PRYM REPRESENTATIONS OF MAPPING CLASS GROUPS

Eduard Looijenga

In memory of Nicolaas H. Kuiper (1920-1994)

Abstract. Let S be a closed orientable surface of genus at least two and let $\tilde{S} \to S$ be a connected finite abelian covering with covering group G. The lifts of liftable mapping classes of S determine a central extension (by G) of a subgroup of finite index of the mapping class group of S. This extension acts on $H_1(\tilde{S})$. With a few exceptions for genus two, we determine the Zariski closure of the image of this representation, and prove that the image is an arithmetic group.

Introduction

This paper deals with arithmetic representations of the mapping class group of genus $g \geq 2$ that arise from abelian coverings. They are defined as follows. Suppose S is a closed orientable surface of genus $g \geq 2$ and $\tilde{S} \to S$ is a connected finite abelian covering with covering group G. The mapping classes of S that lift to $\tilde{S}$ are those that leave the kernel of the natural map $H_1(S) \to G$ invariant. (When in a homology group no coefficient group is mentioned we always mean integral coefficients.) Let $\Gamma_{S,G}$ be the set of mapping classes that in addition induce the identity on G; this is a subgroup of finite index in the mapping class group Γ_S of S. Given $f \in \Gamma_{S,G}$ and a lift $\tilde{f} \in \Gamma_{\tilde{S}}$, then $\tilde{f}$ commutes with the covering transformations, and every other lift is the composition of $\tilde{f}$ and a covering transformation. Let Sp_G be the group of symplectic transformations of $H_1(\tilde{S})$ that commute with the action of the covering group G. Its center contains the image of G, so if PSp_G denotes the quotient of Sp_G by its center, then we have a well-defined homomorphism $\Gamma_{S,G} \to PSp_G$. One of our main results implies that the image of this homomorphism is a subgroup of PSp_G of finite index, at least if $g \geq 3$. (If $g = 2$ our proof only works in case the order of G is relatively prime to 6.)

The analogously defined group $PSp_G(\mathbb{Q})$ is in a natural way the group of rational points of a semi-simple algebraic group defined over $\mathbb{Q}$, and as we will see, its simple quotients are naturally indexed in a one–to–one manner by the cyclic quotient groups of G. A nontrivial cyclic quotient of order n corresponds to a factor which is definable over the number field $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ followed by restriction of scalars. For $n \geq 3$, this is a projectivized unitary group of rank $g-1$, for $n = 2$ it is a

Key words and phrases. Prym covering, mapping class group, arithmetic group.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

projectivized symplectic group of rank $g-1$, and if $n=1$, we are dealing with the standard projectivized representation of Γ_S on $H_1(S)$ (of rank g). We actually obtain a precise description of the image in each factor. All of this is functorial in G, so that these factors are in fact labeled by the finite cyclic quotients of $H_1(S)$, or equivalently, by the cyclic subgroups of $H^1(S;\mathbb{Q}/\mathbb{Z})$. So there is no upper bound on the rank of an arithmetically defined quotient of a finite index subgroup of Γ_S.

Finally a somewhat philosophical remark. Since the pioneering work of D. Johnson, the kernel of the standard symplectic representation of Γ_S on $H_1(S)$, called the *Torelli group*, has come under close scrutiny. In many investigations, including Johnson's, this group is studied via its nilpotent quotients. This is a sensible approach for many reasons, one being that this group is known to be residually torsion free nilpotent. But our results show that the Torelli group can be mapped onto an arithmetic subgroup of a $\mathbb{Q}$-semi-simple algebraic groups whose $\mathbb{Q}$-rank may be arbitrary large, a property which is obviously not shared by any of its nilpotent quotients. So passing to its pronilpotent completion results in loss of some important arithmetic properties. Incidentally, it could be worthwhile to identify the cohomology classes of the Torelli group that arise from these Prym representations.

Acknowledgements. This work started as a joint effort with Dick Hain, while he was visiting the University of Utrecht with grants provided by the Dutch Organization for the Advancement of Scientific Research (NWO) and the Mathematics Department of the University of Utrecht. I am indebted to him for many inspiring conversations on this topic, and I thank NWO and my department for supporting his visit.

1. Skew-hermitian modules

(1.1) Let G be a finite abelian group. A *character* of G is by definition a homomorphism from G to the multiplicative group of a (fixed) algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The characters of G also form a finite abelian group, called the *dual of* G that is denoted by $\widehat{G}$. Notice that G is naturally isomorphic to its double dual.

Any character $\chi\in\widehat{G}$ extends to a ring homomorphism $\tilde{\chi}:\mathbb{Z}[G]\to\overline{\mathbb{Q}}$. If the image of χ has order d, then the image of χ, resp. $\tilde{\chi}$, will be the group of d-th roots of unity in $\overline{\mathbb{Q}}$, resp. the ring of integers generated by these. If $\sigma\in\operatorname{Aut}(\overline{\mathbb{Q}})$, then σ raises every primitive d-th root of unity to a power k with $(k,d)=1$, and so $\sigma\chi:=\chi^k$. It follows that the $\operatorname{Aut}(\overline{\mathbb{Q}})$-orbit of χ in $\widehat{G}$ is precisely the set of generators of the cyclic subgroup generated by χ. For this reason we prefer to do our constructions in terms of a cyclic subgroup of $\widehat{G}$, rather than in terms of a single element. Notice that a cyclic factor group C of G dualizes to a cyclic subgroup $\widehat{C}$ of $\widehat{G}$ and vice versa. (We should perhaps explicitly state that two factor groups G/H_1, G/H_2 are considered identical if and only if $H_1=H_2$.) We shall denote the set of cyclic factor groups of G by $X(G)$; it includes the trivial group 0.

