On the first cohomology group of cofinite subgroups in surface mapping class groups

John D. McCarthy

Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA

(17 June 1997)

Abstract

Following the well-known analogy between arithmetic groups and surface mapping class groups, Ivanov asked whether the first cohomology group of any subgroup of finite index in a surface mapping class group must be trivial. In this note, we establish, as our first result, an affirmative answer to Ivanov's question, provided the surface in question has genus at least 3, and the subgroup of finite index contains the Torelli group. Secondly, we show that our first result does not hold for any surface of genus 2. This second result establishes, in particular, a negative answer to Ivanov's question for any surface of genus 2.

0 Introduction

Let S be a compact orientable surface, possibly with boundary. The mapping class group of S is the group $\mathcal{M}_S$ of isotopy classes of orientation-preserving homeomorphisms $S \to S$. $\mathcal{M}_S$ acts naturally on the first homology group $\mathrm{H}_1(S)$ of S with integer coefficients. The Torelli group of S is the kernel $\mathcal{T}_S$ of this action.

It is well known that $\mathrm{H}^1(\mathcal{M}_S) = 0$. Ivanov asked whether it is true that $\mathrm{H}^1(\Gamma) = 0$ for any subgroup Γ of finite index in $\mathcal{M}_S$ [9, p. 135]. (Note that Ivanov formulated his question for the extended mapping class group, which includes the isotopy classes of orientation-reversing homeomorphisms $S \to S$. Since the extended mapping class group is a finite extension of $\mathcal{M}_S$, his question is equivalent to the question stated above.) In this note, we prove the following theorem.

Theorem A *Let S be a connected closed orientable surface of genus g at least 3. Suppose that Γ is a subgroup of finite index in the mapping class group $\mathcal{M}_S$*

of S containing the Torelli group $\mathcal{T}_S$ of S. Then the first cohomology $\mathrm{H}^1(\Gamma)$ *of* Γ *with integer coefficients is trivial.*

Our proof of Theorem A is an elementary argument involving fundamental results of Johnson's on generators and relations in the Torelli group. An alternative argument for Theorem A, relying on deeper results of Johnson's on the structure of the Torelli group, has been given by Hain and Looijenga [4].

Ivanov's question, which Theorem A addresses, has an interesting relationship to the analogy between arithmetic groups and mapping class groups introduced by Harvey [5]. The vanishing theorem of Kajdan [8] implies that arithmetic groups of rank greater than 2 have trivial first cohomology (i.e. trivial first Betti number). (Note that a cofinite subgroup of an arithmetic group Γ is an arithmetic group with the same rank as Γ.) The results of Millson [13], on the other hand, provide examples of arithmetic groups of rank 1 with nontrivial first cohomology. Hence, Ivanov's question relates to the analogy between arithmetic groups and surface mapping class groups and the corresponding question concerning the rank of surface mapping class groups. In a similar vein, consider Ivanov's question [9, p. 135] concerning whether surface mapping class groups satisfy the vanishing theorem of Kajdan, (i.e. whether they satisfy Kajdan's Property T).

Note that, as explained by Bass, Milnor and Serre [1], the vanishing of first cohomology for arithmetic groups follows from arguments involving the congruence subgroup property [12]. Since the notion of a congruence subgroup of Γ involves passing to a quotient of the ring of integers over which Γ is defined, this notion is defined only for arithmetic groups. Ivanov, however, has introduced an analogous notion of congruence subgroups for surface mapping class groups and has formulated the corresponding congruence subgroup property. Ivanov asked [9, p. 134] whether surface mapping class groups satisfy this congruence subgroup property.

It appears that an affirmative answer to Ivanov's question could result from establishing, for surface mapping class groups, either Kajdan's property T or the congruence subgroup property described by Ivanov. Unfortunately, the tools which have been used to establish these properties, tools involving algebraic groups, Lie groups and the representation theory of groups, are not available for surface mapping class groups.

Suppose that r is a positive integer. $\mathcal{M}_S$ acts naturally on $\mathrm{H}_1(S, \mathbb{Z}_r)$. We recall that the level r subgroup of $\mathcal{M}_S$ is the subgroup $\Gamma_r(S)$ of $\mathcal{M}_S$ consisting of those mapping classes which act trivially on $\mathrm{H}_1(S, \mathbb{Z}_r)$. Since the Torelli group $\mathcal{T}_S$ acts trivially on $\mathrm{H}_1(S)$, $\mathcal{T}_S \subset \Gamma_r(S)$.

The assumption that g is at least 3 is a necessary hypothesis for Theorem A. Indeed, we shall prove the following result.

Theorem B *Let S be a connected closed orientable surface of genus two and r be an integer divisible by 2 or 3. Let $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$, the subgroup of $\mathcal{M}_S$ consisting of those mapping classes which act trivially on $\mathrm{H}_1(S, \mathbb{Z}_r)$. Then the first cohomology $\mathrm{H}^1(\Gamma_r(S))$ is nontrivial.*

Here is an outline of the paper. In Section 1, we shall prove the main result of the paper, Theorem A (Theorem 1.1), for surfaces of genus g at least 3. In Section 2, we shall demonstrate the failure of Theorem A in genus 2 by proving Theorem B (Theorem 2.1).

1 The Main Result

In this section, we prove the main result of the paper, Theorem A:

Theorem 1.1 *Let S be a connected closed orientable surface of genus g at least 3. Suppose that Γ is a subgroup of finite index in the mapping class group $\mathcal{M}_S$ of S containing the Torelli group $\mathcal{T}_S$ of S. Then the first cohomology $\mathrm{H}^1(\Gamma)$ of Γ with integer coefficients is trivial.*

PROOF. Let $\lambda : \Gamma \to \mathbb{Z}$ be a homomorphism.

Let γ be a simple closed curve on S. We shall denote the Dehn twist about γ by $T_\gamma \in \mathcal{M}_S$. We recall that a bounding pair is a pair (γ, δ) of nonseparating disjoint homologous simple closed curves on S. Let (γ, δ) be a bounding pair. Since Γ has finite index in $\mathcal{T}_S$, there exists a positive integer r such that T_γ^r is in Γ. By Lemma 11 of [7], $(T_\gamma \circ T_\delta^{-1})^r$ is in the commutator $[\Gamma, \mathcal{T}_S]$ of Γ and $\mathcal{T}_S$. Since $\mathcal{T}_S$ is contained in Γ, this implies that $\lambda((T_\gamma \circ T_\delta^{-1})^r) = 0$.

The mapping class $T_\gamma \circ T_\delta^{-1}$ is an element of $\mathcal{T}_S$. Such a mapping class is called a bounding pair map. Since $T_\gamma \circ T_\delta^{-1}$ is in $\mathcal{T}_S$, $T_\gamma \circ T_\delta^{-1}$ is in Γ. Hence, $\lambda((T_\gamma \circ T_\delta^{-1})^r) = r\lambda(T_\gamma \circ T_\delta^{-1})$. Since $\lambda((T_\gamma \circ T_\delta^{-1})^r) = 0$ and $r > 0$, we conclude that $\lambda(T_\gamma \circ T_\delta^{-1}) = 0$. Thus, the kernel of λ contains all bounding pair maps. Since the genus g of S is at least 3, Theorem 2 of [6] implies that $\mathcal{T}_S$ is generated by bounding pair maps. Hence, $\mathcal{T}_S$ is contained in the kernel of λ.

Since S is a closed surface of genus g, the intersection pairing on $\mathrm{H}_1(S)$ is a unimodular symplectic form on a lattice of rank $2g$. Hence, the natural action of $\mathcal{M}_S$ on $\mathrm{H}_1(S)$ yields a homomorphism $\eta : \mathcal{M}_S \to \mathrm{Sp}(2g, \mathbb{Z})$ with kernel $\mathcal{T}_S$. This homomorphism restricts to an epimorphism $\eta| : \Gamma \to \eta(\Gamma)$. Since $\mathcal{T}_S$ is contained in Γ, the kernel of $\eta| : \Gamma \to \eta(\Gamma)$ is equal to $\mathcal{T}_S$. Since $\mathcal{T}_S$ is contained in the kernel of λ, λ factors through the epimorphism $\eta|$. That is, there exists a homomorphism $\mu : \eta(\Gamma) \to \mathbb{Z}$ such that $\lambda = \mu \circ \eta|$.

It is well known that $\eta : \mathcal{M}_S \to \mathrm{Sp}(2g, \mathbb{Z})$ is surjective ([11],p. 178). Since Γ has finite index in $\mathcal{M}_S$, the image $\eta(\Gamma)$ has finite index in $\mathrm{Sp}(2g, \mathbb{Z})$. Since g is greater than 1, Corollary 3 of [12] implies that $\eta(\Gamma)$ contains a full congruence subgroup $\mathrm{N}(2g, m)$ of $\mathrm{Sp}(2g, \mathbb{Z})$ for some natural number m. Since $\mathrm{N}(2g, m)$ has finite index in $\mathrm{Sp}(2g, \mathbb{Z})$, $\mathrm{N}(2g, m)$ has finite index in $\eta(\Gamma)$. It is easy to see that the commutator subgroup $[\mathrm{N}(2g, m), \mathrm{N}(2g, m)]$ of $\mathrm{N}(2g, m)$ is a noncentral subgroup of $\mathrm{Sp}(2g, \mathbb{Z})$. (Indeed, the commutator of two transvections in symplectically nonorthogonal directions is a noncentral element of $\mathrm{Sp}(2g, \mathbb{Z})$.) Since $\mathrm{N}(2g, m)$ is normal in $\mathrm{Sp}(2g, \mathbb{Z})$, $[\mathrm{N}(2g, m), \mathrm{N}(2g, m)]$ is normal in $\mathrm{Sp}(2g, \mathbb{Z})$. Since g is greater than 1, Corollary 1 of [12] implies that $[\mathrm{N}(2g, m), \mathrm{N}(2g, m)]$ has finite index in $\mathrm{Sp}(2g, \mathbb{Z})$ and, hence, in $\eta(\Gamma)$. Since $\mathrm{N}(2g, m) \subset \eta(\Gamma)$, the homomorphism $\mu : \eta(\Gamma) \to \mathbb{Z}$ is trivial on the commutator subgroup $[\mathrm{N}(2g, m), \mathrm{N}(2g, m)]$ of $\mathrm{N}(2g, m)$. Since $[\mathrm{N}(2g, m), \mathrm{N}(2g, m)]$ has finite index in $\eta(\Gamma)$, we conclude that $\mu : \eta(\Gamma) \to \mathbb{Z}$ is trivial. Since $\lambda = \mu \circ \eta|$, λ is trivial. $\square$

2 Counterexamples in Genus 2

In this section, we shall demonstrate the failure of Theorem 1.1 in genus 2, by proving the following result, Theorem B:

Theorem 2.1 *Let S be a connected closed orientable surface of genus two and r be an integer divisible by 2 or 3. Let $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$, the subgroup of $\mathcal{M}_S$ consisting of those mapping classes which act trivially on $\mathrm{H}_1(S, \mathbb{Z}_r)$. Then the first cohomology $\mathrm{H}^1(\Gamma_r(S))$ is nontrivial.*

In order to prove this theorem, we shall need some preliminary results about certain representations of the level r subgroup $\Gamma_r(S)$ of $\mathcal{M}_S$.

