Proposition 8.3 we have that $\mathrm{Sp}_{2g}(\mathbb{Z}/2p) = \mathrm{Sp}_{2g}(\mathbb{Z}/2) \oplus \mathrm{Sp}_{2g}(\mathbb{Z}/p)$. By the homomorphism $\rho : B_n \to \mathrm{Sp}_{2g}(\mathbb{Z}/2p)$ we deduce that $\rho(B_n[2] \cap B_n[p])$ is trivial. Hence, $B_n[2] \cap B_n[p] < B_n[2p]$. □

Now we can prove the main theorem of the section.

Proof of Theorem 8.15. Denote by s_i the transposition $(i, i+1)$, that is, the generators of S_n. We have the following presentation.

$$S_n = \left\langle s_1, ..., s_{n-1} \mid s_i^2 = 1, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, s_i s_j = s_j s_i \text{ when } |i-j| > 1 \right\rangle.$$

Consider the natural epimorphism $\tau : B_n \to S_n$ defined by $\tau(\sigma_i) = s_i$. Fix a prime number $p > 2$; then the restriction $\tau : B_n[p] \to S_n$ is a surjective homomorphism as well. Indeed, we have that $\tau(\sigma_i^p) = s_i^p = s_i$, and for any other generator $g \in B_n[p]$ we have $\tau(g) = 1$. Finally, $\ker(\tau) = B_n[2] \cap B_n[p] = B_n[2p]$ by Lemma 8.16. □

In Theorem 8.15 we computed quotients of $B_n[p]$ when p is prime. In the future, it would be interesting to examine quotients of $B_n[m]$ where $m = 2p_1...p_k$ or $m = 4p_1...p_k$ and p_i are prime numbers.

Bibliography

[1] C. A. Abad. Introduction to representations of braid groups. *arXiv preprint arXiv:1404.0724*, 2014.

[2] Norbert A'Campo. Tresses, monodromie et le groupe symplectique. *Comment. Math. Helv.*, 54(2):318–327, 1979.

[3] Susumu Ariki. Robinson-Schensted correspondence and left cells. In *Combinatorial methods in representation theory (Kyoto, 1998)*, volume 28 of *Adv. Stud. Pure Math.*, pages 1–20. Kinokuniya, Tokyo, 2000.

[4] V. I. Arnol′d. A remark on the branching of hyperelliptic integrals as functions of the parameters. *Funkcional. Anal. i Priložen.*, 2(3):1–3, 1968.

[5] E. Artin. Theorie der Zöpfe. *Abh. Math. Sem. Univ. Hamburg*, 4(1):47–72, 1925.

[6] J. Assion. Einige endliche Faktorgruppen der Zopfgruppen. *Math. Z.*, 163(3):291–302, 1978.

[7] Paolo Bellingeri and Sylvain Gervais. Surface framed braids. *Geom. Dedicata*, 159:51–69, 2012.

[8] Joan Birman and Tara Brendle. Braids: a survey. In *Handbook of knot theory*, pages 19–103. Elsevier B. V., Amsterdam, 2005.

[9] Joan S. Birman. *Braids, links, and mapping class groups.* Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974. Annals of Mathematics Studies, No. 82.

[10] Joan S. Birman and Hugh M. Hilden. On the mapping class groups of closed surfaces as covering spaces. In *Advances in the theory of Riemann surfaces (Proc. Conf., Stony Brook, N.Y., 1969)*, pages 81–115. Ann. of Math. Studies, No. 66. Princeton Univ. Press, Princeton, N.J., 1971.

[11] Anders Björner and Francesco Brenti. *Combinatorics of Coxeter groups*, volume 231 of *Graduate Texts in Mathematics*. Springer, New York, 2005.

[12] Tara Brendle and Dan Margalit. The level four congruence subgroup of braid group. *Preprint*.

[13] Tara Brendle, Dan Margalit, and Andrew Putman. Generators for the hyperelliptic torelli group and the kernel of the burau representation at t=-1. *arXiv preprint arXiv:1211.4018*, 2012.

[14] Thomas Church and Andrew Putman. Generating the johnson filtration. *Geometry & Topology*, 19(4):2217–2255, 2015.

[15] Thomas Church and Andrew Putman. Generating the Johnson filtration. *Geom. Topol.*, 19(4):2217–2255, 2015.

[16] H.S.M. Coxeter. Factor groups of the braid group. pages 95–122, 1957.

[17] Max Dehn. Die gruppe der abbildungsklassen,. *Acta Math.*, 69:135–206, 1938.

[18] Persi Diaconis. *Chapter 7: Representation Theory of the Symmetric Group*, volume Volume 11 of *Lecture Notes–Monograph Series*, pages 131–140. Institute of Mathematical Statistics, Hayward, CA, 1988.

[19] Ben Elias and Geordie Williamson. The Hodge theory of Soergel bimodules. *Ann. of Math. (2)*, 180(3):1089–1136, 2014.

[20] B. Farb and D. Margalit. *A Primer on Mapping Class Groups (PMS-49)*. Princeton Mathematical Series. Princeton University Press, 2011.

[21] A. T. Fomenko and S. V. Matveev. *Algorithmic and computer methods for three-manifolds*, volume 425 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 1997. Translated from the 1991 Russian original by M. Tsaplina and Michiel Hazewinkel and revised by the authors, With a preface by Hazewinkel.

[22] J. S. Frame, G. de B. Robinson, and R. M. Thrall. The hook graphs of the symmetric groups. *Canadian J. Math.*, 6:316–324, 1954.

[23] Louis Funar. On the TQFT representations of the mapping class groups. *Submitted to: Pacific J. Math.*, 1998.