Let a cyclic factor group C of G be given. If χ is a generator of its dual $\widehat{C}\subset\widehat{G}$, then the kernel of $\tilde{\chi}$ depends on C only; we therefore denote it by I_C, and we put $R_C:=\mathbb{Z}[G]/I_C$, $K_C:=\mathbb{Q}\otimes R_C$. So K_C is isomorphic to the subfield of $\overline{\mathbb{Q}}$ generated by its $|C|$th roots of unity (but not canonically) and R_C is its ring of integers. Notice that the involution "bar" of $\mathbb{Q}[G]$ which inverts the generators,

$$\overline{\sum_{g\in G} c_g g} := \sum_{g\in G} c_g g^{-1},$$

induces in each factor K_C the standard involution ("complex conjugation"). The elements of K_C fixed under this involution form the maximal (totally) real subfield of K_C, which we shall denote by K'_C. Notice that K'_C is isomorphic to $\mathbb{Q}(\cos(\frac{2\pi}{|C|}))$; we have $K'_C = K_C$ if C has order at most two, otherwise K_C is an imaginary quadratic extension of K'_C.

Consider the ring homomorphisms

$$\mathbb{Z}[G] \to \bigoplus_{C\in X(G)} R_C, \quad \mathbb{Q}[G] \to \bigoplus_{C\in X(G)} K_C.$$

A chinese remainder theorem shows that the second map is an isomorphism. So the first homomorphism is injective and has finite cokernel.

(1.2) Suppose that the finite abelian group G acts on an abelian group W. For every $C \in X(G)$ we put

$$W_C := R_C \bigotimes_{\mathbb{Z}[G]} W.$$

Notice that if W happens to be a $\mathbb{Q}$-vector space, then W_C is in fact a K_C-vector space.

(1.3) Now assume that W is a finitely generated free abelian group. Then the natural map

$$W \to \bigoplus_{C\in X(G)} W_C \tag{1.3.1}$$

is injective and has finite cokernel and $W_{\mathbb{Q}} \to \oplus_{C\in X(G)} W_{\mathbb{Q},C}$ is an isomorphism. We shall sometimes use this isomorphism to identify W_C and $W_{\mathbb{Q},C}$ with subgroups of $W_{\mathbb{Q}}$. If T is a G-equivariant endomorphism of $W_{\mathbb{Q}}$, then for every $C \subset G(X)$, we have an induced endomorphism T_C of $W_{\mathbb{Q},C}$, which is K_C-linear. As such it has a determinant $\det_{K_C}(T) \in K_C$. We define the $\mathbb{Q}[G]$-determinant of T simply as the collection of these:

$$\det{}_{\mathbb{Q}[G]}(T) = (\det{}_{K_C}(T) \in K_C)_{C\in X(G)} \in \oplus_{C\in X(G)} K_C = \mathbb{Q}[G].$$

(1.4) Let us make the additional assumption that W comes with a G-invariant nondegenerate $\mathbb{Q}$-valued symplectic form $(\ ,\ )$. We then turn it into a $\mathbb{Q}[G]$-valued skew-hermitian form over $\mathbb{Z}[G]$:

$$\langle x, y\rangle := \sum_{g\in G} (x, gy)g \in \mathbb{Q}[G],$$

that is, this form is $\mathbb{Z}[G]$-linear in the first variable and has the property that $\langle y, x\rangle = -\overline{\langle x, y\rangle}$. Upon taking the tensor product with R_C, we find a K_C-valued skew-hermitian form over R_C on W_C. If we regard the target of the homomorphism (1.3.1) as a direct sum of skew-hermitian (mutually perpendicular) modules, then this homomorphism preserves the skew-hermitian structures.

Let us denote by $U(W_C)$, resp. $U(W_{\mathbb{Q},C})$, the group of R_C-linear automorphisms of W_C, resp. K_C-linear automorphisms of $W_{\mathbb{Q},C}$, which preserve the form. This is a symplectic group if C has order at most two and is a unitary group otherwise. Notice that $U(W_{\mathbb{Q},C})$ is the group of K'_C-rational points of a reductive algebraic group over K'_C. Restriction of scalars à la Weil allows us to view this group also as the group of $\mathbb{Q}$-rational points of a group defined over $\mathbb{Q}$. It contains $U(W_C)$ as an arithmetic subgroup.

If $Sp_G(W)$ denotes the group of symplectic automorphisms of W that commute with the G-action, then it follows from the preceding that we have group homomorphisms

$$Sp_G(W) \to \prod_{C\in X(G)} U(W_C), \quad Sp_G(W_{\mathbb{Q}}) \to \prod_{C\in X(G)} U(W_{\mathbb{Q},C}).$$

The latter is an isomorphism, and the former is an isomorphism onto a subgroup of finite index. We will however be mostly concerned with groups related to the special unitary group $SU(W_C)$. By definition $SU(W_C)$ is the group of unitary transformations of R_C-determinant 1. It too, is the group of K'_C-rational points of a reductive group over K'_C. Taking the R_C-determinant defines a homomorphism of $U(W_C)$ to the group of units R_C^* of R_C. By the Dirichlet unit theorem, the rank of R_C^* is $\max\{0, \frac{1}{2}\phi(|C|) - 1\}$ (where ϕ is the euler function) and its torsion subgroup is the group of roots of unity in R_C, which we may identify with C.