We recall that a circle on S is the image of an embedding $S^1 \to S$. For each circle C on S, S_C denotes the surface obtained by cutting S along C. A circle C is nonseparating if S_C is connected. Let C be a nonseparating circle on S.

Let S' be a closed orientable surface of genus g with a given orientation. Let $\langle , \rangle : \mathrm{H}_1(S') \times \mathrm{H}_1(S') \to \mathbb{Z}$ denote the algebraic intersection pairing on $\mathrm{H}_1(S')$. Suppose that $(A_1, B_1, ..., A_g, B_g)$ is a family of oriented circles on S' such that (i) A_i and B_i are tranverse and meet at exactly one point, (ii) $\langle a_i, b_i \rangle = 1$, where a_i and b_i are the elements of $\mathrm{H}_1(S')$ represented by A_i and B_i, and (iii) $A_i \cup B_i$ is disjoint from $A_j \cup B_j$ if $i \neq j$. Then, we say that $(A_1, B_1, ..., A_g, B_g)$ is a standard symplectic configuration on S'. Note that if $(A_1, B_1, ..., A_g, B_g)$ is a standard symplectic configuration on S', then $(a_1, b_1, ..., a_g, b_g)$ is a standard symplectic basis for the integral symplectic lattice $\mathrm{H}_1(S')$.

Choose an orientation on S and an orientation of C. We may extend C to a standard symplectic configuration (A, B, C, D) on S. Let a, b, c, and d be the elements of $\mathrm{H}_1(S)$ represented by the oriented circles A, B, C, and D, respectively. Then, (a, b, c, d) is a standard symplectic basis for the integral symplectic lattice $(\mathrm{H}_1(S), \langle , \rangle)$.

Let $r \geq 2$ be an integer. As in Looijenga [10], we may construct an r-fold cyclic covering of S as follows. Since S has genus two, S_C is a torus with two holes. The two boundary components of S_C correspond to the sides of C. Let C_+ be the boundary component of S_C corresponding to the left side of C and C_- be the boundary component of S_C corresponding to the right side of C. S is obtained from S_C by gluing C_+ and C_- to one another via a homeomorphism $h : C_+ \to C_-$. We denote the corresponding quotient map by $p_C : S_C \to S$. Note that $p_C(h(x)) = p_C(x)$ for each $x \in C_+$. Let $\tilde{S}$ be the quotient of $S_C \times \mathbb{Z}_r$ obtained by identifying (x, i) with $(h(x), i + 1)$ for each $x \in C_+$ and $i \in \mathbb{Z}_r$. The rule $[(x, i)] \mapsto p_C(x)$ yields a well defined r-fold cyclic covering $p : \tilde{S} \to S$. The rule $[(x, i)] \mapsto [(x, i + 1)]$ defines a generator $\sigma : \tilde{S} \to \tilde{S}$ of the covering group G of $p : \tilde{S} \to S$.

Orient $\tilde{S}$ such that $p : \tilde{S} \to S$ is orientation-preserving. A straightforward examination of the preimages $p^{-1}(A)$, $p^{-1}(B)$, $p^{-1}(C)$, and $p^{-1}(D)$ yields the following result.

Lemma 2.2 *Let A, B, C, D be a standard symplectic configuration on the surface S of genus 2. Let $p : \tilde{S} \to S$ be the r-fold cyclic covering obtained by cutting S along C. Then, there exists a configuration of oriented circles $(A_1, B_1, ..., A_r, B_r, C_1 ..., C_r, D_1)$ on $\tilde{S}$ such that:*

(1) $p^{-1}(A)$ is the disjoint union of the circles $A_1, ..., A_r$,
(2) $p^{-1}(B)$ is the disjoint union of the circles $B_1, ..., B_r$,
(3) $p^{-1}(C)$ is the disjoint union of the circles $C_1, ..., C_r$,
(4) $p^{-1}(D) = D_1$,
(5) $A_i = \sigma^{i-1}(A_1)$ (as oriented circles),
(6) $B_i = \sigma^{i-1}(B_1)$ (as oriented circles),
(7) $C_i = \sigma^{i-1}(C_1)$ (as oriented circles),
(8) $D_1 = \sigma(D_1)$ (as oriented circles),
(9) $p| : A_i \to A$ is orientation-preserving,
(10) $p| : B_i \to B$ is orientation-preserving,
(11) $p| : C_i \to C$ is orientation-preserving,
(12) $p| : D_1 \to D$ is orientation-preserving.
(13) $(A_1, B_1, ..., A_r, B_r, C_1, D_1)$ is a standard symplectic configuration on $\tilde{S}$.

Let a_i, b_i, c_i and d_1 be the elements of $\mathrm{H}_1(\tilde{S})$ represented by A_i, B_i, C_i and D_1 respectively. Then, $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ is a standard symplectic basis for $\mathrm{H}_1(\tilde{S})$.

Let Λ denote the kernel of the induced homomorphism $p_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(S)$. For each element g in G, $p \circ g = p$ and, hence, $p_* \circ g_* = p_*$. It follows that g_* maps the kernel Λ of p_* to itself. Hence, we obtain an action of G on Λ. Thus, Λ is a $\mathbb{Z}G$-module.

The homomorphism $p_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(S)$ is determined by the conditions: (i) $p_*(a_i) = a$, (ii) $p_*(b_i) = b$, (iii) $p_*(c_1) = c$ and (iv) $p_*(d_1) = rd$. It follows that Λ is the subgroup of $\mathrm{H}_1(\tilde{S})$ generated by the classes e_i and f_i defined by the rule $e_i = a_i - a_{i+1}$ and $f_i = b_i - b_{i+1}$. Moreover, the classes $e_1, f_1, ..., e_{r-1}, f_{r-1}$ form a free basis for the free abelian group Λ.

The action of σ on Λ is determined by the conditions: $\sigma_*(e_i) = e_{i+1}$, $\sigma_*(f_i) = f_{i+1}$. Note that $e_r = a_r - a_1 = -(e_1 + ... + e_{r-1})$ and $f_r = -(f_1 + ... + f_{r-1})$. It follows that the element $N = 1 + \sigma + ... + \sigma^{r-1}$ of $\mathbb{Z}G$ acts trivially on Λ. Let I denote the ideal in $\mathbb{Z}G$ generated by N. Then the action of $\mathbb{Z}G$ on Λ factors through the quotient ring $\mathbb{Z}G/I$.

We assume, henceforth, that r is a prime. Then $\mathbb{Z}G/I$ is isomorphic to the ring $\mathbb{Z}[\zeta] \subset \mathbb{C}$ obtained by adjoining the primitive r-th root of unity $\mathrm{e}^{\mathrm{i}2\pi/r}$ to $\mathbb{Z}$. Hence, the action of $\mathbb{Z}G$ on Λ equips Λ with the structure of a $\mathbb{Z}[\zeta]$-module via the rule $\zeta \cdot v = \sigma_*(v)$ for all $v \in \Lambda$.

Lemma 2.3 *Let $e_1 = a_1 - a_2$, $f_1 = b_1 - b_2$. Then the kernel Λ of the homomorphism $p_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(S)$ induced by the covering map $p : \tilde{S} \to S$ is a free $\mathbb{Z}[\zeta]$-module of rank 2 with free basis e_1, f_1.*

PROOF. Note that $\mathbb{Z}[\zeta]$ is a free abelian group of rank $(r-1)$, (whereas $\mathbb{Z}G$ is a free abelian group of rank $|G| = r$). Let $\Lambda^2(\mathbb{Z}[\zeta])$ denote the free $\mathbb{Z}[\zeta]$-module of rank 2 with free basis e, f. Consider the unique $\mathbb{Z}[\zeta]$-module homomorphism $\eta : \Lambda^2(\mathbb{Z}[\zeta]) \to \Lambda$ such that $\eta(e) = e_1$ and $\eta(f) = f_1$. Since $\sigma_*(e_i) = e_{i+1}$ and $\sigma_*(f_i) = f_{i+1}$, and Λ is generated by $e_1, f_1, ..., e_{r-1}, f_{r-1}$, η is surjective. On the other hand, $\Lambda^2(\mathbb{Z}[\zeta])$ and Λ are both free abelian groups of rank $2(r-1)$. Thus, $\eta : \Lambda^2(\mathbb{Z}[\zeta]) \to \Lambda$ is injective and, hence, a $\mathbb{Z}[\zeta]$-module isomorphism. Hence, Λ is a free $\mathbb{Z}[\zeta]$-module of rank 2 with free basis e_1, f_1. $\square$

Since $p : \tilde{S} \to S$ is an r-fold cyclic covering space of S, we have a short exact sequence:

$$1 \to \pi_1(\tilde{S}) \xrightarrow{p_*} \pi_1(S) \xrightarrow{\chi} G \to 1$$

where $\chi : \pi_1(S) \to G$ is the canonical homomorphism. Since G is a cyclic group of order r generated by σ we may identify $\mathbb{Z}_r$ with G via the rule $i \mapsto \sigma^i$. Since $\mathbb{Z}_r$ is abelian, there exists a unique homomorphism $\rho : \mathrm{H}_1(S) \to \mathbb{Z}_r$ such that

$\rho \circ \eta = \chi$, where $\eta : \pi_1(S) \to \mathrm{H}_1(S)$ is the natural homomorphism. Since χ is surjective, ρ is surjective.

