Geom. Funct. Anal. Vol. 25 (2015) 1493–1542
DOI: 10.1007/s00039-015-0352-5
Published online November 14, 2015

GAFA Geometric And Functional Analysis

ARITHMETIC QUOTIENTS OF THE MAPPING CLASS GROUP

Fritz Grunewald, Michael Larsen, Alexander Lubotzky and Justin Malestein

Abstract. To every $\mathbb{Q}$-irreducible representation r of a finite group H, there corresponds a simple factor A of $\mathbb{Q}[H]$ with an involution τ. To this pair (A,τ), we associate an arithmetic group Ω consisting of all $(2g-2)\times(2g-2)$ matrices over a natural order $\mathfrak{O}^{op}$ of A^{op} which preserve a natural skew-Hermitian sesquilinear form on A^{2g-2}. We show that if H is generated by less than g elements, then Ω is a virtual quotient of the mapping class group $\mathrm{Mod}(\Sigma_g)$, i.e. a finite index subgroup of Ω is a quotient of a finite index subgroup of $\mathrm{Mod}(\Sigma_g)$. This shows that $\mathrm{Mod}(\Sigma_g)$ has a rich family of arithmetic quotients (and "Torelli subgroups") for which the classical quotient $\mathrm{Sp}(2g,\mathbb{Z})$ is just a first case in a list, the case corresponding to the trivial group H and the trivial representation. Other pairs of H and r give rise to many new arithmetic quotients of $\mathrm{Mod}(\Sigma_g)$ which are defined over various (subfields of) cyclotomic fields and are of type $\mathrm{Sp}(2m)$, $\mathrm{SO}(2m,2m)$, and $\mathrm{SU}(m,m)$ for arbitrarily large m.

1 Introduction

Let $\Sigma=\Sigma_g$ be a closed surface of genus $g\geq 2$ and $\mathrm{Mod}(\Sigma)$ the mapping class group of Σ, which is the group of orientation-preserving homeomorphisms of Σ modulo those isotopic to the identity. It is well-known that there is an epimorphism from $\mathrm{Mod}(\Sigma)$ onto the arithmetic group $\mathrm{Sp}(2g,\mathbb{Z})$. The purpose of this paper is to show that many more arithmetic groups are quotients of $\mathrm{Mod}(\Sigma)$. Specifically, for every pair (H,r), where H is a finite group minimally generated by $d(H)<g$ elements and r is a nontrivial irreducible $\mathbb{Q}$-representation of H, we associate a finite index subgroup Γ_H of $\mathrm{Mod}(\Sigma)$, an arithmetic group $\Omega_{H,r}$ (whose exact structure will be described below) and a homomorphism $\rho_{H,r}:\Gamma_H\to\Omega_{H,r}$ whose image is of finite index in $\Omega_{H,r}$. We call such a homomorphism a *virtual epimorphism* of $\mathrm{Mod}(\Sigma)$ onto $\Omega_{H,r}$ (Of course, via the induced representation, every virtual homomorphism also gives a representation of the full group $\mathrm{Mod}(\Sigma)$, but it is more natural to study the original representation). The homomorphism $\mathrm{Mod}(\Sigma)\to\mathrm{Sp}(2g,\mathbb{Z})$ is the special case where H is the trivial group. The homomorphism from a finite index subgroup of $\mathrm{Mod}(\Sigma_g)$ to $\mathrm{Sp}(2(g-1),\mathbb{Z})$ studied in [LM12] and [MS13] is the one corresponding to the case $H=\mathbb{Z}/2\mathbb{Z}$ and r the nontrivial one-dimensional representation. The first to show that $\mathrm{Mod}(\Sigma)$ has a large collection of virtual arithmetic quotients beside $\mathrm{Sp}(2g,\mathbb{Z})$

was Looijenga [L97] who analyzed the case where H is abelian. In [L97], [LM12], [MS13], all representations have degree bounded by $2g$ and the target arithmetic groups are limited, while we obtain irreducible representations of arbitrarily large degree and a wider range of target arithmetic groups.

The homomorphism ρ is obtained from the action of $\mathrm{Mod}(\Sigma)$ (or more precisely, of a finite index subgroup of $\mathrm{Mod}(\Sigma)$) on the first integral homology group of a finite Galois cover of Σ corresponding to H; equivalently, on $\overline{R} \stackrel{\mathrm{def}}{=} R/[R,R]$ where R is a finite index normal subgroup of $T_g = \pi_1(\Sigma_g)$ with $T_g/R \cong H$. This action on the homology of finite covers was also studied by Koberda, but with the goal of showing that one can determine whether a mapping class is periodic, reducible or pseudo-Anosov by considering enough finite covers [K12].

Our work is also related to that of Grunewald and Lubotzky [GL09] whose results we will use in our proofs. Recall that by the Dehn–Nielsen–Baer Theorem, $\mathrm{Mod}(\Sigma_g)$ is naturally isomorphic to an index 2 subgroup of $\mathrm{Out}(T_g)$, the outer automorphism group of $T_g = \pi_1(\Sigma_g)$ (Allowing orientation-reversing homeomorphisms would give all of $\mathrm{Out}(T_g)$). In [GL09], Grunewald and Lubotzky studied the analogous problem where $\mathrm{Out}(T_g)$ is replaced by $\mathrm{Aut}(F_n)$ the automorphism group of F_n, the free group of rank n. While there are a few similarities between the papers, the theory developed in the current paper requires several advances (which we will discuss), and the main techniques of proof in [GL09], as far as we can determine, are unusable in this case. The difference is nicely illustrated already in the easiest case; while the fact that $\pi : \mathrm{Aut}(F_n) \to \mathrm{GL}(n,\mathbb{Z})$ is surjective is easy to establish, the fact that $\mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}(2g,\mathbb{Z})$ is surjective is a classical but nontrivial result due to Burkhardt and Clebsch-Gordan [B89].

We begin by describing the general procedure for obtaining representations to arithmetic groups from $\mathrm{Mod}(\Sigma_g, *)$, the mapping class group fixing the point $* \in \Sigma_g$ up to isotopy fixing $*$. We will denote these representations also by ρ. A short argument (Section 8.2) shows that the representations descend (virtually) to $\mathrm{Mod}(\Sigma_g)$. Via the natural map $\mathrm{Mod}(\Sigma_g, *) \to \mathrm{Aut}(T_g)$, we can identify $\mathrm{Mod}(\Sigma, *)$ with its image, which is of index 2 and which we denote by $\mathrm{Aut}(T_g)^+$. Let $p : T_g \to H$ be a surjective homomorphism with kernel R onto a finite group H, and let $\Gamma_{H,p} = \{\gamma \in \mathrm{Aut}(T_g)^+ | p \circ \gamma = p\}$. Then, $\Gamma_{H,p}$ is a finite index subgroup of $\mathrm{Aut}(T_g)^+$ which preserves R and acts on $\overline{R}$ as a $\mathbb{Z}[H]$-module. Thus, $\Gamma_{H,p}$ acts by $\mathbb{Q}[H]$-automorphisms on $\hat{R} = \overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$ and we obtain a representation $\rho_{H,p} : \Gamma_{H,p} \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R})$ (See Section 6 for a discussion of these and some other properties of $\rho_{H,p}$).

By an analogue of a classical result of Gaschütz, the module $\hat{R}$ can be identified precisely. Note that here, and elsewhere unless stated otherwise, $\mathbb{Q}$ is considered to be the trivial $\mathbb{Q}[H]$-module.

PROPOSITION 1.1. *Let $T = T_g$ be the fundamental group of a surface Σ of genus $g \geq 2$. Let R be a finite index normal subgroup of T and $H = T/R$. Then $\hat{R} = \mathbb{Q} \otimes_{\mathbb{Z}} (R/[R,R])$ is isomorphic as a $\mathbb{Q}[H]$-module to $\mathbb{Q}^2 \oplus \mathbb{Q}[H]^{2g-2}$.*

This result was proved in [CW34]. We give an alternate proof in Section 2. The group ring $\mathbb{Q}[H]$ decomposes as a direct sum of simple algebras $\mathbb{Q}[H] = \mathbb{Q} \oplus \bigoplus_{i=1}^{\ell} A_i$ where each A_i is the ring of $m_i \times m_i$ matrices over a division algebra D_i with a number field $L_i/\mathbb{Q}$ as its center. Consequently, $\hat{R} \cong \mathbb{Q}^{2g} \oplus \bigoplus_{i=1}^{\ell} A_i^{2g-2}$, and so we can project to representations $\rho_{H,p,i} : \Gamma_{H,p} \to \mathrm{Aut}_{A_i}(A_i^{2g-2})$. The action on $\mathbb{Q}^{2g}$ is the standard symplectic representation.