We shall denote by $U^{\#}(W_C)$ the group of elements of $U(W_C)$ whose determinant is a square of a root of unity. This is an extension of a subgroup of C by $SU(W_C)$. The pre-image of $\prod_{C\in X(G)} U^{\#}(W_C)$ in $Sp_G(W)$ is denoted by $Sp_G^{\#}(W)$. We define $Sp_G^{\#}(W_{\mathbb{Q}})$ similarly.

2. Statements of the results

(2.1) Let S be a closed oriented surface of genus $g \geq 2$. If $\pi : \tilde{S} \to S$ is a finite connected abelian covering with covering group G, then the cokernel of $\pi_* : H_1(\tilde{S}) \to H_1(S)$ is naturally isomorphic to G. The resulting epimorphism $H_1(S) \to G$ dualizes to a monomorphism $\hat{G} \to \mathrm{Hom}(H_1(S), \mu) \cong H^1(S; \mu)$, where μ denotes the group of roots of unity in $\overline{\mathbb{Q}}$. Conversely, any finite factor group G of $H_1(S)$ comes from a connected abelian covering $\tilde{S}_G \to S$ with covering group G, which is unique up to isomorphism. The group G acts on $H_1(\tilde{S}_G)$ and this action preserves its (symplectic) intersection form. This brings us in the situation of section 1; in particular, the groups $Sp_G^{\#}(H_1(\tilde{S}_G))$ and $Sp_G^{\#}(H_1(\tilde{S}_G; \mathbb{Q}))$ are defined. If we are given $\tilde{S}_G$, then for every factor group $G' = G/H$ of G, a natural choice for $\tilde{S}_{G'}$ is the H-orbit space of $\tilde{S}_G$. The resulting homomorphism $H_1(\tilde{S}_G) \to H_1(\tilde{S}_{G'})$ is G-equivariant (via the homomorphism $G \to G'$), and induces therefore a $\mathbb{Z}[G']$-

homomorphism

$$\mathbb{Z}[G'] \bigotimes_{\mathbb{Z}[G]} H_1(\tilde{S}_G) \to H_1(\tilde{S}_{G'}).$$

This homomorphism is injective with cokernel isomorphic to H. It has degree equal to $|H|$ in the sense that it takes the $\mathbb{Z}[G']$-valued skew-hermitian form on the left to $|H|$ times the form on the right.

For C a finite cyclic quotient of $H_1(S)$, we denote the skew-hermitian module $H_1(\tilde{S}_C)_C$ by H_C. So with this convention, $H_0 = H_1(S)$.

(2.2) Proposition. *If $C \neq 0$, then H_C has a free R_C-basis $e_1, e_{-1}, \dots, e_{g-1}, e_{1-g}$, such that the skew-hermitian form is given by $\langle z, w\rangle = \sum_{i=1}^{g-1}(z_i\bar{w}_{-i} - z_{-i}\bar{w}_i)$.*

This proposition implies that every square in C is realized as the determinant of a unitary transformation in H_C, so that $U^{\#}(H_C)$ is an extension of the group of squares, $C^{(2)}$, by $SU(H_C)$.

(2.3) Let $\Gamma_{S,G}$ the group of mapping classes of S that leave the subgroup $\widehat{G}$ of $H^1(S;\mu)$ pointwise fixed. The lifts of these classes to $\Gamma_{\tilde{S}_G}$ define a central extension

$$1 \to G \to \Gamma^{\#}_{S,G} \to \Gamma_{S,G} \to 0.$$

We have a natural representation of $\Gamma^{\#}_{S,G}$ on $H_1(\tilde{S}_G)$. Its image is of course contained in $Sp_G(H_1(\tilde{S}_G))$.

(2.4) Theorem. *If C is a nontrivial finite cyclic factor group of $H_1(S)$, then the image of the representation of $\Gamma^{\#}_{S,C}$ on H_C is equal to $U^{\#}(H_C)$.*

For a finite cyclic factor group C of $H_1(S)$, the representation of $\Gamma^{\#}_{S,G}$ on H_C descends to a projective representation $\Gamma_{S,C} \to PU(H_C)$. Theorem (2.4) implies that the image is a subgroup of index at most two. The following theorem (2.5) says essentially that these homomorphisms are virtually independent, at least if $g \geq 3$.

(2.5) Theorem. *Let $C_1, \dots, C_s$ be a finite set of distinct finite cyclic factor groups of $H_1(S)$. In case $g = 2$, assume that none of these groups has order 2, 3 or 4. Then the image of the homomorphism*

$$\bigcap_{k=1}^{s} \Gamma_{S,C_k} \to \prod_{k=1}^{s} PU(H_{C_k})$$

is a subgroup of finite index.

I do not know whether the excluded cases of the theorem are genuine or just an artefact of the proof. Their appearance is due to an application of a theorem of Margulis on arithmetic groups, which requires their ambient $\mathbb{Q}$-algebraic groups to have $\mathbb{Q}$-rank at least two. For $g = 2$ and C of order 2, 3 or 4, the ambient algebraic group of $PU(H_C)$ is isomorphic to PSL_2, and hence of $\mathbb{Q}$-rank one.