[24] Louis Funar and Toshitake Kohno. Free subgroups within the images of quantum representations. *Forum Math.*, 26(2):337–355, 2014.

[25] J. Gambaudo and É. Ghys. Braids and signatures. *Bull. Soc. Math. France*, 133(4):541–579, 2005.

[26] M. Geck and G. Pfeiffer. *Characters of Finite Coxeter Groups and Iwahori-Hecke Algebras*. London Mathematical Society monographs. Clarendon Press, 2000.

[27] Meinolf Geck and Nicolas Jacon. *Representations of Hecke algebras at roots of unity*, volume 15 of *Algebra and Applications*. Springer-Verlag London, Ltd., London, 2011.

[28] Andr Gramain. Le type d'homotopie du groupe des diffomorphismes d'une surface compacte. *Annales scientifiques de l'cole Normale Suprieure*, 6(1):53–66, 1973.

[29] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, New York, 2002. Autre(s) tirage(s) : 2003,2004,2005,2006.

[30] Stephen P. Humphries. Normal closures of powers of Dehn twists in mapping class groups. *Glasgow Math. J.*, 34(3):313–317, 1992.

[31] StephenP. Humphries. Generators for the mapping class group. In Roger Fenn, editor, *Topology of Low-Dimensional Manifolds*, volume 722 of *Lecture Notes in Mathematics*, pages 44–47. Springer Berlin Heidelberg, 1979.

[32] C.J. Isham. *Modern Differential Geometry for Physicists*. World Scientific lecture notes in physics. World Scientific, 1999.

[33] Dennis Johnson. Homeomorphisms of a surface which act trivially on homology. *Proceedings of the American Mathematical Society*, 75(1):pp. 119–125, 1979.

[34] Dennis Johnson. Quadratic forms and the Birman-Craggs homomorphisms. *Trans. Amer. Math. Soc.*, 261(1):235–254, 1980.

[35] Dennis Johnson. The structure of the Torelli group. I. A finite set of generators for $\mathcal{I}$. *Ann. of Math. (2)*, 118(3):423–442, 1983.

[36] Dennis Johnson. The structure of the Torelli group. II: A characterization of the group generated by twists on bounding curves. *Topology*, 24(2):113 – 126, 1985.

[37] Dennis Johnson. The structure of the Torelli group. III: The abelianization of i. *Topology*, 24(2):127 – 144, 1985.

[38] V. F. R. Jones. Hecke algebra representations of braid groups and link polynomials. *Ann. of Math. (2)*, 126(2):335–388, 1987.

[39] Yasushi Kasahara. An expansion of the Jones representation of genus 2 and the Torelli group. *Algebr. Geom. Topol.*, 1:39–55, 2001.

[40] C. Kassel and V. Turaev. *Braid groups*, volume 247 of *Graduate Texts in Mathematics*. Springer, New York, 2008. With the graphical assistance of Olivier Dodane.

[41] David Kazhdan and George Lusztig. Representations of Coxeter groups and Hecke algebras. *Invent. Math.*, 53(2):165–184, 1979.

[42] W. B. R. Lickorish. A finite set of generators for the homotopy group of a 2-manifold. *Proceedings of the Cambridge Philosophical Society*, 60:769–778, 1964.

[43] D.D. Long and M. Paton. The burau representation is not faithful for $n \geq 6$. *Topology*, 32(2):439 – 447, 1993.

[44] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory*. Dover Publications, Inc., Mineola, NY, second edition, 2004. Presentations of groups in terms of generators and relations.

[45] W.S. Massey. *Algebraic Topology: An Introduction*. Graduate Texts in Mathematics. Springer New York, 1989.

[46] D. B. McReynolds. The congruence subgroup problem for braid groups: Thurston's proof, 2009. cite arxiv:0901.4663 Comment: Version 2. Expanded with numerous mistakes from the Version 1 fixed.

[47] Geoffrey Mess. The torelli groups for genus 2 and 3 surfaces. *Topology*, 31(4):775 – 790, 1992.

[48] M. Newman and J. R. Smart. Symplectic modulary groups. *Acta Arith*, 9:83–89, 1964.

[49] Luis Paris and Dale Rolfsen. Geometric subgroups of mapping class groups. *J. Reine Angew. Math.*, 521:47–83, 2000.

[50] B. Perron and J. P. Vannier. Groupe de monodromie géométrique des singularités simples. *Mathematische Annalen*, 306(1):231–245, 1996.

[51] Jerome Powell. Two theorems on the mapping class group of a surface. *Proceedings of the American Mathematical Society*, 68(3):pp. 347–350, 1978.

[52] Andrew Putman. Cutting and pasting in the Torelli group. *Geom. Topol.*, 11:829–865, 2007.

[53] Andrew Putman. The Picard group of the moduli space of curves with level structures. *Duke Math. J.*, 161(4):623–674, 2012.

[54] Andrew Putman. Small generating sets for the Torelli group. *Geom. Topol.*, 16(1):111–125, 2012.

[55] J. Tits. Systèmes générateurs de groupes de congruence. *C. R. Acad. Sci. Paris Sér. A-B*, 283(9):Ai, A693–A695, 1976.

[56] B. Wajnryb. A braidlike presentation of $\mathrm{Sp}(n, p)$. *Israel J. Math.*, 76(3):265–288, 1991.

[57] Hans Wenzl. Hecke algebras of typea n and subfactors. *Inventiones mathematicae*, 92(2):349–383, 1988.

[58] Y. Yin. *W-graph representations for Coxeter groups and Hecke algebras.* PhD thesis, University of Sydney, 2004.