Up to now, the above procedure follows that of [GL09] with the important exception that Grunewald and Lubotzky use the actual theorem of Gaschütz in place of Proposition 1.1. Via such representations, they show that $\mathrm{Aut}(F_n)$ virtually surjects onto a rich class of arithmetic groups, including $\mathrm{SL}_{\ell(n-1)}(\mathbb{Z})$ and $\mathrm{SL}_{\ell(n-1)}(\mathcal{O}_m)$ where ℓ ranges over all positive integers, m ranges over all integers ≥ 3, and $\mathcal{O}_m$ is the ring of integers in the number field generated by $\mathbb{Q}$ and a primitive mth root of unity.

What makes the surface case much more difficult (and interesting) is the fact that in our case $\hat{R}$ is equipped with a $\mathbb{Q}[H]$-valued skew-Hermitian sesquilinear form $\langle -, - \rangle$ on $\hat{R}$ with respect to the standard involution τ on $\mathbb{Q}[H]$ which is defined by $\tau(h) = h^{-1}$. This form can be defined in terms of the group action H and the natural symplectic structure on $\hat{R}$ coming from its identification with the rational first homology of the covering surface (see Section 3 for a detailed discussion of this form). As we will see in Section 6, $\rho_{H,p}(\Gamma_{H,p})$ preserves this form. The sesquilinear form descends to a nondegenerate A_i-valued form on each factor $M_i = A_i^{2g-2}$, and the image of $\rho_{H,p,i}$ lies in $\mathrm{Aut}_{A_i}(A_i^{2g-2}, \langle -, - \rangle)$.

On account of this, we obtain an even richer class of arithmetic quotients. We illustrate it here by some simple to state examples obtained by appropriate choices of H and p. See Section 9 for more. We denote by ζ_n the primitive nth root of unity, and by $\mathbb{Q}(\zeta_n)^+$ we denote the index 2 subfield of $\mathbb{Q}(\zeta_n)$ which is fixed by the order 2 Galois automorphism of $\mathbb{Q}(\zeta_n)$ mapping ζ_n to ζ_n^{-1}. By $\mathrm{SU}(m, m, \mathcal{O})$, we denote the subgroup of $\mathrm{SL}_{2m}(\mathcal{O})$ preserving the Hermitian form of signature (m, m), namely

$$\langle (a_1, \ldots, a_m, b_1, \ldots, b_m), (a_1', \ldots, a_m', b_1', \ldots, b_m') \rangle = \sum_{i=1}^{m} (a_i \overline{a_i'} - b_i \overline{b_i'})$$

where $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\zeta_n)$ and $\bar{}$ is the order 2 automorphism of $\mathbb{Q}(\zeta_n)$ just described.

Theorem 1.2. *For a fixed $g \geq 2$, there are virtual epimorphisms of $\mathrm{Mod}(\Sigma_g)$ onto the following arithmetic groups*:

(a) $\mathrm{Sp}(2m(g-1), \mathbb{Z})$ *for all* $m \in \mathbb{N}$,
(b) *for all* $m \in \mathbb{N}$ *and* $n \geq 3$, *the group* $\mathrm{Sp}(4m(g-1), \mathcal{O})$ *where* $\mathcal{O}$ *is the ring of integers in* $\mathbb{Q}(\zeta_n)^+$,
(c) *for all* $m \in \mathbb{N}$ *and* $n \geq 3$, *the group* $\mathrm{SU}(m(g-1), m(g-1), \mathcal{O})$ *where* $\mathcal{O}$ *is the ring of integers in* $\mathbb{Q}(\zeta_n)$,

(d) *for all* $m \in \mathbb{N}$ *and* $n \geq 3$, *an arithmetic group of type* $\mathrm{SO}(2m(g-1), 2m(g-1))$ (*whose precise description will be given in Section* 9).

Theorem 1.3. *Let* L *be an arbitrary subfield of a finite cyclotomic extension of* $\mathbb{Q}$ *and* $\mathcal{O}$ *the ring of integers of* L. *Then there is some* s_L *and* N_L *such that for every* $g \geq N_L$ *and every* $m \in \mathbb{N}$, *there is a virtual epimorphism of* $\mathrm{Mod}(\Sigma_g)$ *onto*

- $\mathrm{Sp}(2ms_L(g-1), \mathcal{O})$ *if* L *is a totally real field,*
- $\mathrm{SU}(ms_L(g-1), ms_L(g-1), \mathcal{O})$ *if* L *is a totally imaginary field.*

Note that any subfield of a cyclotomic field is necessarily either totally real or totally imaginary (see Lemma 4.2).

Taking $g = 2$ and $m = 1$ in (a) of Theorem 1.2, we obtain the following corollary which has been proven previously by Korkmaz by a different method [K03] and by McCarthy via similar techniques [M01].

Corollary 1.4. *There is a virtual epimorphism from* $\mathrm{Mod}(\Sigma_2)$ *onto* $\mathrm{Sp}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})$. *In particular, there is a virtual epimorphism of* $\mathrm{Mod}(\Sigma_2)$ *onto a free group, and hence* $\mathrm{Mod}(\Sigma_2)$ *is large.*

We also deduce the main result of [MR12] in Section 9.7.

Corollary 1.5. *For every genus* $g \geq 2$ *and every finite group* G, *there is a finite index subgroup of* $\mathrm{Mod}(\Sigma_g)$ *which surjects onto* G.

We now explain the main technical result of the paper. The standard involution τ of $\mathbb{Q}[H]$, defined above, descends to an involution on each simple factor A_i of $\mathbb{Q}[H]$ (see Lemma 3.2). Let $K_i = L_i^\tau$ be the subfield of the center L_i fixed by τ, and let $\mathfrak{O}_i$ be the image of $\mathbb{Z}[H]$ in A_i which is an order in A_i. Let $\mathcal{G}_{H,i}$ be the K_i-defined algebraic group $\mathrm{Aut}_{A_i}(A_i^{2g-2}, \langle -, - \rangle)$, and let $\mathcal{G}^1_{H,i}$ be those elements of reduced norm 1 over L_i (see Section 3.4 for the definition of reduced norm). Let $\mathcal{G}^1_{H,i}(\mathfrak{O}_i)$ be the arithmetic subgroup $\mathcal{G}^1_{H,i} \cap \mathrm{Aut}_{\mathfrak{O}_i}(\mathfrak{O}_i^{2g-2})$. Our main result says that, under a suitable condition, the image of $\Gamma_{H,p}$ contains a finite index subgroup of $\mathcal{G}^1_{H,i}(\mathfrak{O}_i)$. Namely, the suitable condition is that p be *ϕ-redundant*, which means that p factors through a surjective map $\phi : T_g \to F_g$ where F_g is the rank g free group and the induced map $p' : F_g \to H$ is *redundant*, i.e. p' contains a free generator in its kernel.

Theorem 1.6. *Suppose* $g \geq 3$ *and* $p : T_g \to H$ *is* ϕ*-redundant. Then, for* $\rho_{H,p,i}$, $\Gamma_{H,p}$, $\mathcal{G}^1_{H,i}(\mathfrak{O}_i)$ *as defined above,* $\rho_{H,p,i}(\Gamma_{H,p})$ *is commensurable with* $\mathcal{G}^1_{H,i}(\mathfrak{O}_i)$.

It is the structure of $(A_i^{2g-2}, \langle -, - \rangle)$ which ultimately determines $\mathcal{G}^1_{H,i}(\mathfrak{O}_i)$, and this structure is intimately related to the representation theory of the finite group H. The structure is determined by the pair $(A_i, \tau|_{A_i})$, and the simple factors A_i of $\mathbb{Q}[H]$ are in natural one-to-one correspondence with the nontrivial irreducible $\mathbb{Q}$-representations r_i of H (and the factor $\mathbb{Q}$ of $\mathbb{Q}[H]$ corresponds to the trivial representation). We can also extract information about the structure (Theorem 1.7

below) by extending scalars to get $\mathbb{R}$-algebras and $\mathbb{C}$-representations as follows. Let $n_i^2 = \dim_{L_i}(A_i)$. As we will see later (Proposition 4.3), K_i is a totally real field. As A_i is simple, so are $A_i \otimes_{L_i} \mathbb{C}$ and $A_i \otimes_{K_i} \mathbb{R}$; consequently, $A_i \otimes_{L_i} \mathbb{C} \cong \mathrm{Mat}_{n_i}(\mathbb{C})$, and $A_i \otimes_{K_i} \mathbb{R}$ is isomorphic to one of $\mathrm{Mat}_{n_i}(\mathbb{R}), \mathrm{Mat}_{n_i}(\mathbb{C})$, or $\mathrm{Mat}_{n_i/2}(\mathbb{H})$ where $\mathbb{H}$ denotes the Hamiltonian quaternions. Note that the projection $\mathbb{Q}[H] \to A_i$ induces a representation $H \to (A_i \otimes_{L_i} \mathbb{C})^\times$ which by the isomorphism $A_i \otimes_{L_i} \mathbb{C} \cong \mathrm{Mat}_{n_i}(\mathbb{C})$ gives an irreducible $\mathbb{C}$-representation $r_{i,\mathbb{C}} : H \to \mathrm{GL}_{n_i}(\mathbb{C})$.