Combining theorem (2.5) with the discussion in section 1 yields:

(2.6) Corollary. *Let G a finite factor group of $H_1(S)$. Assume that in case $g = 2$, the order of G is not divisible by 2 or 3. Then the image of the representation of $\Gamma^{\#}_{S,G}$ on $H_1(\tilde{S}_G)$ is a subgroup of finite index of $Sp^{\#}_G(H_1(\tilde{S}))$.*

3. Liftable Dehn twists and bounding pairs

In this section G is a finite factor group of $H_1(S)$ and $\pi : \tilde{S}_G \to S$ is an associated connected abelian G-covering. We have a closer look at certain elements of $\Gamma^{\#}_{S,G}$ and we prove that they generate this group when G is cyclic.

(3.1) Suppose that E is an embedded circle in S. A diffeomorphism of the open cylinder $(-1,1)\times S^1$ on an neighorhood of E determines an orientation preserving diffeomorphism of S (a "Dehn twist") whose support is contained in this neighborhood. Its class τ_E in Γ_S only depends on the isotopy class of E. An orientation of E determines a class $e\in H_1(S)$, and the action of τ_E on $H_1(S)$ is given by the symplectic transvection T_e defined by this class:

$$T_e : x \mapsto x + (x,e)e.$$

Let H denote the subgroup of G generated by the image of e in G, and let d be its order. Then T_e^d preserves the kernel of the surjection $H_1(S)\to G$ and induces the identity in G. It is actually the smallest positive power of T_e with these properties. So τ_E^d lifts to a mapping class of $\tilde{S}_G$. There is in fact privileged lift, $\widetilde{\tau_E^d}$, which is the product of the Dehn twists about all the connected components of the pre-image of E in $\tilde{S}_G$. (They clearly commute, so the order is irrelevant.) The action it induces in $H_1(\tilde{S}_G)$ is given by

$$\widetilde{T_E^d}(x) = x + \sum_{g\in G/H}(x, g\tilde{e})\tilde{e} = x + d^{-1}\sum_{g\in G}(x,g\tilde{e})g\tilde{e},$$

where $\tilde{e}$ is the class of an oriented connected component of the pre-image of E. We can also write this as

$$\widetilde{T_E^d}(x) = x + d^{-1}\langle x,\tilde{e}\rangle\tilde{e},$$

which shows that $\widetilde{T_E^d}$ is a unitary transvection. In particular, its $\mathbb{Q}[G]$-determinant is equal to 1. If $G=C$ is cyclic then the induced action in H_C is given by the same expression.

The case when E is a separating circle is noteworthy: then $H_1(E)\to H_1(S)$ is the zero map, and so $e=0$, hence T_e is the identity, whereas $\tilde{e}$ may be nonzero (so that $\widetilde{T_E}\neq 1$).

(3.2) Suppose now that we are given a *bounding pair* (E,E') on S. This means that E and E' are disjoint circles on S with the property that $H_1(E)$ and $H_1(E')$ have the same image in $H_1(S)$. This last property is equivalent to the condition that $S-E-E'$ be disconnected. Then $\tau^E_{E'} := \tau_{E'}\tau_E^{-1}$ acts as the identity on $H_1(S)$, so that this mapping class will lift to a mapping class of $\tilde{S}_G$. We shall see that there are two distinguished lifts in this case.

Denote the closures of the two connected components of $S-E-E'$ by S_0, S_1, and let $G_i\subset G$, resp. H be the image of $H_1(S_i)$ resp. $H_1(E)$ in G. (So $H\subset G_i$.) Choose Dehn twists D, D' about E and E' with disjoint supports. Let U denote the union of the supports of these Dehn twists. The corresponding representative $D'D^{-1}$ of $\tau^E_{E'}$ admits a unique lift which leaves $\pi^{-1}(S_0-U)$ pointwise fixed. This lift preserves every connected component of $\pi^{-1}U$, and is there a fractional power of a Dehn twist. It also preserves every connected component of $\pi^{-1}(S_1 - U)$ and induces in every connected component the covering transformation defined by a generator h of H. We denote the transformation of $H_1(\tilde{S}_G)$ induced by $D'D^{-1}$ by $\tilde{T}^E_{E'}$.

Choose connected components $\tilde{E}$, $\tilde{E}'$, $\tilde{S}_i$ of the pre-image of the corresponding subsets of S. Now $\tilde{S}_i \to S_i$ is a connected abelian covering with covering group G_i. Similarly, $\tilde{E} \to E$ and $\tilde{E}' \to E'$ are connected abelian H-coverings. Every connected component of $\pi^{-1}S_i$ is a G_i-translate of $\tilde{S}_i$, and so $H_\bullet(\pi^{-1}S_i) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_i]} H_\bullet(\tilde{S}_i)$ as $\mathbb{Z}[G]$-modules. Similarly, $H_j(\pi^{-1}E) \cong H_j(\pi^{-1}E')$ is isomorphic to $\mathbb{Z}[G/H]$ for $j = 0, 1$. Our lift acts on these homology groups. It acts as the identity in all cases, except for $H_1(\pi^{-1}S_1) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_1]} H_1(\tilde{S}_1)$, where it acts as multiplication by a generator h of H. From the Mayer-Vietoris sequence of the pair $(\pi^{-1}S_0, \pi^{-1}S_1)$ we then see that the $\mathbb{Q}[G]$-determinant of $\tilde{T}^E_{E'}$ is equal to the $\mathbb{Q}[G]$-determinant of the action of h in $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G_1]} H_1(\tilde{S}_1)$. This is of course equal to the $\mathbb{Q}[G_1]$-determinant of the action of h in $H_1(\tilde{S}_1)$.