Lemma 2.4 *The homomorphism $\rho : \mathrm{H}_1(S) \to \mathbb{Z}_r$ is given by the rule $\rho(v) = [\langle c, v\rangle] \in \mathbb{Z}_r$. A circle K on S lifts to a circle $\tilde{K}$ on $\tilde{S}$ if and only if $\rho(k) = 0$, where k is the element of $\mathrm{H}_1(S)$ represented by K (with any given orientation).*

PROOF. Let K be an oriented circle on S and k be the element of $\mathrm{H}_1(S)$ represented by K. K determines an element γ of $\pi_1(S)$ which is well-defined up to conjugacy. By covering space theory, K lifts to $\tilde{S}$ if and only if $\gamma \in p_*(\pi_1(\tilde{S}))$. By the previous exact sequence, it follows that K lifts to $\tilde{S}$ if and only if $\chi(\gamma) = 0$. Since $\eta(\gamma) = k$ and $\chi = \rho \circ \eta$, we conclude that K lifts to a circle $\tilde{K}$ on S if and only if $\rho(k) = 0$.

Since A, B and C each lift to $\tilde{S}$, $\rho(a) = \rho(b) = \rho(c) = 0$. Let $*$ be the point of intersection of C and D so that the oriented circle D yields a loop in S based at $*$. Let y be the unique point in C_- such that $p_C(y) = *$ and $\tilde{*} = [y, 1]$. Let z be the unique point in C_+ such that $p_C(z) = *$, so that $h(z) = y$. The lift $\tilde{D}$ of D beginning at $\tilde{*}$ ends at $[z, 1] = [h(z), 2] = [y, 2] = \sigma([y, 1]) = \sigma(\tilde{*})$, and, hence, $\rho(d) = 1$. It follows that ρ is given by the rule $\rho(v) = [\langle c, v\rangle] \in \mathbb{Z}_r$. $\square$

By the naturality of η and the definition of ρ, we have a commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_1(\tilde{S}) & \xrightarrow{p_*} & \pi_1(S) & \xrightarrow{\chi} & G & \longrightarrow & 1 \\
\downarrow & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} & & \downarrow & & \\
\Lambda & \longrightarrow & \mathrm{H}_1(\tilde{S}) & \xrightarrow{p_*} & \mathrm{H}_1(S) & \xrightarrow{\rho} & \mathbb{Z}_r & \longrightarrow & 1.
\end{array}$$

Since η is surjective, the exactness of the first row in this diagram implies the exactness of the second. Thus, $p_*(\pi_1(\tilde{S})) = kernel(\chi)$ and $p_*(\mathrm{H}_1(\tilde{S})) = kernel(\rho)$.

Let $\phi : S \to S$ be a homeomorphism. We say that ϕ lifts to $\tilde{S}$ if there exists a homeomorphism $\tilde{\phi} : \tilde{S} \to \tilde{S}$ such that $p \circ \tilde{\phi} = \phi \circ p$. In this event, we say that $\tilde{\phi}$ is a lift of ϕ to $\tilde{S}$. Suppose that ϕ lifts to $\tilde{S}$. Then $\tilde{\phi}$ is well-defined up to composition with an element $g \in G$. Moreover, conjugation by $\tilde{\phi}$ determines an automorphism of G, $g \mapsto \tilde{\phi} \circ g \circ \tilde{\phi}^{-1}$. Since G is abelian and $\tilde{\phi}$ is well-defined up to composition with an element $g \in G$, this automorphism depends only upon ϕ. We shall denote this automorphism by $\phi_* : G \to G$. Finally, since $p_* \circ \tilde{\phi}_* = \phi_* \circ p_*$, the action of $\tilde{\phi}$ on $\mathrm{H}_1(\tilde{S})$, $\tilde{\phi}_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(\tilde{S})$, restricts to an automorphism of Λ, $\tilde{\phi}_* : \Lambda \to \Lambda$.

We may choose a homeomorphism $\psi : S \to S$ such that ψ is isotopic to ϕ and $\psi(*) = *$, where $*$ is a basepoint for the fundamental group $\pi_1(S) = \pi_1(S, *)$. The automorphism $\psi_* : \pi_1(S) \to \pi_1(S)$ induced by ψ depends only on the isotopy class of ϕ up to an inner automorphism of $\pi_1(S)$. By abuse of notation, we shall denote this automorphism by $\phi_* : \pi_1(S) \to \pi_1(S)$.

By the naturality of η and the definition of ρ, we have a commutative diagram:

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & \pi_1(\tilde{S}) & \xrightarrow{p_*} & \pi_1(S) & \xrightarrow{\phi_*} & \pi_1(S) & \xrightarrow{\chi} & G & \longrightarrow & 1 \\
\downarrow & & \downarrow \eta & & \downarrow \eta & & \downarrow \eta & & \downarrow & & \\
\Lambda & \longrightarrow & \mathrm{H}_1(\tilde{S}) & \xrightarrow{p_*} & \mathrm{H}_1(S) & \xrightarrow{\phi_*} & \mathrm{H}_1(S) & \xrightarrow{\rho} & \mathbb{Z}_r & \longrightarrow & 1.
\end{array}$$

The homeomorphism $\phi : S \to S$ lifts to $\tilde{S}$ if and only if $\phi_*(p_*(\pi_1(\tilde{S}))) \subset p_*(\pi_1(\tilde{S}))$. That is, $\phi : S \to S$ lifts to $\tilde{S}$ if and only if $\chi \circ \phi_* \circ p_* = 0$. On the other hand, by the preceding commutative diagram, since η is surjective, $\chi \circ \phi_* \circ p_* = 0$ if and only if $\rho \circ \phi_* \circ p_* = 0$. That is, $\chi \circ \phi_* \circ p_* = 0$ if and only if $\phi_*(p_*(\mathrm{H}_1(\tilde{S}))) \subset p_*(\mathrm{H}_1(\tilde{S}))$. Thus, we have the following result.

Lemma 2.5 *Let $\phi : S \to S$ be a homeomorphism of S. ϕ lifts to $\tilde{S}$ if and only if $\phi_*(p_*(\mathrm{H}_1(\tilde{S}))) \subset p_*(\mathrm{H}_1(\tilde{S}))$.*

Suppose that ϕ lifts to $\tilde{S}$. Let $\phi_\# : G \to G$ be the automorphism of G induced by conjugation by a lift $\tilde{\phi}$ of ϕ. Then, we have the equation $\phi_\# \circ \chi = \chi \circ \phi_*$. Since χ is surjective, it follows that $\tilde{\phi}$ commutes with each element $g \in G$ if and only if $\chi \circ \phi_* = \chi$. Again, on the other hand, by the preceding observations, $\chi \circ \phi_* = \chi$ if and only if $\rho \circ \phi_* = \rho$. Hence, $\tilde{\phi}$ commutes with each element $g \in G$ if and only if $\rho \circ \phi_* = \rho$.

Let $Stab_\rho$ denote the subgroup of $\mathcal{M}_S$ consisting of the mapping classes of orientation-preserving homeomorphisms $\phi : S \to S$ such that $\rho \circ \phi_* = \rho$. We call $Stab_\rho$ the stabilizer of ρ in $\mathcal{M}_S$.

Lemma 2.6 *Suppose that $\phi : S \to S$ represents an element of the stabilizer $Stab_\rho$ of ρ in $\mathcal{M}_S$. Then there exists a lift of ϕ to $\tilde{S}$. Moreover, each lift $\tilde{\phi}$ of ϕ commutes with each element $g \in G$ and, hence, induces a $\mathbb{Z}G$-automorphism of $\mathrm{H}_1(\tilde{S})$, $\tilde{\phi}_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(\tilde{S})$, and a $\mathbb{Z}[\zeta]$-module automorphism of Λ, $\tilde{\phi}_* : \Lambda \to \Lambda$.*

Suppose that $\phi : S \to S$ represents an element of $Stab_\rho$. With respect to the $\mathbb{Z}[\zeta]$-basis e_1, f_1 for Λ, $\tilde{\phi}_* : \Lambda \to \Lambda$ is represented by an element of $\mathrm{GL}(2, \mathbb{Z}[\zeta])$, the group of 2×2 matrices with coefficients in $\mathbb{Z}[\zeta]$ which are invertible over $\mathbb{Z}[\zeta]$. Henceforth, we shall abuse notation and write $\tilde{\phi}_* \in \mathrm{GL}(2, \mathbb{Z}[\zeta])$ for the matrix of $\tilde{\phi}_* : \Lambda \to \Lambda$ with respect to the basis e_1, f_1.

Suppose now that $\gamma \in \Gamma_r(S)$. Let ϕ be a representative of the mapping class γ. By the definition of $\Gamma_r(S)$, the homomorphism $\phi_* : \mathrm{H}_1(S, \mathbb{Z}_r) \to \mathrm{H}_1(S, \mathbb{Z}_r)$ induced by ϕ is equal to the identity. There exists a unique homomorphism $\rho_r : \mathrm{H}_1(S, \mathbb{Z}_r) \to \mathbb{Z}_r$ such that $\rho_r \circ \eta_r = \rho$, where $\eta_r : \pi_1(S) \to \mathrm{H}_1(S, \mathbb{Z}_r)$ is the natural homomorphism. Hence, $\rho \circ \phi_* = \rho_r \circ \eta_r \circ \phi_* = \rho_r \circ \phi_* \circ \eta_r = \rho_r \circ \eta_r = \rho$. Thus, $\Gamma_r(S) \subset Stab_\rho$.

We now wish to describe generators for $\Gamma_r(S)$.