After extending scalars to $\mathbb{C}$, the group $\mathcal{G}_{H,i}$ "becomes" one of the classical algebraic groups over $\mathbb{C}$. The following theorem describes the structure after extending scalars and summarizes, essentially, how we obtain the different types of arithmetic groups $(\mathrm{Sp}, \mathrm{O}, U)$ in Theorem 1.2 (For definitions of first/second kind and symplectic/orthogonal type, see Section 3.3).

Theorem 1.7. *The group $\mathcal{G}_{H,i}$ is the group of K_i-points of a K_i-defined complex algebraic group G with the additional property that*

- *$G \cong \mathrm{Sp}_{(2g-2)n_i}(\mathbb{C}) \Leftrightarrow r_{i,\mathbb{C}}(H)$ preserves a nondegenerate symmetric bilinear form $\Leftrightarrow A_i \otimes_{K_i} \mathbb{R} \cong \mathrm{Mat}_{n_i}(\mathbb{R}) \Leftrightarrow \tau|_{A_i}$ is of first kind and orthogonal type.*
- *$G \cong \mathrm{O}_{(2g-2)n_i}(\mathbb{C}) \Leftrightarrow r_{i,\mathbb{C}}(H)$ preserves a nondegenerate alternating bilinear form $\Leftrightarrow A_i \otimes_{K_i} \mathbb{R} \cong \mathrm{Mat}_{n_i/2}(\mathbb{H}) \Leftrightarrow \tau|_{A_i}$ is of first kind and symplectic type.*
- *$G \cong \mathrm{GL}_{(2g-2)n_i}(\mathbb{C}) \Leftrightarrow r_{i,\mathbb{C}}(H)$ preserves no nonzero bilinear form $\Leftrightarrow A_i \otimes_{K_i} \mathbb{R} \cong \mathrm{Mat}_{n_i}(\mathbb{C}) \Leftrightarrow \tau|_{A_i}$ is of second kind.*

Theorem 1.6 and its proof show that we have the following "procedure" to obtain a rich collection of arithmetic quotients of $\mathrm{Mod}(\Sigma_g)$. We present this procedure in the form of a theorem. Note that the homomorphism $\rho_{H,A}$ below is explicit and constructive.

Theorem 1.8. *Let H be a finite group with $d(H) < g$ generators and let A be a nontrivial simple component of $\mathbb{Q}[H]$. Let τ be the involution on A induced by the standard one of $\mathbb{Q}[H]$, let L be the center of A, and let $K = L^\tau$ be the τ-fixed subfield. Set $M = A^{2g-2}$ with free basis $x_1, \ldots, x_{g-1}, y_1, \ldots, y_{g-1}$, and endow M with the skew-Hermitian sesquilinear form satisfying $\langle x_i, y_j \rangle = \delta_{ij}, \langle y_i, x_j \rangle = -\delta_{ij}, \langle x_i, x_j \rangle = 0$, and $\langle y_i, y_j \rangle = 0$. Set $\mathcal{G}$ to be the K-algebraic group of the A-automorphisms of $(M, \langle -, - \rangle)$ and $\mathcal{G}^1$ to be its elements of reduced norm 1 over L. Set $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O}) = \mathcal{G}^1 \cap \mathrm{Aut}_{\mathfrak{O}}(\mathfrak{O}^{2g-2})$ where $\mathfrak{O}$ is the order in A which is the image of $\mathbb{Z}[H]$. Then, there is a finite index subgroup $\Gamma_H < \mathrm{Mod}(\Sigma_g)$ and a homomorphism $\rho_{H,A} : \Gamma_H \to \Omega_{H,A}$ whose image is of finite index.*

Note that since there is a bijection between nontrivial simple components A of $\mathbb{Q}[H]$ and nontrivial irreducible $\mathbb{Q}$-representations r of H, we could, with appropriate rewording, replace A with r in the above theorem. Thus, if A corresponds to r, then $\rho_{H,r} = \rho_{H,A}$ and $\Omega_{H,r} = \Omega_{H,A}$ are respectively the representation and arithmetic group promised at the beginning. Note, in addition, that in Theorem 1.8, we did not reference the ϕ-redundant homomorphism $p : T_g \to H$. The homomorphism ρ

does depend on the choice of p, but under certain conditions (such as $g \gg d(H)$) we know that different choices of p lead to representations ρ which are equivalent in a natural way. In Section 8.4, we discuss the notion of equivalence of representations ρ and when they are known to be equivalent.

Theorem 1.2 is deduced from Theorem 1.8 by making special choices of finite groups H and simple components A of $\mathbb{Q}[H]$ and then analyzing the resulting arithmetic groups, in some cases using Theorem 1.7 (see Section 9 for the corresponding irreducible representations r). For (a), we use $H = \mathrm{Sym}(m+1)$ and $A = \mathrm{Mat}_m(\mathbb{Q})$. For (b) and $m \geq 3$, we use $H = \mathrm{Alt}(m+1) \times \mathrm{Dih}(2n)$ where $\mathrm{Dih}(2n)$ is the dihedral group of order $2n$, and $A = \mathrm{Mat}_n(L)$ where L is the field $\mathbb{Q}(\zeta_n)^+$. For (c) and $m \geq 2$, we use $H = \mathrm{Sym}(m+1) \times \mathbb{Z}/n\mathbb{Z}$ and $A = \mathrm{Mat}_n(\mathbb{Q}(\zeta_n))$. For (d) and $m \geq 3$, we use $H = \mathrm{Alt}(m+1) \times \mathrm{Dic}(4n)$ where $\mathrm{Dic}(4n)$ is the dicyclic group of order $4n$ (definition in Section 9) and $A = \mathrm{Mat}_n(D)$ where D is the quaternion algebra

$$D = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Q}(\zeta_n)) | \alpha, \beta \in \mathbb{Q}(\zeta_n) \right\}.$$

For smaller m in cases (b),(c),(d), see Section 9 for the corresponding H. Theorem 1.3 is also deduced from Theorem 1.8, and the fact that, for such L, the algebra $\mathrm{Mat}_{s_L}(L)$ appears as a simple factor of $\mathbb{Q}[H]$ for some finite group H and some s_L. The reader may notice that the group $\mathcal{G}$ obtained is always of type A_n, C_n, or D_n but never B_n, G_2, F_4, E_6, E_7 or E_8.

The above mentioned results open a lot of questions. They show that the classical Torelli group of $\mathrm{Mod}(\Sigma)$ is just a first in a list of countably many "generalized Torelli subgroups"—$\ker(\rho_{H,r})$ as above. Are these subgroups (or any of them) finitely generated? Note that these are very different from the "higher Torelli groups" (or equivalently, groups in the Johnson filtration) obtained from nilpotent quotients of T_g; in fact, for any group $\mathfrak{I}$ in the Johnson filtration and any $\mathfrak{T}_{H,r} = \ker(\rho_{H,r})$ for H nontrivial, the product $\mathfrak{I}\mathfrak{T}_{H,r}$ is of finite index in $\mathrm{Mod}(\Sigma)$ (see Section 8.6).

Our theorem can be useful also toward solving the long-standing problem whether $\mathrm{Mod}(\Sigma_g)$, for $g \geq 3$, can virtually surject onto $\mathbb{Z}$. In [PW13], Putman and Wieland showed, roughly speaking, that if $\rho_{H,p}(\Gamma_{H,p})$ has no finite orbits for all p and H (a collection for which $\ker(p)$ is cofinal would suffice), then the mapping class group (for a surface of genus 1 greater) does not virtually surject to $\mathbb{Z}$. Theorem 1.6 easily implies this condition for ϕ-redundant p. This is just a step in this direction since the subgroups $\ker(p)$ for all such p do not form a cofinal family (To get the conclusion that $\mathrm{Mod}(\Sigma)$ does not virtually surject onto $\mathbb{Z}$, one must prove a similar result for covers of a surface with one boundary component. See [PW13] for the precise formulation).