Let $S_1 \to S_1^*$ identify the two boundary components of S_1 in such a way that the result is a closed oriented surface S_1^*. The image of the two boundary components is a circle E_1 on S_1^*, and we may think of $S_1^* - E$ as the interior of S_1. The homomorphism $H_1(S_1) \to G_1$ factors through $H_1(S_1^*)$, and so the covering $\tilde{S}_1 \to S_1$ is the pull-back of a covering $\tilde{S}_1^* \to S_1^*$ (which we shall also denote by π). The element h acts trivially on the homology of the mapping cone of $\tilde{S}_1 \to \tilde{S}_1^*$ and so the determinant of h acting on $H_1(\tilde{S}_1)$ is the same as the determinant of its action on $H_1(\tilde{S}_1^*)$.

(3.3) Proposition. *When $G = C$ is cyclic, then the group $\Gamma_{S,C}$ is generated by the following transformations:*

(1) *$\tilde{\tau}^E_{E'}$, where (E, E') is a bounding pair on S,*

(2) *$\tilde{\tau}_E$ where E is a circle whose class in $H_1(S)$ maps to zero in C.*

Proof. According to a theorem due to Powell [4] the kernel of the representation of Γ_S on $H_1(S)$ (the "Torelli group") is generated by the mapping classes defined by bounding pairs and by Dehn twists about separating circles. (He proves this for $g \geq 3$, but it is well-known that this is also true in case $g = 2$.) Therefore we only need to prove that the group of those $T \in Sp(H_1(S))$ that leave $\hat{C}$ pointwise fixed is generated by the images of the elements (2) in $Sp(H_1(S))$. The latter is just the subgroup of $Sp(H_1(S))$ generated by the symplectic transvections T_e^k with $ke \in \mathrm{Ker}(H_1(S) \to C)$. The proposition now follows from the following lemma.

(3.4) Lemma. *Let V be an integral unimodular symplectic lattice of rank $2g$, $g \geq 2$. Let $\phi : V \to \mathbb{Z}/d$ be a surjective homomorphism, and let $Sp(V)_\phi$ be the stabilizer of ϕ in $Sp(V)$. Then $Sp(V)_\phi$ is generated by its symplectic transvections.*

Proof. The transvections in the principal level d congruence subgroup $Sp(V)[d]$ of $Sp(V)$ generate a normal subgroup $E(V, dV)$ of $Sp(V)$. Form the quotient $Sp(V)[d]/E(V, dV)$; this is a factor group of $KSp_{2g,1}(d\mathbb{Z})$ and it is known that the latter group is trivial [1]. Hence $Sp(V)_\phi$ contains $Sp(V)[d]$, and so it suffices to prove the corresponding statement in $Sp(V/dV)$.

We put $W := V/dV$ and regard it as a nonsingular symplectic module over $\mathbb{Z}/d$. Let $e \in W$ be the element such that $\phi(x) = (x, e)$ and let $I \subset W$ be the span of e. Since I is an isotropic direct summand, it is contained in $I^\perp$ (perp taken with respect to the symplectic form) and $I^\perp/I$ is a nonsingular symplectic module over $\mathbb{Z}/d$. The $Sp(W)$-stabilizers of ϕ and e coincide. Let U_e denote the group of elements of $Sp(W)_e$ that act trivially on $I^\perp/I$. If W' is a supplementary module of I in $I^\perp$, then we have a semi-direct product decomposition $Sp(W)_\phi = Sp(W') \ltimes U_e$. Every element of U_e is uniquely written $x \mapsto x + (x, e)a + (x, a)e + k(x, e)e$ with $a \in W'$ and $k \in \mathbb{Z}/d$. But this is just $T_e^{k-1}T_{-a}T_{a+e}$ and hence a product of symplectic transvections. Since $Sp(W')$ is also generated by symplectic transvections, it follows that $Sp(W)_\phi$ is.

4. The cyclic case

(4.1) Let C be a cyclic factor group of $H_1(S)$ of order $d > 1$. We first describe a simple model for the corresponding cyclic covering $\tilde{S}_C \to S$. Choose a generator c of C, so that C may be identified with $\mathbb{Z}/d$. The covering is then given by a surjective homomorphism $H_1(S) \to \mathbb{Z}/d$. Such a homomorphism is obtained by intersection with an indivisible class $e \in H_1(S)$ followed by reduction modulo d. The symplectic group of $H_1(S)$ acts transitively on the set of indivisible elements of $H_1(S)$, hence so does the mapping class group of S. Therefore, we can represent e by by an embedded oriented circle E with $S - E$ connected. We give $S - E$ a boundary (two copies of E) and call the resulting compact surface with boundary, S_E. (More intrinsically S_E could be characterized as the real oriented blow-up of E in S.) Notice that S_E has two boundary components E_+, E_-, that there is natural diffeomorphism $h : E_+ \to E_-$, and that S is recovered from the pair (S_E, h) by identifying points of E_- with points of E_+ via h. Now let $\tilde{S}_C$ be the quotient of $S_E \times \mathbb{Z}/d$ obtained by identifying $(x, i) \in E_+ \times \mathbb{Z}/d$ with $(h(x), i + 1) \in E_- \times \mathbb{Z}/d$. There is a natural map $\tilde{S}_C \to S$, and the C-action given by translation in the $\mathbb{Z}/d$-factor makes this a connected C-covering. It is easy to see that the sequence $H_1(\tilde{S}_C) \to H_1(S) \to G$ is exact, so that $\tilde{S}_C \to S$ is the right cyclic covering.