We recall that an element $w \in \mathrm{H}_1(S)$ is said to be primitive if w cannot be written in the form $w = mz$, where m is an integer such that $m > 1$ and $z \in \mathrm{H}_1(S)$. Note that a primitive element is necessarily nonzero. An element $w \in \mathrm{H}_1(S)$ is primitive if and only if there exists an oriented circle K on S such that w is represented by K. Since a primitive element w is nonzero, any circle K representing w is nonseparating.

Suppose that $(V, \langle , \rangle)$ is a symplectic space. Let $\mathrm{Sp}(V, \langle , \rangle)$ be the group of symplectic transformations of $(V, \langle , \rangle)$. We recall that a right transvection of $(V, \langle , \rangle)$ is an element $\tau_w \in \mathrm{Sp}(V, \langle , \rangle)$ defined by the rule $v \mapsto v + \langle w, v \rangle w$ for some element $w \in V$. Suppose that $w \in V$. Let I be the identity homomorphism $V \to V$. Since the pairing $\langle , \rangle$ of V is nondegenerate, $\tau_w = I$ if and only if $w = 0$. Suppose that m is a nonnegative integer. Then $\tau_{mw} = \tau_w^{m^2}$.

Let R be a commutative ring with identity and n be a positive integer. Let $\mathrm{M}(n, R)$ be the algebra of $n \times n$ matrices with coefficients in R and $\mathrm{GL}(n, R)$ be the group of multiplicative units of $\mathrm{M}(n, R)$. Suppose that G is a subgroup of $\mathrm{GL}(n, R)$ and r is a positive integer. The level r subgroup of G is the subgroup $\Gamma_r(G)$ of G consisting of those elements A in G which may be expressed in the form $A = I + rB$ for some matrix B in $\mathrm{M}(n, R)$. Note that the level r subgroup of G is the intersection of the level r subgroup of $\mathrm{GL}(n, R)$ with G.

Let $\alpha : \mathrm{H}_1(S) \to \mathrm{H}_1(S, \mathbb{Z}_r)$ and $\beta : \mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle) \to \mathrm{Sp}(\mathrm{H}_1(S, \mathbb{Z}_r), \langle , \rangle)$ be the natural homomorphisms. Suppose that $w \in \mathrm{H}_1(S)$. Then $\alpha(w) = 0$ if and only if $w = ry$ for some element $y \in \mathrm{H}_1(S)$. Moreover, $\beta(\tau_w) = \tau_{\alpha(w)}$.

By definition, the level r subgroup $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ is the kernel of β. We have the following result ([12]).

Theorem 2.7 *The level r subgroup $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ is generated by the powers of transvections τ_z^r, where z is a primitive element of $\mathrm{H}_1(S)$.*

PROOF. Suppose that z is an element of $\mathrm{H}_1(S)$. Then $\tau_z^r(w) = w + r\langle z, w \rangle z$, for every w in $\mathrm{H}_1(S)$, and, hence, $\tau_z^r \in \Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$. In particular, this holds for every primitive element z of $\mathrm{H}_1(S)$.

Consider the symplectic lattice $(\mathrm{H}_1(S), \langle , \rangle)$. Using the standard symplectic basis (a, b, c, d) for this lattice, we may identify $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ with the integral symplectic group $\mathrm{Sp}(4, \mathbb{Z})$. Under this identification, $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ is identified with the congruence subgroup $\mathrm{N}(4, r)$ of $\mathrm{Sp}(4, \mathbb{Z})$ as in [12].

According to Theorem 10 of [12], $\mathrm{N}(4, r) = \mathrm{Q}(4, r)$, where $\mathrm{Q}(4, r)$ is the normal closure in $\mathrm{Sp}(4, \mathbb{Z})$ of the matrix $I + re_{12}$. Under the identification $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle) \equiv \mathrm{Sp}(4, \mathbb{Z})$, the matrix $I + re_{12}$ is identified with the power τ_a^r of the transvection τ_a corresponding to the primitive element a of $\mathrm{H}_1(S)$. It follows that $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ is generated by the conjugates of τ_a^r in $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$.

Suppose that ψ is an element of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$, and let $z = \psi(a)$. Since a is a primitive element of $\mathrm{H}_1(S)$ and $\psi : \mathrm{H}_1(S) \to \mathrm{H}_1(S)$ is an isomorphism, z is a primitive element of $\mathrm{H}_1(S)$. Moreover, $\psi \circ \tau_a \circ \psi^{-1} = \tau_{\psi(a)} = \tau_z$, and, hence, $\psi \circ \tau_a^r \circ \psi^{-1} = \tau_z^r$.

It follows that the level r subgroup $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ is generated by elements in $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ of the form τ_z^r, where z is a primitive element of $\mathrm{H}_1(S)$. Since all such elements are in $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$, we conclude that $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ is generated by the powers of transvections τ_z^r, where z is a primitive element of $\mathrm{H}_1(S)$. $\square$

For each circle K on S, let $t_K : S \to S$ denote a right Dehn twist about the circle K.

Theorem 2.8 *Let $r > 1$ be an integer and $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$, the kernel of the natural homomorphism $\mathcal{M}_S \to Aut(\mathrm{H}_1(S, \mathbb{Z}_r))$. Then $\Gamma_r(S)$ is generated by the mapping classes of the following two types of homeomorphisms of S: (i) t_K, where K is a nontrivial separating circle on S, and (ii) t_K^r, where K is a nonseparating circle on S.*

PROOF. Suppose that z is a primitive element in $\mathrm{H}_1(S)$. Let K be an oriented circle on S representing z, and $T_K \in \mathcal{M}_S$ be the mapping class of the right Dehn twist $t_K : S \to S$ about K. Then $\xi(T_K) = \tau_z$, and, hence, $\xi(T_K^r) = \tau_z^r$. It follows that $T_K \in \Gamma_r(S)$, for every nontrivial separating circle K on S, and $T_K^r \in \Gamma_r(S)$, for every nonseparating circle K on S.

As is well-known, the action of $\mathcal{M}_S$ on the integral symplectic lattice $\mathrm{H}_1(S)$ affords a homomorphism $\eta : \mathcal{M}_S \to \mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$. By Theorem 2.7, the level r subgroup $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$ is generated by the powers of transvections τ_z^r, where z is a primitive element of $\mathrm{H}_1(S)$. By definition, the level r subgroup $\Gamma_r(S)$ of $\mathcal{M}_S$ is the preimage under η of the level r subgroup $\Gamma_r(\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle))$ of $\mathrm{Sp}(\mathrm{H}_1(S), \langle , \rangle)$. On the other hand, by definition, the kernel of η is the Torelli group $\mathcal{T}_S$ of S. $\mathcal{T}_S$ is generated by the mapping classes of right Dehn twists t_K about nontrivial separating circles K on S [14]. (Note that Powell provides generators for $\mathcal{T}_S$ only for genus $g \geq 3$. His argument, however, establishes the assertion of the previous sentence for genus $g = 2$, given the generators for $\mathcal{T}_S$ in genus 2 as described in [2].) It follows that $\Gamma_r(S)$ is generated by the indicated mapping classes. $\square$

Lemma 2.9 *Let ϕ be a right Dehn twist about a circle K on S such that $\langle c, k\rangle \equiv 0 \pmod r$, where k is the element of $\mathrm{H}_1(S)$ represented by K (with any given orientation). Then ϕ represents an element of $Stab_\rho$ and there exists a lift $\tilde{\phi}$ of ϕ such that $\tilde{\phi}_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$.*

PROOF. Let $v \in \mathrm{H}_1(S)$. Then $\langle c, \phi_*(v)\rangle = \langle c, v + \langle k, v\rangle k\rangle = \langle c, v\rangle + \langle k, v\rangle\langle c, k\rangle$. Since $\langle c, k\rangle \equiv 0 \pmod r$, $\rho(\phi_*(v)) = [\langle c, \phi_*(v)\rangle] = [\langle c, v\rangle] = \rho(v)$. We conclude that $\rho \circ \phi_* = \rho$ and, hence, ϕ represents an element of $Stab_\rho$.

As shown above, $\rho(v) = [\langle c, v\rangle] \in \mathbb{Z}_r$. Hence, a circle K on S lifts to $\tilde{S}$ if and only if the algebraic intersection $\langle C, K\rangle$ of K and C (with respect to any given orientation of K) satisfies the congruence $\langle C, K\rangle \equiv 0 \pmod r$. By assumption, $\langle C, K\rangle \equiv 0 \pmod r$ and, hence, K lifts to $\tilde{S}$.

Let $\tilde{K}$ be a lift of K and $K_i = \sigma^{i-1}(\tilde{K})$, so that $K_1 = \tilde{K}$. Then, the preimage $p^{-1}(K)$ consists of the r disjoint circles $K_1, ..., K_r$ in $\tilde{S}$. Let ϕ be a right Dehn twist about K supported on an annular neighborhood A of K. The preimage $p^{-1}(A)$ consists of r disjoint annuli $A_1, ..., A_r$, where A_i is an annular neighborhood of K_i and $p| : A_i \to A$ is a homeomorphism. Let ϕ_i be the right Dehn twist about K_i supported on A_i and satisfying the identity $p \circ \phi_i|_{A_i} = \phi \circ p|_{A_i}$. Then $\tilde{\phi} = \phi_1 \circ ... \circ \phi_r$ is a lift of ϕ.

Let k_i be the element of $\mathrm{H}_1(\tilde{S})$ represented by K_i. We may express k_1 in terms of the basis $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ of $\mathrm{H}_1(\tilde{S})$:

$$k_1 = \Sigma_{i=1}^r (x_i a_i + y_i b_i) + z c_1 + w d_1.$$

Since K_1 is a circle in $\tilde{S}$ and K_i is disjoint from K_1 if $2 \leq i \leq r$, the algebraic intersection $\langle K_1, K_i\rangle$ of K_1 and K_i is equal to zero. Hence, since $K_i = \sigma^{i-1}(\tilde{K})$:

$$\langle k_1, \sigma^j(k_1)\rangle = 0; 1 \leq j \leq r.$$

Since $\sigma_*(a_i) = a_{i+1}$, $\sigma_*(b_i) = b_{i+1}$, $\sigma_*(c_1) = c_1$, and $\sigma_*(d_1) = d_1$:

$$\begin{aligned}\sigma^j(k_1) &= \Sigma_{i=1}^r (x_i a_{i+j} + y_i b_{i+j}) + z c_1 + w d_1 \\ &= \Sigma_{i=1}^r (x_{i-j} a_i + y_{i-j} b_i) + z c_1 + w d_1.\end{aligned}$$

Using the fact that $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ is a standard symplectic basis for $(\mathrm{H}_1(\tilde{S}), \langle,\rangle)$, we conclude that:

$$0 = \Sigma_{i+1}^r (x_i y_{i-j} - y_i x_{i-j})$$

where $1 \leq j \leq r$.