The key idea for proving Theorem 1.6 is that the handlebody subgroup of the mapping class group behaves like a maximal parabolic subgroup of a semisimple Lie group. Let us elaborate. Along the way, we will indicate where each step in the argument is proved. As explained above, we are getting a representation $\rho_{H,p,i}$ of $\mathrm{Mod}(\Sigma)$, or to be more precise a finite index subgroup of it, into $\mathcal{G}_{H,i}$.

Let $\Sigma \cong \partial\mathcal{H}$ be an identification inducing $\phi : T_g \to \pi_1(\mathcal{H}) \cong F_g$ where $\mathcal{H}$ is a genus g handlebody. From [J69, Theorem 5.2], it follows that all surjective homomorphisms $\phi : T_g \to F_g$ arise this way. We analyze first the image of $\mathrm{Map}(\mathcal{H})$, the handlebody subgroup of $\mathrm{Mod}(\Sigma)$ for a handlebody $\mathcal{H}$ with boundary Σ (More accurately, we will study $\mathrm{Map}(\mathcal{H}, *)$, the handlebody group with a fixed point). This is the subgroup of $\mathrm{Mod}(\Sigma)$ consisting of all isotopy classes containing homeomorphisms which extend to $\mathcal{H}$. This important subgroup of $\mathrm{Mod}(\Sigma)$ has been actively studied in recent years—see for example [HH12,HH13]. Via its action on the fundamental group of $\mathcal{H}$, it is mapped onto $\mathrm{Out}(F_g)$, the outer automorphism group of the free group on g generators. Following carefully the definitions, one sees that when $p : T_g \to H$ is ϕ-redundant, $\rho_{H,p,i}(\mathrm{Map}(\mathcal{H}))$ acts on a submodule of M_i in precisely the same way as $\rho(\mathrm{Out}(F_g))$ in [GL09] (Section 6). We can therefore appeal to the results of [GL09] to deduce that $\rho_{H,p,i}(\mathrm{Map}(\mathcal{H}))$ contains an arithmetic subgroup of the Levi factor $\mathcal{L}$ of a suitable maximal parabolic subgroup $\mathcal{P} = \mathcal{L}\mathcal{N}^+$ of $\mathcal{G}_{H,i}$ (Section 6).

Moreover, we use again the ϕ-redundant assumption to show that the image of $\Gamma_{H,p} < \mathrm{Mod}(\Sigma_g, *)$ contains nontrivial unipotent elements in the unipotent radical $\mathcal{N}^+$ of $\mathcal{P}$ as well as of $\mathcal{N}^-$, its opposite subgroup (upper triangular versus lower triangular). At this point, we use both results as well as the fact that $\mathcal{L}$ acts irreducibly on $\mathcal{N}^+$ and on $\mathcal{N}^-$, to deduce that the image of $\mathrm{Mod}(\Sigma)$ contains finite index subgroups of $\mathcal{U}^+(\mathfrak{O}) = \mathcal{U}^+ \cap \mathcal{G}(\mathfrak{O})$ and $\mathcal{U}^-(\mathfrak{O}) = \mathcal{U}^- \cap \mathcal{G}(\mathfrak{O})$ where $\mathcal{U}^+$ and $\mathcal{U}^-$ are opposite maximal unipotent subgroups of $\mathcal{G}_{H,i}$ (Section 7). Now, we can appeal to the result of Raghunathan [R92] (see also Venkataramana [V94]) that two such subgroups generate a finite index subgroup of $\mathcal{G}^1_{H,i}(\mathfrak{O})$ and Theorem 1.6 is deduced (Section 8).

The paper is organized as follows. In Section 2, we prove an analogue of Gaschütz's Theorem for surface groups, and in Section 3, we develop what we call "Symplectic Gaschütz theory", i.e. identifying the structure of $\hat{R} = \overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$, not merely as a $\mathbb{Q}[H]$-module but also as a module with a skew-Hermitian form over $\mathbb{Q}[H]$ – an algebra with involution. We relate its structure to the representation theory of the finite group H. In Section 4, we elaborate on this connection. Most of the material in Section 4 is likely known to experts on simple algebras, but we chose to include a quick presentation which seems not to be available in this form. This material is useful when one comes to producing examples of arithmetic quotients out of finite groups H and their representations. But the reader can skip this section on a first reading, going right away to Section 5.

In Section 5, we describe a submodule of $\hat{R}$ isomorphic to $\mathbb{Q}[H]^2$ which leads (in Section 7) to an identification of two unipotent elements in $\rho_{H,p,i}(\Gamma_{H,p})$, and we prove that the sesquilinear form $\langle -, - \rangle$ on $M_i = A_i^{2g-2}$ has an isotropic submodule M_i' isomorphic to A_i^{g-1}. The parabolic subgroup $\mathcal{P}$ mentioned above consists precisely of those elements of $\mathcal{G}_{H,i}$ preserving M_i'. Some of the content of Sections 6, 7, and 8 have been indicated above; additionally, Section 6 establishes the basic properties of

$\rho_{H,p}$, and in Section 8, we finish the proof of Theorem 1.8. We end in Section 9 with proofs of the remaining results claimed in the introduction and some discussion of the arithmetic groups $\Omega_{H,A}$ as (H, A) ranges over all pairs of finite groups H and simple components A of $\mathbb{Q}[H]$.

1.1 Index of notation. For the convenience of the reader, we collect here some of the more important notation that is consistent throughout the paper.

$\mathrm{Mod}(\Sigma)$: the mapping class group of the closed surface Σ
$\mathrm{Mod}(\Sigma, *)$: the mapping class group of the closed surface Σ fixing the point $*$
g: genus of the surface
H: a finite group
r, r_i: an irreducible $\mathbb{Q}$-representation of H
A, A_i: a simple $\mathbb{Q}$-algebra (almost always denoting a component of $\mathbb{Q}[H]$)
M, M_i: modules over A, A_i (almost always denoting A^{2g-2}, A_i^{2g-2})
L, L_i: the center of A, A_i
τ: the canonical involution on $\mathbb{Q}[H]$ and each A, A_i (see Lemma 3.2.)
K, K_i: the τ-fixed subfield of L, L_i
$\langle -, - \rangle$: the sesquilinear pairing on A_i^{2g-2} (or $\hat{R}$; see Section 3.1.)
$\mathcal{G}_{H,i}$: the algebraic group $\mathrm{Aut}_{A_i}(A_i^{2g-2}, \langle -, - \rangle)$ (defined over K_i)
$\mathcal{G}^1_{H,i}$: the elements in $\mathcal{G}_{H,i}$ of reduced norm 1
$\mathfrak{O}, \mathfrak{O}_i$: an order in A, A_i which is the image of $\mathbb{Z}[H]$
$\Omega, \Omega_{H,r}, \Omega_{H,A}$: the arithmetic group consisting of $\mathfrak{O}, \mathfrak{O}_i$ points of $\mathcal{G}^1_{H,i}$ (where $A = A_i$ and r is the representation $\mathbb{Q}[H] \to A$).
$T_g := \pi_1(\Sigma_g)$
$p : T_g \to H$: some surjective homomorphism
$R := \ker(p)$
$\overline{R} = R/[R, R]$
$\hat{R} = \overline{R} \otimes \mathbb{Q}$
$\Gamma_{H,p} = \{\gamma \in \mathrm{Aut}(T_g)^+ = \mathrm{Mod}(\Sigma, *) | p \circ \gamma = p\}$
$\rho_{H,p} : \Gamma_{H,p} \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R})$: the representation for the induced action of $\Gamma_{H,p}$ on $\hat{R}$
$\rho_{H,p,i} : \Gamma_{H,p} \to \mathcal{G}^1_{H,i}$: the map $\rho_{H,p}$ followed by the projection onto the action of the ith isotypic component of $\hat{R}$
Γ_H: a finite index subgroup of $\mathrm{Mod}(\Sigma)$ (of some relation to $\Gamma_{H,p}$; see Section 8.2.)
$\rho_{H,r}, \rho_{H,A}$: alternative names for the representation $\Gamma_H \to \Omega_{H,A} = \Omega_{H,r}$ where $r : \mathbb{Q}[H] \to A$ is an irreducible representation.
$\mathcal{H}, \mathcal{H}_g$: the genus g handlebody
$\mathrm{Map}(\mathcal{H}), \mathrm{Map}(\mathcal{H}, *)$: the mapping class group of the handlebody (also called the handlebody group) respectively without and with a fixed point.
F_g: the free group of rank g
$\phi : T_g \to F_g$: a surjective homomorphism
$p' : F_g \to H$: a surjective homomorphism satisfying $p' \circ \phi = p$ (when p is ϕ-redundant)
$S := \ker(p')$

$\overline{S} = S/[S,S]$
$\hat{S} = \overline{S} \otimes \mathbb{Q}$
$\mathcal{P}$: a maximal parabolic in $\mathcal{G}_{H,i}$
$\mathcal{L}$: a Levi factor of $\mathcal{G}_{H,i}$
$\mathcal{N}^+$: the unipotent radical of $\mathcal{P}$
$\mathcal{N}^-$: the opposite subgroup of $\mathcal{N}^+$
$\mathcal{U}^+$,$\mathcal{U}^-$: opposite maximal unipotent radicals of $\mathcal{G}_{H,i}$

2 A Theorem of Gaschütz and a Generalization to Surface Groups

Suppose we have an exact sequence of groups

$$1 \to R \to T \xrightarrow{p} H \to 1$$

where T is the fundamental group of a closed orientable surface of genus g and H is a finite group. The action of T on $\overline{R} = R/[R,R]$ by conjugation descends to an action of H. Thus, $\overline{R}$ has the structure of a $\mathbb{Z}[H]$ module. In this section, we prove Proposition 1.1 from the introduction. We recall the proposition here.