Put $E'_g := E$, and extend this to a standard set of embedded oriented circles, labeled $E'_1, E'_{-1}, \dots, E'_g, E'_{-g}$ on S; by this we mean that for $|i| \neq |j|$, E'_i and E'_j are disjoint, and E'_i meets E'_{-i} tranversally in a single point with index 1 (resp. -1) if $i > 0$ (resp. < 0). For $|i| \neq g$, let E_i be the image of $E'_i \times \{0\}$ in $\tilde{S}_C$, and let E_g be the image of $E_- \times \{0\}$. We take for E_{-g} the oriented pre-image of E'_{-g}; this is a connected d-covering of E'_{-g}. We denote the class of E_i in $H_1(\tilde{S}_C)$ by e_i. The following proposition is now clear (see figure 1):

(4.2) Proposition. *The $\mathbb{Z}$-module $H_1(\tilde{S}_C)$ is freely generated by the classes $c^k e_i$ with $|i| \leq g - 1, k \in \mathbb{Z}/d$, and $e_{\pm g}$. So as a $\mathbb{Z}[C]$-module, $H_1(\tilde{S}_C)$ is the direct sum of the free $\mathbb{Z}[C]$-module generated by $e_{\pm 1}, \dots, e_{\pm(g-1)}$ and the trivial $\mathbb{Z}[C]$-module generated by $e_{\pm g}$:*

$$H_1(\tilde{S}_C) \cong \mathbb{Z}[C]\{e_{\pm 1}, \dots, e_{\pm(g-1)}\} \oplus \mathbb{Z}\{e_{\pm g}\}.$$

Moreover, the intersection number $(e_i, c^k e_j)$ is zero unless $k \equiv 0 \pmod{d}$ and $i = -j$, in which case it is 1 ($i > 0$) or -1 ($i < 0$).

FIG 1: THE $\mathbb{Z}[C]$-MODULE $H_1(\tilde{S}_C)$.

Proof of (2.2). It follows that the associated skew-hermitian form over $\mathbb{Z}[G]$ is given by

$$\langle e_i, e_j\rangle = \begin{cases} 1 & \text{if } 0 < i = -j; \\ -1 & \text{if } 0 > i = -j; \\ 0 & \text{else.} \end{cases}$$

Tensoring this module with R_C shows that H_C is the free R_C-module generated by $e_{\pm 1}, \dots, e_{\pm(g-1)}$ with skew-hermitian form

$$\langle z, w\rangle = \sum_{i=1}^{g-1} (z_i \overline{w}_{-i} - z_{-i}\overline{w}_i).$$

This proves (2.2).

(4.3) Proposition. *The image of the representation of $\Gamma^{\#}_{S,C}$ on H_C is contained in $U^{\#}(H_C)$.*

Proof. We need to show that every element $\tilde{f} \in \Gamma^{\#}_{S,C}$ induces a transformation in H_C whose determinant is an even power of c. Multiplication c^k in H_C has determinant $c^{k(2g-2)}$. So this property only depends on the image of $\tilde{f}$ in $\Gamma_{S,C}$. It is therefore enough to prove this for lifts of generators of $\Gamma_{S,C}$. We found a set of generators in (3.3) consisting of certain Dehn twists and bounding pairs. In

(3.1) and (3.2) we described lifts of them. For a Dehn twist we got determinant 1, but the case of a bounding pair was more complicated. In fact, we constructed a closed surface S_1^*, a connecting cyclic covering $\tilde{S}_1^* \to S_1^*$ whose covering group is canonically a subgroup C_1 of C, and an element $h \in C_1$, such that the $\mathbb{Q}[C]$-determinant of the lift of this bounding pair is equal to the $\mathbb{Q}[C_1]$-determinant of the action of h on $H_1(\tilde{S}_1^*)$. If we apply (4.2) to S_1^* and C_1, we find that the determinant is h^{2g_1-2}, where g_1 is the genus of S_1^*. In particular, it is an even power of c.

(4.4) In the remainder of this section we shall omit the subscript C in R_C, K_C, R'_C, and K'_C. We shall write $U_{2g-2}(R)$ for the group of automorphisms of the skew-hermitian R-module above. We will use the following so-called *elementary transformations*:

$$\begin{aligned} T_i(r') &: z \mapsto z + r'\langle z, e_i\rangle e_i, \quad i = \pm 1, \pm 2, \ldots, \text{ and } r' \in R'_n; \\ T_{i,j}(r) &: z \mapsto z + r\langle z, e_i\rangle e_j + \overline{r}\langle z, e_j\rangle e_i, \quad i, j = \pm 1, \pm 2, \ldots, |i| \neq |j|, \text{ and } r \in R_n. \end{aligned}$$

(Our indexing slightly differs from the one used in [2, p.224].) Note that these transformations lie in $SU_{2n}(R)$. Moreover, T_i resp. $T_{i,j}$ is a homomorpism of the additive group of R' resp. R to $SU_{2n}(R)$; we call them the *elementary one parameter subgroups*. It is known that $SU_{2n}(R)$ is generated by its elementary one parameter subgroups. (See [2], (9.2.6) in the case $n > 1$, and (1.4.3.10ff) in case $n = 1$.)