Let $x = \Sigma_{i=1}^r x_i \zeta^{i-1} \in \mathbb{Z}[\zeta]$ and $y = \Sigma_{i=1}^r y_i \zeta^{i-1} \in \mathbb{Z}[\zeta]$. Then $(1-\sigma)k_1 = xe_1 + yf_1$, $\overline{x} = \Sigma_{k=1}^r x_k \zeta^{1-k} \in \mathbb{Z}[\zeta]$, and $\overline{y} = \Sigma_{k=1}^r y_k \zeta^{1-k} \in \mathbb{Z}[\zeta]$.

The previous equations imply that:

$$\begin{aligned}
\overline{x}y &= \Sigma_{1\leq i,j\leq r} y_i \zeta^{i-1} x_j \zeta^{1-j} \\
&= \Sigma_{1\leq i,j\leq r} y_i x_j \zeta^{i-j} \\
&= \Sigma_{k=1}^r (\Sigma_{i=1}^r y_i x_{i-k}) \zeta^k \\
&= \Sigma_{k=1}^r (\Sigma_{j=1}^r x_j y_{j-k}) \zeta^k \\
&= x\overline{y}.
\end{aligned}$$

Hence, $\overline{x}y = x\overline{y} \in \mathbb{Z}[\zeta] \cap \mathbb{R}$.

Using the fact that ϕ_i acts on $\mathrm{H}_1(\tilde{S})$ as the transvection corresponding to the class of K_i in $\mathrm{H}_1(\tilde{S})$, we have the following identities:

$$\begin{aligned}
\tilde{\phi}_*(e_1) &= \tilde{\phi}_*((1-\sigma)a_1) = (1-\sigma)\tilde{\phi}_*(a_1) \\
&= (1-\sigma)(a_1 + \Sigma_{j=1}^r \langle k_j, a_1\rangle k_j) \\
&= e_1 + (1-\sigma)(\Sigma_{j=1}^r \langle \sigma^{j-1}(k_1), a_1\rangle k_j) \\
&= e_1 + (1-\sigma)(\Sigma_{j=1}^r \langle k_1, \sigma^{1-j}(a_1)\rangle k_j) \\
&= e_1 + (1-\sigma)(\Sigma_{j=1}^r \langle k_1, a_{2-j}\rangle \sigma^{j-1}(k_1)) \\
&= e_1 + (1-\sigma)(\Sigma_{j=1}^r (-y_{2-j}) \sigma^{j-1}(k_1)) \\
&= e_1 - (\Sigma_{j=1}^r y_{2-j} \sigma^{j-1})(1-\sigma)(k_1) \\
&= e_1 - (\Sigma_{k=1}^r y_k \sigma^{1-k})(xe_1 + yf_1) \\
&= e_1 - (\Sigma_{k=1}^r y_k \zeta^{1-k})(xe_1 + yf_1) \\
&= e_1 - \overline{y}xe_1 - \overline{y}yf_1 \\
&= (1 - x\overline{y})e_1 - (y\overline{y})f_1.
\end{aligned}$$

Likewise:

$$\tilde{\phi}_*(f_1) = (x\overline{x})e_1 + (1 + x\overline{y})f_1.$$

We conclude that, with respect to the $\mathbb{Z}[\zeta]$-module basis (e_1, f_1), the action of $\tilde{\phi}$ on Λ is given by the matrix:

$$\tilde{\phi}_* = \begin{pmatrix} 1 - x\overline{y} & x\overline{x} \\ -y\overline{y} & 1 + \overline{x}y \end{pmatrix}.$$

By the preceding equations, all the entries of $\tilde{\phi}_*$ lie in $\mathbb{Z}[\zeta] \cap \mathbb{R}$. Moreover, we may compute the determinant of $\tilde{\phi}_*$:

$$\begin{aligned} \det(\tilde{\phi}_*) &= (1 - x\overline{y})(1 + \overline{x}y) + x\overline{x}y\overline{y} \\ &= 1 - x\overline{y} + \overline{x}y - x\overline{x}y\overline{y} + x\overline{x}y\overline{y} \\ &= 1 - x\overline{y} + \overline{x}y = 1. \end{aligned}$$

Thus, $\tilde{\phi}_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$. $\square$

Lemma 2.10 *Let ψ be a right Dehn twist about a circle K on S such that $\langle C, K \rangle \not\equiv 0 \pmod r$ and $\phi = \psi^r$. Then there exists a lift $\tilde{\phi}$ of ϕ such that $\tilde{\phi}_* : \Lambda \to \Lambda$ is equal to the identity homomorphism of Λ.*

PROOF.

Since $\langle C, K \rangle \not\equiv 0 \pmod r$, K does not lift to $\tilde{S}$. Since r is a prime and $p : \tilde{S} \to S$ is an r-fold cyclic covering, it follows that the preimage $p^{-1}(K)$ consists of a single circle K_1 in $\tilde{S}$ and the restriction $p| : K_1 \to K$ is an r-fold connected cyclic covering space of K. Orient K and K_1 so that the restriction $p| : K_1 \to K$ is orientation-preserving.

Let k_1 be the element of $\mathrm{H}_1(\tilde{S})$ represented by K_1. We may express k_1 in terms of the basis $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ of $\mathrm{H}_1(\tilde{S})$:

$$k_1 = \Sigma_{i=1}^r (x_i a_i + y_i b_i) + z c_1 + w d_1.$$

Since $K_1 = p^{-1}(K)$ and σ is a covering transformation, we have a well-defined orientation-preserving restriction $\sigma| : K_1 \to K_1$. Hence, $\sigma_*(k_1) = k_1$. On the other hand, as in the previous case:

$$\begin{aligned} \sigma^j(k_1) &= \Sigma_{i=1}^r (x_i a_{i+1} + y_i b_{i+1}) + z c_1 + w d_1 \\ &= \Sigma_{i=1}^r (x_{i-1} a_i + y_{i-1} b_i) + z c_1 + w d_1, \end{aligned}$$

where $x_0 = x_r$ and $y_0 = y_r$. Thus, $x_i = x_{i-1}$ and $y_i = y_{i-1}$ and, hence:

$$
\begin{aligned}
k_1 &= \Sigma_{i=1}^r (x_1 a_i + y_1 b_i) + z c_1 + w d_1 \\
&= \Sigma_{i=1}^r (x_1 \sigma^{i-1} a_1 + y_1 \sigma^{i-1} b_1) + z c_1 + w d_1 \\
&= (\Sigma_{i=1}^r \sigma^{i-1})(x_1 a_1 + y_1 b_1) + z c_1 + w d_1.
\end{aligned}
$$

Suppose that ψ is supported on the annular neighborhood A of K. The preimage $p^{-1}(A)$ is an annular neighborhood A_1 of K_1 and the restriction $p| : A_1 \to A$ is a connected r-fold cyclic covering of A. There is an obvious lift $\tilde{\phi}$ of ϕ, where $\tilde{\phi}$ is a right Dehn twist about K_1 supported on A_1. Using the fact that $\tilde{\phi}$ acts on $\mathrm{H}_1(\tilde{S})$ as the transvection corresponding to the class of K_1 in $\mathrm{H}_1(\tilde{S})$, we have the following identities:

$$
\begin{aligned}
\tilde{\phi}_*(e_1) &= \tilde{\phi}_*((1-\sigma)a_1) = (1-\sigma)\tilde{\phi}_*(a_1) \\
&= (1-\sigma)(a_1 + \langle k_1, a_1\rangle k_1) \\
&= e_1 + \langle k_1, a_1\rangle (1-\sigma) k_1.
\end{aligned}
$$

On the other hand:

$$
\begin{aligned}
(1-\sigma)k_1 &= (1-\sigma)(\Sigma_{i=1}^r \sigma^{i-1})(x_1 a_1 + y_1 b_1) \\
&\quad + z(1-\sigma)c_1 + w(1-\sigma)d_1 \\
&= (1-\sigma^r)(x_1 a_1 + y_1 b_1) = 0.
\end{aligned}
$$

Thus, $\tilde{\phi}_*(e_1) = e_1$. Likewise, $\tilde{\phi}_*(f_1) = f_1$ and, hence, $\tilde{\phi}_* = I$, where $I : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(\tilde{S})$ is the identity homomorphism. □

Lemma 2.11 *Suppose that $r = 2$ and $\phi : S \to S$ represents an element of the level r subgroup $\Gamma_r(S)$ of $\mathcal{M}_S$. Then ϕ represents an element of $Stab_\rho$ and for each lift $\tilde{\phi}$ of ϕ, $\tilde{\phi}_* \in \mathrm{SL}(2, \mathbb{Z})$.*

PROOF. Since $\Gamma_r(S) \subset Stab_\rho$, ϕ represents an element of $Stab_\rho$. Thus, for each lift $\tilde{\phi}$ of ϕ, $\tilde{\phi}_* \in \mathrm{GL}(2, \mathbb{Z}[\zeta])$. Since $r = 2$, $\zeta = \mathrm{e}^{\mathrm{i}2\pi/r} = -1$ and, hence, $\mathbb{Z}[\zeta] = \mathbb{Z}$.

The lift $\tilde{\phi}$ of ϕ is well-defined up to composition with the unique nontrivial covering transformation σ. σ acts on Λ as $-I$, where I is the identity homomorphism $\Lambda \to \Lambda$. Since the determinant of $-I$ is equal to 1, it suffices to prove that there exists a lift $\tilde{\phi}$ of ϕ such that $\tilde{\phi}_*$ has determinant equal to 1.