Proposition 1.1. *Let $T = T_g$ be the fundamental group of a surface Σ of genus $g \geq 2$. Let R be a finite index normal subgroup of T and $H = T/R$. Then $\hat{R} = \mathbb{Q} \otimes_{\mathbb{Z}} (R/[R,R])$ is isomorphic as a $\mathbb{Q}[H]$-module to $\mathbb{Q}^2 \oplus \mathbb{Q}[H]^{2g-2}$.*

As mentioned in the introduction, this is a known result due to Chevalley–Weil. We adopt a topological viewpoint to give an alternative proof of Proposition 1.1, and we begin by translating algebraic objects into topological ones. For any normal finite index subgroup $R < T$, there is a corresponding finite index regular cover $\tilde{\Sigma} \to \Sigma$ such that the image $\pi_1(\tilde{\Sigma}) \to \pi_1(\Sigma)$ is precisely R. Using this, one can identify $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Z})$ with $\overline{R}$ and $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q}) \cong \hat{R}$. The group $H = T/R$ acts on the cover by deck transformations and thereby induces an action of H on $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$. The isomorphism $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q}) \cong \hat{R}$ is an isomorphism of $\mathbb{Q}[H]$-modules.

2.1 Gaschütz's Theorem. In the case where T is replaced by a free group F, the description of $\hat{R}$ is a classical result of Gaschütz. Since we require its use in later sections, we present Gaschütz's theorem. We also provide a new topological proof of the theorem which we then adapt for the analagous theorem for surfaces.

Theorem 2.1 (Gaschütz). *Suppose $1 \to R \to F_n \xrightarrow{p} H \to 1$ is a short exact sequence where F_n is the free group on n generators and H is a finite group. Let $\overline{R} = R/[R,R]$ and $\hat{R} = \overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, there is a $\mathbb{Q}[H]$-module isomorphism:*

$$\hat{R} \cong \mathbb{Q}[H]^{n-1} \oplus \mathbb{Q}.$$

Proof. To prove this, let us first identify F_n with the fundamental group of an n-petalled rose Y with oriented edges where each edge is one of the free generators x_i

of F_n. Let $\widetilde{Y} \to Y$ be the cover corresponding to R. Lift the orientation of Y to an orientation of the edges of $\widetilde{Y}$.

We compute $\mathrm{H}_1(\widetilde{Y}, \mathbb{Q})$ via cellular homology. Let $C_i(\widetilde{Y}, \mathbb{Q})$ denote formal sums with $\mathbb{Q}$ coefficients of i-cells of $\widetilde{Y}$. Since there are no 2-cells, $\mathrm{H}_1(\widetilde{Y}, \mathbb{Q})$ is the kernel of the boundary map ∂_1. Pick some vertex $\tilde{*}$ of the graph $\widetilde{Y}$, and let $e_1, \dots, e_n$ be the (oriented) edges going out from $\tilde{*}$ where e_i covers the edge corresponding to the generator x_i of F_n. The group H acts freely on the orbit of e_i, the H-orbit of e_i and e_j are disjoint if $i \neq j$, and the H-orbits of all the e_i cover $\widetilde{Y}$. Thus, we have an internal $\mathbb{Q}[H]$-module direct sum decomposition of the space of 1-chains

$$C_1(\widetilde{Y}, \mathbb{Q}) = \bigoplus_{i=1}^{n} \mathbb{Q}[H] \cdot e_i \cong \mathbb{Q}[H]^n.$$

Furthermore, $C_0(\widetilde{Y}, \mathbb{Q}) = \mathbb{Q}[H] \cdot \tilde{*} \cong \mathbb{Q}[H]$. The boundary map is a $\mathbb{Q}[H]$-homomorphism, and furthermore, $\partial_1(e_i) = (h_i - 1) \cdot \tilde{*}$ where $h_i = p(x_i)$.

The above argument shows that the image of ∂_1 lies in $\mathfrak{h} \cdot \tilde{*}$ where $\mathfrak{h}$ is the augmentation ideal; i.e. $\mathfrak{h}$ is the kernel of the augmentation map $\epsilon : \mathbb{Q}[H] \to \mathbb{Q}$ defined by $\sum_{h \in H} \alpha_h h \mapsto \sum_{h \in H} \alpha_h$. Since we know that $\dim_{\mathbb{Q}}(\mathrm{H}_0(\widetilde{Y}, \mathbb{Q})) = 1$, the image of ∂_1 must be the entire augmentation ideal. Semi-simplicity of $\mathbb{Q}[H]$-modules implies

$$\mathbb{Q}[H]^n \cong C_1(\widetilde{Y}, \mathbb{Q}) \cong \mathrm{H}_1(\widetilde{Y}, \mathbb{Q}) \oplus \mathfrak{h}.$$

Note that ϵ is a $\mathbb{Q}[H]$-module homomorphism from $\mathbb{Q}[H]$ to the trivial module so $\mathbb{Q}[H] \cong \mathbb{Q} \oplus \mathfrak{h}$ and $\mathrm{H}_1(\widetilde{Y}, \mathbb{Q}) \cong \mathbb{Q}[H]^{n-1} \oplus \mathbb{Q}$.

2.2 Theorem for surface groups. We now prove Proposition 1.1. Let Y_1 be the $2g$-petalled rose with oriented loops, and label the loops by a_i, b_i for $i = 1, \dots g$. Let Y be the 2-dimensional CW-complex obtained by gluing a 2-cell along its boundary to the path $[a_1, b_1][a_2, b_2] \dots [a_g, b_g]$ in Y_1 where $[x, y] = xyx^{-1}y^{-1}$. It is well known that Y is a closed, genus g surface. Let $\widetilde{Y}$ be the cover corresponding to the subgroup $R < T = \pi_1(Y)$.

As in the above proof, $\partial_1(C_1(\widetilde{Y}, \mathbb{Q})) = \mathfrak{h}$ still holds. However, in this case, $\partial_2(C_2(\widetilde{Y}, \mathbb{Q}))$ is nontrivial, so we must determine it to compute $\mathrm{H}_1(\widetilde{Y}, \mathbb{Q})$. The group H acts freely and transitively on the 2-cells of $\widetilde{Y}$, so $C_2(\widetilde{Y}, \mathbb{Q}) \cong \mathbb{Q}[H] \cdot c_2 \cong \mathbb{Q}[H]$ where c_2 is some oriented 2-cell of $\widetilde{Y}$. By semi-simplicity then, finding $\partial_2(C_2(\widetilde{Y}, \mathbb{Q}))$ is equivalent to determining $\ker(\partial_2)$ which, since there are no 3-cells, is $\mathrm{H}_2(\widetilde{Y}, \mathbb{Q})$. Since $\widetilde{Y}$ is a surface, $\mathrm{H}_2(\widetilde{Y}, \mathbb{Q}) \cong \mathbb{Q}$ as a $\mathbb{Q}$-vector space. However, we must verify that the $\mathbb{Q}[H]$-module structure is trivial. The action of $h \in H$ on $\mathrm{H}_2(\widetilde{Y}, \mathbb{Q})$ is multiplication by the degree of the map, and since H acts by orientation-preserving homeomorphisms, that degree is necessarily 1.