(4.5) Corollary. *Let T be the element of $U_{2n}^{\#}(R)$ which multiplies e_1 and e_{-1} with c and leaves every other basis vector e_i, $i \neq \pm 1$, fixed. Then for $n > 1$, $U_{2n}^{\#}(R)$ is generated by T, and its subgroup $Sp_{2n}(\mathbb{Z})$.*

Proof. Let Δ denote the subgroup of $U_{2n}^{\#}(R)$ generated by these elements. Since $\det(T) = c^2$, in view of the preceding it is enough to prove that Δ contains the elementary one parameter subgroups.

To this end, consider the $\mathbb{Z}$-span V of the generators. This is clearly a symplectic lattice. For a hyperbolic plane $H \subset V$, let T_H denote the transformation which is multiplication by c on H and the identity on the perpendicular summand. Since H is an $Sp_{2n}(\mathbb{Z})$-translate of $\mathbb{Z}e_1 \oplus \mathbb{Z}e_{-1}$, we have that $T_H \in \Delta$. Now let e_i, e_j be generators with $|i| \neq |j|$. Let H, resp. H' be the integral span of (e_i, e_{-i}), resp. $(e_i, e_{-i} + e_j)$. Both are hyperbolic summands of V, so that $T_H, T_{H'} \in \Delta$, and a straightforward computation shows that

$$T_H^{-k} T_{H'}^k = T_{i,j}(1 - c^k)$$

Since $T_{i,j}(1) \in Sp_{2n}(\mathbb{Z}))$, it follows that Δ contains the image of the full one parameter subgroup $T_{i,j}$. Another straightforward computation yields

$$[T_{i,-j}(r), T_{i,j}(1)] = T_i(r + \overline{r}).$$

Notice that $T_i(1) \in Sp_{2n}(\mathbb{Z})$. Since R' is additively spanned by 1 and the elements $c^k + c^{-k}$, it follows that Δ contains T_i also.

(4.6) Lemma. *The image of* $\Gamma^{\#}_{S,C}$ *in* $U_{2g-2}(R)$ *contains* $Sp_{2g-2}(\mathbb{Z})$.

Proof. The diffeomorphisms that leave the E'_g and E'_{-g} pointwise fixed lift uniquely to diffeomorphisms of $\tilde{S}_C$ which leave thier pre-images pointwise fixed. The representation of this group of diffeomorphisms on $H_1(S - E'_g - E'_{-g})$ is the full symplectic group. Its action on $H_1(\tilde{S}_C)$ respects the decomposition of (4.2); the action on the second summand is trivial, and if we write the first summand as $\mathbb{Z}[C] \otimes H_1(S - E'_g - E'_{-g})$, then the action on this summand is through its action on $H_1(S - E'_g - E'_{-g})$. The lemma follows.

FIG. 2

Proof of (2.4) for $g = 2$. Let for $k = 1, 2, 3, \dots,$ F'_k be the embedded oriented circle in figure 2. It is null-homologous, but its pre-image in $\tilde{S}_C$ has a connected component whose class is $(c^k - 1)e_1$. The covering group C acts simply transitively on these connected components, and so their classes are of the form $c^{k+l} - c^l$. The Dehn twist over F'_k lifts to product of the Dehn twists over these connected components. The action of this product on H_C is just the elementary transformation $T_1((c^k - 1)(c^{-k} - 1)) = T_1(2 - c^k - c^{-k})$. According to (4.6), the symplectic transvection $T_1(1)$ is also in the image of $\Gamma^{\#}_{S,C}$. Hence the image contains the whole one parameter elementary subgroup T_1. Interchanging the roles of E_1 and E_{-1} give the same statement for T_{-1}. As recalled in (4.4), these two subgroups generate $SU_2(R) = SL_2(R')$. Since $U_2^{\#}(R) = C.SU_2(R)$, this completes the proof.

FIG. 3

Proof of (2.4) for $g \geq 3$. Let F' be the circle in figure 3. It is homologous to E'_{-g} and disjoint with the E'_i for $i \neq g$. It forms with E'_{-g} a so-called bounding pair. The Dehn twists along E'_{-g} and F' commute, and have the same effect on homology. Therefore, $\tau := \tau_{E'_{-g}} \tau_{F'}^{-1}$ is an element of $\Gamma_{S,C}$. It lifts to an element $\tilde{\tau}$ in $\Gamma_C^{\#}$ which induces in H_C the operator T. Now apply (4.5) and (4.6).

5. PROOF OF (2.5)

We will derive theorem (2.5) from the proposition below. This in turn is a consequence of some powerful results about arithmetic groups, which in their strongest form are due to Margulis.

(5.1) Proposition. *Let $\mathcal{G}_i$ $(i = 1, \ldots, s)$ be a connected algebraic group over a number field K_i which is almost K_i-simple and has the property that the $\mathbb{Q}$-rank of $Res_{K_i|\mathbb{Q}} \mathcal{G}_i$ is at least two. Let Δ be a subgroup of $\mathcal{G}_1(K_1) \times \cdots \times \mathcal{G}_s(K_s)$ with the property that*

(1) *its image under the projection to any factor $\mathcal{G}_i(K_i)$ is arithmetic in that factor and*

(2) *its image in the product of any two factors $\mathcal{G}_i(K_i) \times \mathcal{G}_j(K_j)$, $i \neq j$ is Zariski dense in that product.*

Then Δ is arithmetic in $\mathcal{G}_1(K_1) \times \cdots \times \mathcal{G}_s(K_s)$.