In order to prove existence, it suffices to construct appropriate lifts of each of the classes of types (i) and (ii) in Theorem 2.8. For classes of type (i), such a lift exists by Lemma 2.9. For classes of type (ii), such a lift exists by Lemma 2.10, provided $\langle C, K\rangle \not\equiv 0 \pmod r$. Suppose, therefore, that K is a nonseparating circle on S, and $\langle C, K\rangle \equiv 0 \pmod r$. Let $\phi = t_K$. By Lemma 2.9, ϕ represents an element of $Stab_\rho$ and there exists a lift $\tilde\phi$ of ϕ such that $\tilde\phi_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$. Clearly, $\tilde\phi^r$ is a lift of ϕ^r. Since $t_K^r = \phi^r$, $\tilde\phi^r$ is a lift of t_K^r. On the other hand, since $\tilde\phi_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$, $\tilde\phi^r \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$. □

Suppose that ϕ is a representative of an element γ of $\Gamma_r(S)$. As observed above, the lift $\tilde\phi$ of ϕ is well-defined up to composition with the unique nontrivial covering transformation σ. Since σ acts on Λ as $-I$, we obtain a well-defined element $[\tilde\phi_* : \Lambda \to \Lambda]$ of $\mathrm{PSL}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})/\pm I$, independently of the lift $\tilde\phi$ of ϕ. Suppose that ψ is another representative of γ. We may lift an isotopy ϕ_t from $\phi_0 = \phi$ to $\phi_1 = \psi$ to an isotopy $\tilde\phi_t$. Then $\tilde\phi_0$ and $\tilde\phi_1$ are isotopic lifts of ϕ and ψ, respectively. It follows that $\tilde\phi_* = \tilde\psi_* : \Lambda \to \Lambda$ and, hence, $[\tilde\phi_*] = [\tilde\psi_*] \in \mathrm{PSL}(2, \mathbb{Z})$. Thus, we have the following result.

Theorem 2.12 *Let $r = 2$ and $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$. Then there is a well-defined representation $\lambda : \Gamma_r(S) \to \mathrm{PSL}(2, \mathbb{Z})$ given by the rule $\gamma \mapsto [\tilde\phi_*]$, where $\phi \in \gamma$ and $\tilde\phi$ is any lift of ϕ.*

Suppose now that $r > 2$. Since r is a prime, r is odd. Since $\zeta \cdot v = \sigma_*(v)$ for each $v \in \Lambda$, the action of σ on Λ is given by the diagonal matrix ζI. This matrix has determinant ζ^2. Since r is odd, ζ^2 is a generator of the cyclic group of order r generated by $\zeta = \mathrm{e}^{\mathrm{i}2\pi/r}$.

Lemma 2.13 *Suppose that $r > 2$ is a prime. Let $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$ and $\phi : S \to S$ represent an element of $\Gamma_r(S)$. Then ϕ represents an element of $Stab_\rho$ and there exists a unique lift $\tilde\phi$ of ϕ such that $\tilde\phi_* \in \mathrm{GL}(2, \mathbb{Z}[\zeta])$ has determinant equal to 1. Moreover, for this unique lift $\tilde\phi$ of ϕ, $\tilde\phi_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$.*

PROOF. Since $\Gamma_r(S) \subset Stab_\rho$, ϕ represents an element of $Stab_\rho$.

Suppose that $\tilde\phi$ and ψ are lifts of ϕ such that the determinants of $\tilde\phi_*$ and ψ_* are equal to 1. There exists an integer j such that $\psi = \tilde\phi \circ \sigma^j$. Since σ acts on Λ by the diagonal matrix ζI, $1 = det(\psi_*) = det(\tilde\phi_*)det(\zeta^j I) = \zeta^{2j} = \mathrm{e}^{\mathrm{i}2\pi j/r}$. Hence, $2j/r \in \mathbb{Z}$. Since r is odd, we conclude that $j = mr$ for some integer m. Thus, $\sigma^j = \sigma^{mr} = 1$ and, hence, $\psi = \tilde\phi \circ \sigma^j = \tilde\phi$. This establishes uniqueness.

In order to prove existence, it suffices to construct appropriate lifts of each of the classes of types (i) and (ii) in Theorem 2.8. For classes of type (i), such a lift exists by Lemma 2.9. For classes of type (ii), such a lift exists by Lemma 2.10, provided $\langle C, K\rangle \not\equiv 0 \pmod r$. Suppose, therefore, that K is a nonseparating circle on S, and $\langle C, K\rangle \equiv 0 \pmod r$. Let $\phi = t_K$. By Lemma 2.9, ϕ represents an element of $Stab_\rho$ and there exists a lift $\tilde\phi$ of ϕ such that

$\tilde{\phi}_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$. Since $t_K^r = \phi^r$, $\tilde{\phi}^r$ is a lift of t_K^r. On the other hand, since $\tilde{\phi}_* \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$, $\tilde{\phi}^r \in \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$. $\square$

By the uniqueness clause of the previous proposition, we obtain the following result.

Theorem 2.14 *Let $r > 2$ be a prime and $\Gamma_r(S)$ be the level r subgroup of $\mathcal{M}_S$. Then there is a well-defined representation $\lambda : \Gamma_r(S) \to \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$ given by the rule $\gamma \mapsto \tilde{\phi}_*$, where $\phi \in \gamma$ and $\tilde{\phi}$ is the unique lift of ϕ such that $\tilde{\phi}_* \in \mathrm{GL}(2, \mathbb{Z}[\zeta])$ has determinant equal to 1.*

We now wish to understand the images of the representations (i) $\lambda : \Gamma_r(S) \to \mathrm{PSL}(2, \mathbb{Z})$, when $r = 2$, and (ii) $\lambda : \Gamma_r(S) \to \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$, when $r > 2$.

Let $\Gamma_r(\mathbb{Z}[\zeta])$ be the level r subgroup of $\mathrm{GL}(2, \mathbb{Z}[\zeta])$.

Lemma 2.15 *Suppose that K is a nonseparating circle on S such that $\langle C, K \rangle \equiv 0 \pmod r$. Let ψ be the right Dehn twist about K, $\phi = \psi^r$ and $\tilde{\phi}$ be a lift of ϕ to $\tilde{S}$. If $r > 2$, let $\tilde{\phi}$ be the unique lift of ϕ given by Lemma 2.13. Then $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z}[\zeta])$.*

PROOF. Note that $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z}[\zeta])$ if and only if, for every element f of Λ, there exists an element h of Λ such that $\tilde{\phi}_*(f) = f + rh$.

As we saw previously, K lifts to a circle K_1 in $\tilde{S}$ such that the preimage $p^{-1}(K)$ is the disjoint union of r circles $K_1, ..., K_r$ with $K_i = \sigma^{i-1}(K_1)$. Moreover, there is a lift Ψ of ψ such that $\Psi = \psi_1 \circ ... \circ \psi_r$, where ψ_i is a right Dehn twist about the circle K_i in $\tilde{S}$. Let $\Phi = (\Psi)^r$. Since Ψ is a lift of ψ, Φ is a lift of ϕ.

Suppose that $r = 2$. Then $\tilde{\phi}_* = \pm\Phi_*$. Since $-I = I - 2I$, $-I \in \Gamma_r(\mathbb{Z}[\zeta])$. Since $\Gamma_r(\mathbb{Z}[\zeta])$ is a subgroup of $\mathrm{GL}(2, \mathbb{Z}[\zeta])$, it follows that $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z}[\zeta])$ if and only if $\Phi_* \in \Gamma_r(\mathbb{Z}[\zeta])$. Hence, we may assume that $\tilde{\phi} = \Phi$ and, hence, $\tilde{\phi} = \psi_1^r \circ ... \circ \psi_r^r$.

Suppose, on the other hand, that $r > 2$. Then, as we saw above, Φ is the unique lift of ϕ given by Lemma 2.13. Thus, by our assumptions, $\tilde{\phi} = \Phi$ and, hence, $\tilde{\phi} = \psi_1^r \circ ... \circ \psi_r^r$.

Thus, in any case, we may assume that $\tilde{\phi} = \psi_1^r \circ ... \circ \psi_r^r$.

Orient K_i so that the restriction $p| : K_i \to K$ is orientation-preserving and let k_i be the element of $\mathrm{H}_1(\tilde{S})$ represented by the oriented circle K_i. Let $l_i = (1 - \sigma)k_i$. Since σ is a covering transformation, l_i is in the kernel Λ of the homomorphism $p_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(S)$.

Let $f \in \Lambda$. Since e_1, f_1 is a $\mathbb{Z}[\zeta]$-basis for Λ, we may express f in terms of e_1 and f_1: $f = xe_1 + yf_1$, where $x, y \in \mathbb{Z}[\zeta]$. Let u and v be elements of $\mathbb{Z}G$ such that the natural homomorphism $\mathbb{Z}G \to \mathbb{Z}[\zeta]$ given by the rule $\sigma \mapsto \zeta$ maps u to x and v to y. Then, we have the following identities:

$$\begin{aligned} f &= xe_1 + yf_1 = x(1-\sigma)a_1 + y(1-\sigma)b_1 \\ &= u(1-\sigma)a_1 + v(1-\sigma)b_1 \\ &= (1-\sigma)(ua_1 + vb_1). \end{aligned}$$

Thus, there exists an element g in $\mathrm{H}_1(\tilde{S})$ such that $f = (1-\sigma)g$.

Since ψ_i is a right Dehn twist about the circle K_i on $\tilde{S}$, we have the following identities:

$$\begin{aligned} \tilde{\phi}_*(f) &= \tilde{\phi}_*((1-\sigma)g) \\ &= (1-\sigma)\tilde{\phi}_*(g) \\ &= (1-\sigma)(z + \Sigma_{i=1}^r r\langle k_i, g\rangle k_i) \\ &= w + r(\Sigma_{i=1}^r \langle k_i, g\rangle (1-\sigma)k_i) \\ &= w + r(\Sigma_{i=1}^r \langle k_i, g\rangle l_i) \end{aligned}$$

Thus, there exists an element $h = \Sigma_{i=1}^r \langle k_i, g\rangle l_i$ in Λ such that $\tilde{\phi}_*(g) = g + rh$. $\square$

We recall that two circles K and L on S are in minimal position if (i) K and L are transverse, and (ii) $\#(K \cap L) \leq \#(K' \cap L')$ for every pair of circles (K', L') on S such that K' is isotopic to K and L' is isotopic to L. (Note that two transverse circles K and L on S are in minimal position if no simply connected component R of $S \setminus (K \cup L)$ is bounded by the union of an arc α of K and an arc β of L such that $\partial\alpha = \alpha \cap \beta = \partial\beta$ (Exposé 3, Proposition 10, [3]). In particular, if there are no simply connected components of $S \setminus (K \cup L)$, then K and L are in minimal position.)