Thus, the image of ∂_2 is isomorphic to $\mathfrak{h}$, and by semi-simplicity of $\mathbb{Q}[H]$-modules,

$$\mathbb{Q}[H]^{2g} \cong C_1(\widetilde{Y}, \mathbb{Q}) \cong \mathrm{H}_1(\widetilde{Y}, \mathbb{Q}) \oplus \mathfrak{h}^2,$$

and the desired result follows. □

3 Symplectic Gaschütz Theory

Let us fix $R < T$, a finite index normal subgroup, and set $H = T/R$ and $\hat{R} = (R/[R,R]) \otimes_{\mathbb{Z}} \mathbb{Q}$ as above. For surface groups T, the $\mathbb{Q}[H]$-module $\hat{R}$ has a richer structure than in the analogous situation for free groups. Specifically, $\hat{R}$ admits a natural $\mathbb{Q}[H]$-valued sesquilinear form $\langle -, - \rangle$. In this section, we describe the form, and we exhibit a decomposition of the pair $(\hat{R}, \langle -, - \rangle)$ into factors. Later in Section 6, we will see that this structure is preserved by the action of $\rho_{H,p}(\Gamma_{H,p})$ (Lemma 6.2).

3.1 The sesquilinear pairing on $\hat{R}$. We first define a few necessary terms. An *anti-homomorphism* $\tau : A \to A$ of a $\mathbb{Q}$-algebra is a $\mathbb{Q}$-linear map of A such that $\tau(a_1 a_2) = \tau(a_2)\tau(a_1)$ for all $a_1, a_2 \in A$; furthermore τ is an *involution* if $\tau^2 = \mathrm{Id}$. Suppose M is an A-module. A form $\langle -, - \rangle : M \times M \to A$ is *sesquilinear* (relative to the involution τ) if it is $\mathbb{Q}$-bilinear and for any $r, s \in A$, $m, m' \in M$

$$\langle rm, sm' \rangle = r \langle m, m' \rangle \tau(s).$$

The form furthermore is *skew-Hermitian* if $\langle m, m' \rangle = -\tau(\langle m', m \rangle)$ and *nondegenerate* if for all nonzero $m \in M$, there is an $m' \in M$ such that $\langle m, m' \rangle \neq 0$.

Any group ring $\mathbb{Q}[H]$ admits a canonical involution τ defined by setting $\tau(h) = h^{-1}$ for $h \in H$ and extending linearly. Recall that $\hat{R}$ is naturally identified with $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$ which has an alternating intersection form, and we denote this form by $\langle -, - \rangle_{\mathrm{Sp}}$. In a similar way to [R34], [H83, Section 3], we define the following $\mathbb{Q}[H]$-valued form on $\hat{R}$:

$$\langle x, y \rangle = \sum_{h \in H} \langle x, hy \rangle_{\mathrm{Sp}} h. \tag{1}$$

LEMMA 3.1. *The form $\langle -, - \rangle$ is nondegenerate, sesquilinear with respect to τ, and skew-Hermitian.*

Proof. Nondegeneracy follows from the nondegeneracy of the symplectic form. It can be readily checked that sesquilinearity follows from the fact that H preserves the symplectic form. The action of H preserves the symplectic form as it is equivalent to the action of deck transformations on $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$ and deck transformations act by orientation preserving homeomorphisms. The form $\langle -, - \rangle$ is skew-Hermitian since $\langle -, - \rangle_{\mathrm{Sp}}$ is alternating. □

3.2 Simple components of $\mathbb{Q}[H]$. We now recall some basic facts about the group ring $\mathbb{Q}[H]$ and its modules. The ring $\mathbb{Q}[H]$ is a semisimple $\mathbb{Q}$-algebra and thus is isomorphic to a finite product of simple $\mathbb{Q}$-algebras

$$\mathbb{Q}[H] = \mathbb{Q} \times \prod_{i=1}^{\ell} A_i.$$

Moreover, for each i, we have $A_i \cong \mathrm{Mat}_{m_i}(D_i)$ for some finite-dimensional division algebra D_i with center L_i which is a finite-dimensional field extension of $\mathbb{Q}$. For all

i, the algebra A_i acts on the $\mathbb{Q}$-vector space $V_i = D_i^{m_i}$ by left multiplication; via the projection to A_i, each V_i is a $\mathbb{Q}[H]$-module which is furthermore irreducible. We say V_i is the irreducible module (or representation) corresponding to A_i. Moreover, every irreducible $\mathbb{Q}[H]$-module (or representation of H) is isomorphic to one of the V_i, and note that as a $\mathbb{Q}[H]$-module, $A_i \cong V_i^{m_i}$.

We describe how τ acts on the decomposition in the following lemma.

LEMMA 3.2. *Each A_i in the decomposition of $\mathbb{Q}[H]$ is τ-invariant.*

Proof. Note that each A_i is a minimal two-sided ideal of $\mathbb{Q}[H]$. For the purpose of the proof, set A_0 to be the trivial factor $\mathbb{Q}$ in the decomposition of $\mathbb{Q}[H]$. Since τ is an anti-homomorphism, τ sends minimal two-sided ideals to minimal two-sided ideals. Since τ is order 2, there are two possibilities; for any i either $\tau(A_i) = A_i$, or there is a $j \neq i$ such that $\tau(A_i) = A_j$ and $\tau(A_j) = A_i$. We must rule out the second possibility (Our proof depends on the base field being the totally real field $\mathbb{Q}$. The lemma is false, for instance, over $\mathbb{C}$).

Let e_i be the unit in A_i. It suffices to show that $\tau(e_i)A_i \neq 0$. Consider the representation

$$\Psi : \mathbb{Q}[H] \to \mathrm{End}_{\mathbb{Q}}(A_i) \cong \mathrm{Mat}_t(\mathbb{Q})$$

given by left multiplication where $t = \dim_{\mathbb{Q}}(A_i)$. Viewing the matrices with entries in $\mathbb{C}$ yields a representation of H to $\mathrm{GL}_t(\mathbb{C})$, and so $\chi(h) = \overline{\chi(h^{-1})}$ where χ is the character for Ψ and $^-$ indicates complex conjugation. Since the traces are necessarily rational, in fact $\chi(h) = \chi(h^{-1})$, and linearity of χ implies $\chi(r) = \chi(\tau(r))$ for any $r \in \mathbb{Q}[H]$. Thus, $0 \neq \chi(e_i) = \chi(\tau(e_i))$ and left multiplication on A_i by $\tau(e_i)$ is non-zero.

Recall from Theorem 2.1 that $\hat{R} \cong \mathbb{Q}[H]^{2g-2} \oplus \mathbb{Q}^2$. Thus, as a $\mathbb{Q}[H]$-module

$$\hat{R} \cong \mathbb{Q}^{2g} \oplus \left(\bigoplus_{i=1}^{\ell} A_i^{2g-2} \right).$$

Let $M_i \subseteq \hat{R}$ be the submodule such that $M_i \cong A_i^{2g-2}$. Each A_i is isomorphic to several copies of an irreducible $\mathbb{Q}[H]$-module V_i and $V_i \ncong V_j$ for $i \neq j$. Hence, the submodule M_i is unique, and furthermore any $\mathbb{Q}[H]$-automorphism φ of $\hat{R}$ restricts to an automorphism of each M_i. Since all A_j except A_i annihilate M_i, we obtain a representation

$$\mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}, \langle -, - \rangle) \to \mathrm{Aut}_{A_i}(M_i, \langle -, - \rangle).$$

Our next task then is to understand this automorphism group (Note that we omitted the module corresponding to the trivial representation. This is because the automorphism group turns out to be $\mathrm{Sp}(2g, \mathbb{Q})$ and the representation $\Gamma_{H,p} \to \mathrm{Sp}(2g, \mathbb{Q})$ is the standard symplectic representation of the mapping class group).

3.3 The automorphism group of M_i. We first need to know the properties of $\langle -, - \rangle$ restricted to each M_i. By abuse of notation, we will view τ as an involution on A_i.

LEMMA 3.3. *For any $m, m' \in M_i$, the pairing $\langle m, m' \rangle$ lies in A_i. Furthermore, $\langle -, - \rangle : M_i \times M_i \to A_i$ is a nondegenerate, sesquilinear, skew-Hermitian form when viewed as a form with values in A_i.*

Proof. Let e_i be the unit in A_i. When restricted to M_i, the form takes values in A_i since sesquilinearity implies that

$$\langle m, m' \rangle = \langle e_i m, e_i m' \rangle = e_i \langle m, m' \rangle \tau(e_i) \in A_i.$$

When viewed as a form with values in A_i, it is clear that the form remains sesquilinear and skew-Hermitian. Since $\langle -, - \rangle$ is nondegenerate on all of $\hat{R}$, to show that it is nondegenerate on M_i, we only need to show that the M_i are mutually perpendicular. This is verified by essentially the same computation. If $m \in M_i$ and $m' \in M_j$ and $i \neq j$, then

$$\langle m, m' \rangle = \langle e_i m, e_j m' \rangle = e_i \langle m, m' \rangle \tau(e_j).$$

Lemma 3.2 implies that $\tau(e_j) = e_j$, so the product is 0. □

The group $\mathrm{Aut}_{A_i}(M_i, \langle -, - \rangle)$ is the set of the K_i-points of an algebraic group defined over K_i where $K_i = L_i^\tau$, the fixed field of τ acting on L_i. Our next goal is to determine the structure of this algebraic group; to this end, we will use some of the basic theory of involutions and follow the exposition in [PR94, Section 2.3.3].