Proof. We proceed with induction on s. For $s = 1$, there is nothing to prove, so assume that $s > 1$ and that the proposition has been settled for $s-1$. We suppose the groups numbered such that $\deg K_s \leq \deg K_i$ for all i. By our induction hypothesis, the projection of Δ' in $\mathcal{G}_1(K_1) \times \cdots \times \mathcal{G}_{s-1}(K_{s-1})$ is arithmetic in that product. By passing to a subgroup of finite index, we may assume without loss of generality that Δ' is a product: $\Delta' = \Delta'_1 \times \cdots \times \Delta'_{s-1}$, with Δ'_i arithmetic in $\mathcal{G}_i(K_i)$. Let Δ'_s be the image of Δ in the last factor, and let Δ_s be the kernel of the projection of $\Delta \to \Delta'$ (regarded as a subgroup of $\mathcal{G}_s(K_s)$). Then Δ'_s is arithmetic in $\mathcal{G}_s(K_s)$ and contains Δ_s as a normal subgroup. According to a theorem of Margulis [3, result (A) on p. 258], either Δ_s is of finite index in Δ'_s or Δ_s is finite. It remains to show that the last case does not occur.

Suppose it does. By passing to a subgroup of finite index, we may assume that Δ_s is trivial. This means that Δ is the graph of a (surjective) homomorphism $f : \Delta' \to \Delta'_s$. If f_i denotes the restriction to the ith factor, then it follows from theorem VIII (3.4) of *loc. cit.* that after passage to subgroups of finite index, f_i is either trivial or the restriction of a nontrivial homomorphism of algebraic groups $F_i : \mathcal{G}_i \to \mathcal{G}_s$ covering a field homomorphism $\phi_i : K_i \to K_s$. Suppose we are in the latter case. Then ϕ_i must be an isomorphism, because $\deg K_s \leq \deg K_i$. Since $\mathcal{G}_i$ is almost-simple over K_i, F_i has finite kernel. The image of F_i is an infinite K_s-subgroup of $\mathcal{G}_s$. These subgroups commute with each other and generate $\mathcal{G}_s$. Since $\mathcal{G}_s$ is almost-simple over K_s, this can happen for exactly one index, say $i = s-1$. It follows that Δ is the direct product $\Delta'_1 \times \cdots \Delta'_{s-2}$ and an arithmetic subgroup of the graph of F_{s-1}. This contradicts our second assumption.

Proof of (2.5). We apply the previous proposition to the case where $K_i = K'_{C_i}$, $\mathcal{G}_i(K_i) = PU(H_{\mathbb{Q},C_i})$, and Δ is the image of $\cap_i \Gamma_{S,C_i}$ in $\Pi_i PU(H_{\mathbb{Q},C_i})$. Then the real rank of $\mathrm{Res}_{K_i|\mathbb{Q}}\, \mathcal{G}_i$ is at least two, unless $g = 2$, C_i is nontrivial, and $K_i = \mathbb{Q}$. The last two properties are equivalent to: C_i has order 2, 3 or 4. Theorem (2.4) implies that first hypothesis of (5.1) is fulfilled. So (2.5) will follow from the lemma below.

(5.2) Lemma. *Let C_1 and C_2 be distinct finite cyclic factor groups of $H_1(S)$. Then $\Gamma_{S,C_1} \cap \Gamma_{S,C_2}$ has Zariski dense image in $PU(H_{\mathbb{Q},C_1}) \times PU(H_{\mathbb{Q},C_2})$.*

Proof. Denote the image by Δ. It follows from (2.4) that the projection Δ'_i of Δ in $PU(H_{C_i})$ is of finite index in $PU(H_{C_i})$. It is therefore enough to show that Δ contains an element of the form $(T_1, 1)$, with $T_1 \neq 1$ and one of the form $(1, T_2)$ with $T_2 \neq 1$: it then also contains the normal subgroup generated by these elements in $\Delta'_1 \times \Delta'_2$, and it is clear that such a subgroup is Zariski dense in $PU(H_{\mathbb{Q},C_1}) \times PU(H_{\mathbb{Q},C_2})$. To produce such elements, suppose that C_1 is nontrivial, and choose on S an embedded circle E which separates S in two connected components S', S'', such that the restriction of C_1 to both $H_1(S')$ and $H_1(S'')$ is nontrivial, whereas the restriction of C_2 to $H_1(S')$ is trivial. Then the Dehn twist about E determines an element of the form $(T_1, 1)$ with $T_1 \neq 1$. If C_1 is trivial, then C_2 is nontrivial. Realize C_2 by an oriented embedded circle E on S, such that a generator of C_2 is given by taking the intersecting number with E followed by reduction modulo a positive integer. Then the Dehn twist about E has the required property.

References

1. H. Bass, J. Milnor, J.-P. Serre, *Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$*, Inst. Hautes Études Sci. Publ. Math. **33** (1967), 59–137.
2. A.J. Hahn and O.T. O'Meara, *The Classical Groups and K-Theory*, Springer, Berlin and New York, 1989.
3. G.A. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, Berlin and New York, 1991.
4. J. Powell, *Two theorems of the Torelli group I: a finite set of generators for $\mathcal{J}$*, Proc. Amer. Math. Soc. **68** (1978), 347–350.

Faculteit Wiskunde en Informatica, Rijksuniversiteit Utrecht, PO Box 80.010, 3508 TA Utrecht, The Netherlands
E-mail address: looijenga@math.ruu.nl