Since $\zeta^r = 1$, the ring $\mathbb{Z}[\zeta]$ is generated by ζ. There is a unique ring homomorphism $\epsilon : \mathbb{Z}[\zeta] \to \mathbb{Z}_r$ given by the rule $\zeta \mapsto 1$. This homomorphism determines a natural homomorphism of groups $\epsilon : \mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$. Let Γ_ϵ be the kernel of $\epsilon : \mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$.

Lemma 2.16 *Let ϕ be a right Dehn twist about a separating circle K on S and $\tilde{\phi}$ be a lift of ϕ. If $r > 2$, let $\tilde{\phi}$ be the unique lift of ϕ given by Lemma 2.13. Then $\tilde{\phi}_* \in \Gamma_\epsilon$.*

PROOF. Choose an orientation of K. As in the proof of Lemma 2.9, we conclude that the preimage $p^{-1}(K)$ consists of r disjoint circles $K_1, ..., K_r$ in $\tilde{S}$ such that $K_i = \sigma^{i-1}(K_1)$. As in the proof of Lemma 2.9, orient K_i so that $p| : K_i \to K$ is orientation-preserving, and let k_i be the element of $\mathrm{H}_1(\tilde{S})$ represented by K_i. Following the proof of Lemma 2.9, express k_1 in terms of the basis $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ of $\mathrm{H}_1(\tilde{S})$:

$$k_1 = \Sigma_{i=1}^{r}(x_i a_i + y_i b_i) + z c_1 + w d_1,$$

and let $x = \Sigma_{i=1}^{r} x_i \zeta^{i-1} \in \mathbb{Z}[\zeta]$ and $y = \Sigma_{i=1}^{r} y_i \zeta^{i-1} \in \mathbb{Z}[\zeta]$.

As in the proof of Lemma 2.9, we conclude that, with respect to the $\mathbb{Z}[\zeta]$-module basis (e_1, f_1), the action of $\tilde{\phi}$ on Λ is given by the matrix:

$$\tilde{\phi}_* = \begin{pmatrix} 1 - x\overline{y} & x\overline{x} \\ -y\overline{y} & 1 + \overline{x}y \end{pmatrix}.$$

Since K is separating, K represents the element 0 of $\mathrm{H}_1(S)$. Since $p(K_1) = K$, k_1 is in the kernel Λ of $p_* : \mathrm{H}_1(\tilde{S}) \to \mathrm{H}_1(S)$. Hence, we may express k_1 in terms of the $\mathbb{Z}[\zeta]$ basis (e_1, f_1) of Λ:

$$k_1 = u e_1 + v f_1,$$

where $u, v \in \mathbb{Z}[\zeta]$. Let w and z be elements of $\mathbb{Z}G$ such that the natural homomorphism $\mathbb{Z}G \to \mathbb{Z}[\zeta]$ given by the rule $\sigma \mapsto \zeta$ maps w to u and z to v. Then, by the definitions of e_1 and f_1, we have the following identities:

$$\begin{aligned} k_1 &= u e_1 + v f_1 = w e_1 + z f_1 \\ &= w(1-\sigma)a_1 + z(1-\sigma)b_1. \end{aligned}$$

Comparing the previous equations, using the fact that $(a_1, b_1, ..., a_r, b_r, c_1, d_1)$ is a basis for $\mathrm{H}_1(\tilde{S})$, we conclude that $x = u(1-\zeta)$ and $y = v(1-\zeta)$. Thus, the ring homomorphism $\epsilon : \mathbb{Z}[\zeta] \to \mathbb{Z}_r$ given by the rule $\zeta \mapsto 1$ maps x and y to 0. Hence, by the previous equation for $\tilde{\phi}_*$, the natural homomorphism of groups $\epsilon : \mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$ maps $\tilde{\phi}_*$ to $I \in \mathrm{GL}(2, \mathbb{Z}_r)$. That is, $\tilde{\phi}_*$ is in the kernel Γ_ϵ of $\epsilon : \mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$. $\square$

Lemma 2.17 *Suppose that $r = 2$ and let $\Gamma_r(S)$ be the level 2 subgroup of $\mathcal{M}_S$. Then, the homomorphism $\lambda : \Gamma_r(S) \to \mathrm{PSL}(2, \mathbb{Z})$ of Theorem 2.12 takes its values in the image under the natural homomorphism $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{PSL}(2, \mathbb{Z})$ of the level 2 subgroup $\Gamma_r(\mathbb{Z})$ of $\mathrm{SL}(2, \mathbb{Z})$.*

PROOF. Suppose that $\phi : S \to S$ represents an element of $\Gamma_r(S)$ and $\tilde{\phi}$ is a lift of ϕ. It suffices to show that $\tilde{\phi}_*$ lies in the level 2 subgroup of $\mathrm{SL}(2, \mathbb{Z})$.

By Theorem 2.8, we may assume that ϕ is one of the homeomorphisms of type (i) or (ii) in Theorem 2.8.

Suppose that ϕ is a Dehn twist about a nontrivial separating circle K on S. By Lemma 2.16, $\tilde{\phi}_*$ lies in Γ_ϵ, the kernel of the natural homomorphism $\mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$ given by the rule $\zeta \mapsto 1$. Since $r = 2$, $\zeta = -1$ and, hence, $\mathbb{Z}[\zeta] = \mathbb{Z}$. Moreover, the natural homomorphism $\mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$ is the natural homomorphism $\mathrm{GL}(2, \mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}_r)$ corresponding to the natural homomorphism $\mathbb{Z} \to \mathbb{Z}_r$. Hence, Γ_ϵ is the level 2 subgroup of $\mathrm{GL}(2, \mathbb{Z})$. We conclude that $\tilde{\phi}_*$ lies in the level 2 subgroup of $\mathrm{GL}(2, \mathbb{Z})$. On the other hand, by Lemma 2.11, $\tilde{\phi}_*$ lies in $\mathrm{SL}(2, \mathbb{Z})$. Hence, $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$.

We may assume, therefore, that ψ is a Dehn twist about a nonseparating circle K on S and $\phi = \psi^r$. Suppose that $\langle C, K \rangle \not\equiv 0 \pmod r$. By Lemma 2.10, there exists a lift Φ of ϕ such that $\Phi_* = I$. Thus, $\tilde{\phi}_* = \pm I$, and, hence, $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$.

Suppose, on the other hand, that $\langle C, K \rangle \equiv 0 \pmod r$. Then, by Lemma 2.15, $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z}[\zeta])$. Since $r = 2$, $\Gamma_r(\mathbb{Z}[\zeta])$ is the level 2 subgroup of $\mathrm{GL}(2, \mathbb{Z})$. As before, we conclude that $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$. $\square$

Lemma 2.18 *Suppose that $r = 3$ and let $\Gamma_r(S)$ be the level 3 subgroup of $\mathcal{M}_S$. Then, the homomorphism $\lambda : \Gamma_r(S) \to \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$ of Theorem 2.14 takes its values in the level 3 subgroup $\Gamma_r(\mathbb{Z})$ of $\mathrm{SL}(2, \mathbb{Z})$.*

PROOF. Since $r = 3$, $\zeta = \mathrm{e}^{\mathrm{i}2\pi/3}$ and, hence $\zeta + \overline{\zeta} = -1$. It follows that $\mathbb{Z}[\zeta] \cap \mathbb{R} = \mathbb{Z}$. Hence, $\mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R}) = \mathrm{SL}(2, \mathbb{Z})$.

Suppose that $\phi : S \to S$ represents an element of $\Gamma_r(S)$ and $\tilde{\phi}$ is the unique lift of ϕ given by Lemma 2.13. It suffices to show that $\tilde{\phi}_*$ lies in the level 3 subgroup of $\mathrm{SL}(2, \mathbb{Z})$.

By Theorem 2.8, we may assume that ϕ is one of the homeomorphisms of type (i) or (ii) in Theorem 2.8.

Suppose that ϕ is a Dehn twist about a nontrivial separating circle K on S. By Lemma 2.16, $\tilde{\phi}_*$ lies in Γ_ϵ, the kernel of the natural homomorphism $\mathrm{GL}(2, \mathbb{Z}[\zeta]) \to \mathrm{GL}(2, \mathbb{Z}_r)$ given by the rule $\zeta \mapsto 1$. In other words, $\epsilon(\tilde{\phi}_*) = I \in \mathrm{GL}(2, \mathbb{Z}_r)$. The restriction of the homomorphism $\epsilon : \mathbb{Z}[\zeta] \to \mathbb{Z}_r$ to $\mathbb{Z} \subset \mathbb{Z}[\zeta]$ is the natural homomorphism $\mathbb{Z} \to \mathbb{Z}_r$. Hence, we conclude that $\tilde{\phi}_*$ is in the kernel of the natural homomorphism $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}_r)$. In other words, $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$.

We may assume, therefore, that ψ is a Dehn twist about a nonseparating circle K on S and $\phi = \psi^r$. Suppose that $\langle C, K\rangle \not\equiv 0 \pmod r$. By Lemma 2.10, there exists a lift Φ of ϕ such that $\Phi_* = I$. Clearly, Φ is the unique lift of ϕ given by Lemma 2.13. Thus, by our assumption, $\tilde{\phi} = \Phi$ and, hence, $\tilde{\phi}_* = I \in \mathrm{GL}(2, \mathbb{Z}[\zeta])$. This implies that $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$.