Involutions In this subsection, we utilize the dictionary between nondegenerate bilinear forms and involutions to describe the structure of $\mathcal{G}_{H,i} = \mathrm{Aut}_{A_i}(M_i, \langle -, - \rangle)$. For convenience, we will fix $A = A_i$, $M = M_i$, and $\mathcal{G} = \mathcal{G}_{H,i}$ as we will only be considering each algebra individually, so $M \cong A^{2(g-1)}$ with the sesquilinear form as described above. We set L to be the center of A and $K = L^\tau$ the subfield of L fixed by τ. The dictionary is that the sesquilinear form goes over to the unique involution $\sigma : \mathrm{End}_A(M) \to \mathrm{End}_A(M)$ satisfying the following for all $m, m' \in M$ and $C \in \mathrm{End}_A(M)$:

$$\langle Cm, m' \rangle = \langle m, \sigma(C) m' \rangle.$$

This is the *adjoint involution* associated to the sesquilinear form. Now,

$$\begin{aligned} \mathrm{Aut}_A(M, \langle -, - \rangle) &= \{C \in \mathrm{End}_A(M) \mid \langle Cm, Cm' \rangle = \langle m, m' \rangle \quad \forall m, m' \in M\} \\ &= \{C \in \mathrm{End}_A(M) \mid \langle m, \sigma(C) C m' \rangle = \langle m, m' \rangle \quad \forall m, m' \in M\} \\ &= \{C \in \mathrm{End}_A(M) \mid \sigma(C) C = \mathrm{Id}\} = \mathcal{G}. \end{aligned}$$

In other words, those automorphisms preserving the form can be entirely determined by the involution alone.

Involutions of finite-dimensional simple algebras over a field k form a trichotomy based on kind/type. The first distinction is that of kind. An involution τ on a finite-dimensional simple algebra A over a field k is *of the first kind* if it fixes the center of A and is *of the second kind* if it does not. Furthermore, if A is of the first kind and $n^2 = \dim_L(A)$, then either $\dim_L(A^\tau) = n(n+1)/2$ or $\dim_L(A^\tau) = n(n-1)/2$ where L is the center of A and A^τ is the subspace of A fixed by τ. If the former is true, we say τ is of *orthogonal type* and if the latter is true, τ is of *symplectic type*. It is a standard fact that these are the only two possible types of involutions of the first kind and this fact is, in particular, implied by Lemma 3.6. We note that in [PR94], orthogonal and symplectic type are called first and second type respectively.

We now set $B = \mathrm{End}_A(M)$ and seek to understand the kind and type of the involution σ in terms of the kind and type of τ. First, however, we prove that B is itself a simple algebra. Since M is a free A-module of rank $2g-2$, B is isomorphic to $\mathrm{Mat}_{2g-2}(A^{op})$ and we henceforth fix some such identification.

LEMMA 3.4. *B is simple.*

Proof. Since A is a simple finite dimensional $\mathbb{Q}$-algebra, so is A^{op}, and so A^{op} is isomorphic to a matrix algebra $\mathrm{Mat}_m(D)$ over a division ring D. Thus, $B \cong \mathrm{Mat}_{2g-2}(A^{op}) \cong \mathrm{Mat}_{(2g-2)m}(D)$ which is simple. □

We now convert our terminology into that of matrices to establish the relation between the type and kind of τ and σ. Note that τ is also an involution on A^{op} of the same kind and type. For a matrix $C = (c_{ij}) \in \mathrm{Mat}_{2g-2}(A^{op}) = B$, we set $C^* = (\tau(c_{ji}))$. Letting $e_1, \ldots, e_{2g-2}$ be the standard free basis of A^{2g-2}, we define a matrix $F = (f_{ij})$ where $f_{ij} := \langle e_j, e_i \rangle$. It can be checked that $\langle Cv, w \rangle = \langle v, Dw \rangle$ for all $v, w \in M$ if and only if $FC = D^*F$. Moreover, $F^* = -F$ as $\langle -, - \rangle$ is skew-Hermitian. Thus, since $(FC)^* = C^*F^* = -C^*F$ and $(D^*F)^* = -FD$, we have

$$\sigma(C) = F^{-1}C^*F.$$

LEMMA 3.5. *The involutions σ and τ are of the same kind. The type of σ is opposite that of τ.*

Proof. It is clear that $L^\sigma = L^\tau$ so they are of the same kind. A straightforward argument counting dimension shows that the involution $*$ on B has the same type as τ if they are both first kind. Because $\langle -, - \rangle$ is skew-Hermitian, it follows that $F^* = -F$. Then, a computation shows that if $C^* = -C$, then $\sigma(F^{-1}C) = F^{-1}C$ and if $C^* = C$, then $\sigma(F^{-1}C) = -F^{-1}C$. Hence, via F^{-1}, the $+1$ eigenspace of $*$ is isomorphic to the -1 eigenspace of σ and vice versa. This implies σ has the opposite type to $*$.

Extending scalars. Consider now the following three examples of involutions ν for matrix algebras over $\mathbb{C}$.

(1) $\nu : \mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C})$ defined by $\nu(N) = N^t$.

(2) $\nu : \mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C})$ defined by $\nu(N) = JN^tJ^{-1}$ where n is even and $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$.

(3) $\nu : \mathrm{Mat}_n(\mathbb{C}) \times \mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C}) \times \mathrm{Mat}_n(\mathbb{C})$ defined by $\nu(A, B) = (B^t, A^t)$.

Note that if we consider the elements satisfying $\nu(M)M = I$, then from (1), we obtain $\mathrm{O}_n(\mathbb{C})$, from (2), $\mathrm{Sp}_n(\mathbb{C})$ and from (3), $\mathrm{GL}_n(\mathbb{C})$. Moreover, it can be easily checked that the involution in (1) is of orthogonal type and the involution in (2) is of symplectic type. We quote the following result [PR94] which essentially tells us these are the only involutions after extending scalars.

LEMMA 3.6. *Let B be a finite-dimensional simple $\mathbb{Q}$-algebra with center L and involution σ. Let $K = L^\sigma$ and let $\tilde{\sigma}$ be the unique $\mathbb{C}$-linear extension of σ to $B \underset{K}{\otimes} \mathbb{C}$. Set $n = \dim_L(B)$.*

- *If σ is of the first kind, then there is a $\mathbb{C}$-algebra isomorphism*

$$\varphi : B \underset{K}{\otimes} \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C})$$

such that $\nu = \varphi\tilde{\sigma}\varphi^{-1}$ is one of the involutions (1) *or* (2).
- *If σ is of the second kind, then there is a $\mathbb{C}$-algebra isomorphism*

$$\varphi : B \underset{K}{\otimes} \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C}) \times \mathrm{Mat}_n(\mathbb{C})$$

such that $\nu = \varphi\tilde{\sigma}\varphi^{-1}$ is the involution (3).

At this point, we can already prove part of Theorem 1.7. Specifically, we can show that the type of $\mathcal{G}$ is determined by the type and kind of τ. We will be able to prove the full theorem after establishing further results in Section 4.

3.4 Reduced norm, reduced trace, and $\mathcal{G}^1(\mathfrak{O})$. We conclude this section with a few facts on reduced norms and apply them to

$$\mathcal{G}(\mathfrak{O}) = \mathrm{Aut}_{\mathfrak{O}}(\mathfrak{O}^{2g-2}, \langle -, - \rangle) \subseteq \mathrm{End}_A(A^{2g-2})$$

where, as defined in the introduction, $\mathfrak{O}$ is the image of $\mathbb{Z}[H]$ in A. Our goal is to prove Proposition 3.9, which gives an "upper bound" on the image of the representation ρ which we study (while Theorem 1.6 gives the "lower bound"). Recall from the introduction that $\mathcal{G}^1(\mathfrak{O}) = \mathcal{G}^1_{H,i}(\mathfrak{O})$ is defined to be the subgroup of $\mathcal{G}(\mathfrak{O})$ consisting of elements of reduced norm 1.