Suppose, on the other hand, that $\langle C, K\rangle \equiv 0 \pmod r$. Then, by Lemma 2.15, $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z}[\zeta])$. Clearly, $\Gamma_r(\mathbb{Z}[\zeta]) \subset \Gamma_\epsilon$. Hence, $\tilde{\phi}_* \in \Gamma_\epsilon$. As before, we conclude that $\tilde{\phi}_* \in \Gamma_r(\mathbb{Z})$. $\square$

We have the following well-known result.

Theorem 2.19 *Let $\Gamma_r(\mathbb{Z})$ be the level r subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and $P\Gamma_r(\mathbb{Z})$ be its image in $\mathrm{PSL}(2,\mathbb{Z})$ under the natural homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z})$. Then $\Gamma_r(\mathbb{Z})$ is a free group, provided $r \geq 3$, and $P\Gamma_r(\mathbb{Z})$ is a free group, provided $r \geq 2$.*

PROOF. The group $\mathrm{PSL}(2,\mathbb{Z})$ is isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_3$, where the subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ corresponding to the factors $\mathbb{Z}_2$ and $\mathbb{Z}_3$ of $\mathbb{Z}_2 * \mathbb{Z}_3$ are the cyclic subgroups generated, respectively, by the classes $[X]$ and $[Y]$ in $\mathrm{PSL}(2,\mathbb{Z})$ of the matrices ([15]):

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

(The generators of $\mathrm{PSL}(2,\mathbb{Z})$ given here correspond to the "transposes" of those given in [15].) Note that:

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

Suppose that $[W]$ is a nontrivial element of finite order in $P\Gamma_r(\mathbb{Z})$. By Corollary 4.4.5 on page 208 of [11], $[W]$ must be a conjugate in $\mathrm{PSL}(2,\mathbb{Z})$ of $[X]$, $[Y]$ or $[Y^2]$. Since $\Gamma_r(\mathbb{Z})$ is a normal subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and the natural homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z})$ is surjective, $P\Gamma_r(\mathbb{Z})$ is a normal subgroup of $\mathrm{PSL}(2,\mathbb{Z})$. Hence, we may assume that $[W]$ is equal to $[X]$, $[Y]$ or $[Y^2]$. On the other hand, clearly, none of the elements $\pm X$, $\pm Y$, $\pm Y^2$ in the preimages of $[X]$, $[Y]$ and $[Y^2]$ lie in $\Gamma_r(\mathbb{Z})$, if $r \geq 2$. This proves that $P\Gamma_r(\mathbb{Z})$ is torsion free, provided $r \geq 2$.

The group $\mathrm{PSL}(2,\mathbb{Z})$ acts on the hyperbolic plane $\mathbb{H}^2$ as a discrete group of isometries of the Poincare metric. The quotient of $\mathbb{H}^2$ by this action is an hyperbolic orbifold M of dimension 2 with one cusp. In particular, M is noncompact.

Suppose that $r \geq 2$. Since $P\Gamma_r(\mathbb{Z})$ is torsion free, $P\Gamma_r(\mathbb{Z})$ acts properly discontinuously and freely on $\mathbb{H}^2$. The quotient M_r of $\mathbb{H}^2$ by the action of $P\Gamma_r(\mathbb{Z})$ is, therefore, an hyperbolic surface. The natural projection $\mathbb{H}^2 \to M$ induces a surjective map $M_r \to M$. Hence, M_r is a noncompact surface. It follows that the fundamental group $\pi_1(M_r)$ of M_r is a free group. On the other hand, since $\mathbb{H}^2$ is simply connected, $\pi_1(M_r)$ is isomorphic to $P\Gamma_r(\mathbb{Z})$. We conclude that $P\Gamma_r(\mathbb{Z})$ is a free group, provided $r \geq 2$.

Suppose that $r \geq 3$. Clearly, $-I$ is not in $\Gamma_r(\mathbb{Z})$. Since the kernel of the natural homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z})$ is equal to $\{\pm I\}$, it follows that the restriction $\Gamma_r(\mathbb{Z}) \to P\Gamma_r(\mathbb{Z})$ of this homomorphism is an isomorphism. Since $P\Gamma_r(\mathbb{Z})$ is a free group, $\Gamma_r(\mathbb{Z})$ is a free group. $\square$

We are now ready to give the proof of Theorem 2.1.

Proof of Theorem 2.1: $\mathcal{M}_S$ acts naturally on $\mathrm{H}_1(S,\mathbb{Z}_r)$. Since $\mathrm{H}_1(S,\mathbb{Z}_r)$ is finite, the kernel $\Gamma_r(S)$ of this action is a subgroup of finite index in $\mathcal{M}_S$. Let p be a prime factor of r. Since $\Gamma_r(S)$ acts trivially on $\mathrm{H}_1(S,\mathbb{Z}_r)$, $\Gamma_r(S)$ acts trivially on $\mathrm{H}_1(S,\mathbb{Z}_p)$. Hence, $\Gamma_r(S)$ is contained in the kernel Γ' of the action of $\mathcal{M}_S$ on $\mathrm{H}_1(S,\mathbb{Z}_p)$. Since $\Gamma_r(S)$ has finite index in $\mathcal{M}_S$, $\Gamma_r(S)$ has finite index in Γ'. Suppose that $\mathrm{H}^1(\Gamma')$ is nontrivial. Then there exists a nontrivial homomorphism $\lambda : \Gamma' \to \mathbb{Z}$. Since $\Gamma_r(S)$ has finite index in Γ', the restriction $\lambda| : \Gamma_r(S) \to \mathbb{Z}$ of λ to $\Gamma_r(S)$ is nontrivial. Hence, $\mathrm{H}^1(\Gamma_r(S))$ is nontrivial. Thus, we may assume that r is equal to 2 or 3.

Suppose that $r = 2$. By Lemma 2.17, the homomorphism $\lambda : \Gamma_r(S) \to \mathrm{PSL}(2,\mathbb{Z})$ of Theorem 2.12 takes its values in the image $P\Gamma_r(\mathbb{Z})$ under the natural homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z})$ of the level r subgroup $\Gamma_r(\mathbb{Z})$ of $\mathrm{SL}(2,\mathbb{Z})$. By Theorem 2.19, $P\Gamma_r(\mathbb{Z})$ is free.

Let ϕ denote the Dehn twist about the curve A on S. Then ϕ represents an element of $Stab_\rho$ and, by the proof of Lemma 2.9:

$$\tilde{\phi}_* = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

On the other hand, ϕ^r represents an element of $\Gamma_r(S)$ and:

$$\tilde{\phi^r}_* = \begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}.$$

Hence, $\lambda(\Gamma_r(S))$ is a nontrivial subgroup of $P\Gamma_r(\mathbb{Z})$. Since $P\Gamma_r(\mathbb{Z})$ is free, $\lambda(\Gamma_r(S))$ is a nontrivial free group. Hence, there exists a surjective homomorphism $\nu : \lambda(\Gamma_r(S)) \to \mathbb{Z}$. The composition $\nu \circ \lambda : \Gamma_r(S) \to \mathbb{Z}$ is a surjective homomorphism and, hence, $\mathrm{H}^1(\Gamma_r(S))$ is nontrivial.

Suppose, on the other hand, that $r = 3$. Then, by Lemma 2.18, the homomorphism $\lambda : \Gamma_r(S) \to \mathrm{SL}(2, \mathbb{Z}[\zeta] \cap \mathbb{R})$ of Theorem 2.14 takes its values in the level 3 subgroup $\Gamma_r(\mathbb{Z})$ of $\mathrm{SL}(2, \mathbb{Z})$. By Theorem 2.19, $\Gamma_r(\mathbb{Z})$ is free.

As in the previous case, we conclude that $\mathrm{H}^1(\Gamma_r(S))$ is nontrivial. $\square$

References

[1] Bass, H., Milnor, J. and Serre, J.-P., Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. *Publications Mathematiques IHES,* 1967, **33**, 59–137.

[2] Birman, J. S., On Siegel's modular group. *Math. Ann.,* 1971, **191**, 59–68.

[3] Fathi, A., Laudenbach, F., Poénaru, V., Travaux de Thurston sur les surfaces. *Astérisque,* 1979, **66–67**, 1–284.

[4] Hain, R. and Looijenga, E., Mapping class groups and moduli spaces of curves. In: *Algebraic geometry–Santa Cruz 1995,* Proc. Sympos. Pure Math., 62, Part 2. Amer. Math. Soc., Providence, RI, 1997, pp. 97–142.

[5] Harvey, W. J., Geometric structure of surface mapping-class groups. In: *Homological group theory*, Ed. by C. T. C. Wall, London Mathematical Society, Lecture Notes Series, Vol. 36. Cambridge University Press, Cambridge, 1979, pp. 255–269.

[6] Johnson, D., Homeomorphisms of a surface which act trivially on homology. *Proc. of the AMS,* 1979, **75**, 119–125.

[7] Johnson, D., Conjugacy relations in subgroups of the mapping class group and a group theoretic description of the Rochlin invariant. *Math. Ann.,* 1980, **249**, 243–263.

[8] Kajdan, D. A., Connection of the dual space of a group with the structure of its closed subgroups. *J. Func. Anal. Appl.,* 1967, 63–65.

[9] Kirby, R., Problems in low-dimensional topology. In: *Geometric Topology*, ed. W. H. Kazez, AMS/IP Studies in Advanced Mathematics, vol. 2, Part 2. American Mathematical Society and International Press, 1997, pp. 35–473.

[10] Looijenga, E., Prym representations of mapping class groups. *Geom. Dedicata,* 1997, **64**, 69–83.

[11] Magnus, W., Karrass, A., and Solitar, D., *Combinatorial Group Theory.* Dover, New York, 1976.

[12] Mennicke, J., Zur Theorie der Siegelschen Modulgruppe. *Math. Annalen,* 1965, **159**, 115–129.

[13] Millson, J. J., On the first Betti number of a constant negatively curved manifold. *Ann. of Math.,* 1976, **104**, 235–247.

[14] Powell, J., Two theorems on the mapping class group of a surface. *Proc. AMS,* 1978, **68**, 347–350.

[15] Serre, J.-P., *Trees.* Springer-Verlag, Berlin-New York, 1980.