The reduced norm (over L) of a finite-dimensional central simple L-algebra B is defined as follows. Let E be any field extension of L such that $B \otimes_L E$ *splits*, i.e. there is some isomorphism $\varphi : B \otimes_L E \to \mathrm{Mat}_n(E)$ for some n. Then the *reduced norm* (over L) for $b \in B$ is

$$\mathrm{nrd}_{B/L}(b) = \det(\varphi(b \otimes 1)).$$

The reduced norm is independent of the isomorphism φ, and $\mathrm{nrd}_{B/L}(B) \subseteq L$ (see e.g. [R75, Section 9]). In later sections, we also use the *reduced trace* which, for $b \in B$, is

$$\mathrm{trd}_{B/L}(b) = \mathrm{Tr}(\varphi(b \otimes 1))$$

where Tr is the trace of the E-linear map $\varphi(b)$. Just as for reduced norm, the reduced trace always lies in L and is independent of φ. From the definitions, it is clear that $\mathrm{trd}_{B/L}$ is L-linear.

LEMMA 3.7. *Let* $B = \mathrm{Mat}_{2g-2}(A^{op})$. *Let* $b \in \mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle) \subseteq B$ *and* $\lambda = \mathrm{nrd}_{B/L}(b)$. *Then,* $\tau(\lambda)\lambda = 1$. *In particular, if* τ *is of the first kind, then* $\lambda = \pm 1$.

Proof. We know that $b \in \mathcal{G}$ satisfies $1 = \sigma(b)b$, and so

$$1 = \mathrm{nrd}_{B/L}(\sigma(b)) \, \mathrm{nrd}_{B/L}(b) = \mathrm{nrd}_{B/L}(\sigma(b))\lambda.$$

Thus, it suffices to show that $\mathrm{nrd}_{B/L}(\sigma(b)) = \tau(\lambda)$.

Let E be a finite Galois field extension of L such that there is an isomorphism $\varphi : B \otimes_L E \cong \mathrm{Mat}_n(E)$ for some n. Let ϕ be the composition $B \to B \otimes_L E \cong \mathrm{Mat}_n(E)$. Let $\nu = \tau|_L$, and let $\tilde{\nu}$ be an extension of ν to a Galois automorphism of E. For $C = (c_{ij}) \in \mathrm{Mat}_n(E)$, define $C^* = (\tilde{\nu}(c_{ji}))$. Now, let $\psi : B \to \mathrm{Mat}_n(E)$ be the map defined by $b \mapsto (\phi(\sigma(b)))^*$. Note that since σ and * are both anti-homomorphisms, ψ is a homomorphism, and moreover, one can check that ψ is an L-algebra homomorphism. By the Skolem–Noether Theorem, ψ and ϕ are the same up to conjugation by an element of $\mathrm{Mat}_n(E)$. Thus,

$$\mathrm{nrd}_{B/L}(\sigma(b)) = \det(\phi(\sigma(b))) = \nu^{-1}(\det(\psi(b))) = \nu^{-1}(\det(\phi(b))) = \nu^{-1}(\mathrm{nrd}_{B/L}(b)).$$

Since $\mathrm{nrd}_{B/L}(b) \in L$, we can replace ν^{-1} with τ^{-1} or equivalently τ. □

We next show that elements in the ring of integers in a cyclotomic field E of "absolute value" ± 1 are roots of unity.

LEMMA 3.8. *Let* $E = \mathbb{Q}(\zeta)$ *be a cyclotomic field, let* $\mathcal{O}_E$ *its ring of integers, and let* $\iota : E \to \mathbb{C}$ *be some embedding into* $\mathbb{C}$. *If* $\lambda \in \mathcal{O}_E$ *and* $|\iota(\lambda)|^2 = 1$, *then* λ *is a root of unity.*

Proof. According to a theorem of Kronecker, if all the Galois conjugates of an algebraic integer λ have absolute value ≤ 1, then λ is a root of unity. Let ν be the order 2 Galois automorphism that is the restriction of complex conjugation (via ι). As $|\iota(e)|^2 = \iota(\nu(e)e)$ for any $e \in E$, it will suffice to show that $\nu(\sigma(\lambda))\sigma(\lambda) = 1$ for all Galois automorphisms σ of E. Since $E/\mathbb{Q}$ is cyclotomic, its Galois group is abelian, and thus

$$\nu(\sigma(\lambda))\sigma(\lambda) = \sigma(\nu(\lambda))\sigma(\lambda) = \sigma(\nu(\lambda)\lambda) = \sigma(1) = 1.$$ □

REMARK. The above lemma holds for any CM-field. The essential point is that complex conjugation always restricts to the same automorphism of E regardless of the embedding of E into $\mathbb{C}$.

PROPOSITION 3.9. *The group $\mathcal{G}^1(\mathfrak{O})$ is of finite index in $\mathcal{G}(\mathfrak{O})$.*

Proof. It suffices to show that the image of $\mathcal{G}(\mathfrak{O})$ under $\mathrm{nrd}_{B/L}$ consists only of roots of unity. If τ is of the first kind, this is obvious by Lemma 3.7. Suppose τ is of the second kind. Any $\lambda \in \mathrm{nrd}_{B/L}(\mathcal{G}(\mathfrak{O}))$ lies in $\mathcal{O}_L$ where $\mathcal{O}_L$ is the ring of integers in L, and by Lemma 3.7, λ satisfies $\tau(\lambda)\lambda = 1$. Fix some embedding $\iota : L \to \mathbb{C}$. By Proposition 4.3 below, $\tau|_L$ extends to complex conjugation, and so $1 = \iota(\tau(\lambda)\lambda) = \overline{\iota(\lambda)}\iota(\lambda) = |\iota(\lambda)|^2$. Since L is a subfield of a cyclotomic field E (to which ι extends), by Lemma 3.8, λ is a root of unity in L. □

4 Determining Type and Kind of τ

The kind of algebraic group into which $\rho_{H,p,i}$ maps depends on $\tau|_{A_i}$. The kind and type of τ depends on the representation theory of the finite group H. We therefore dedicate this section to study this dependency. This will be important later when we come in Section 9 to produce specific arithmetic groups as (virtual) quotients of $\mathrm{Mod}(\Sigma)$. However, this section may be skipped on a first reading if the reader wants to see first why the image of $\rho_{H,p,i}$ is an arithmetic group. Before beginning, we note additionally that the material presented here is known to experts, but we include it for the convenience of the non-expert and for lack of a convenient reference. As in the previous section, we will focus on one nontrivial component of $\mathbb{Q}[H]$ and drop the subscript i. Since we fix some A, by abuse of notation, we will refer to $\tau|_A$ as τ.

Recall that there is a trichotomy: τ can be of the first kind and orthogonal type, of the first kind and symplectic type, or of the second kind. This trichotomy corresponds in a nice way to other trichotomies in the representation theory of the finite group H. The first trichotomy arises from the various kinds of invariant bilinear forms for complex representations. Fix some embedding $L \hookrightarrow \mathbb{C}$ and some isomorphism $A \otimes_L \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C})$. Then the composition $H \to A \to A \otimes_L \mathbb{C} \to \mathrm{Mat}_n(\mathbb{C})$ yields an action of H on $V = \mathbb{C}^n$ which in turn is an irreducible $\mathbb{C}[H]$-module. There are three possibilities: V has an H-invariant non-degenerate symmetric bilinear form, an H-invariant non-degenerate alternating bilinear form, or no nonzero H-invariant bilinear form. This corresponds to the type and kind of τ as follows.

PROPOSITION 4.1. *Keeping notation as above, we have that, restricted to A, the involution τ is*

- *of the first kind and orthogonal type if and only if V has an H-invariant nondegenerate symmetric bilinear form,*
- *of the first kind and symplectic type if and only if V has an H-invariant non-degenerate alternating bilinear form,*

- *of the second kind if and only if V has no invariant non-zero H-invariant nondegenerate bilinear form.*

Before proving this proposition, we first describe two other trichotomies closely related to the trichotomy of kind and type. One of these is a trichotomy involving the real representations of H. This trichotomy also relates to a dichotomy involving the center L of A. In order to present the dichotomy, we first recall some elementary facts about L. A short proof of the lemma is given below.

LEMMA 4.2. *Let A be a simple component of $\mathbb{Q}[H]$ with center L. Then, L is a subfield of a cyclotomic field extension of $\mathbb{Q}$. Moreover, L is either totally imaginary (there are no embeddings $L \hookrightarrow \mathbb{R}$) or totally real (all embeddings $L \hookrightarrow \mathbb{C}$ have image in $\mathbb{R}$).*

The next proposition presents the relation to kind and type. The isomorphisms in the proposition below are as $\mathbb{R}$-algebras.

PROPOSITION 4.3. *Let notation be as above, let $n^2 = \dim_L(A)$ and let $e : L \hookrightarrow \mathbb{C}$ be an arbitrary embedding. Then, the embedding satisfies $K = e^{-1}(\mathbb{R})$, i.e. τ, restricted to A, is of the first kind if and only if L is totally real. If τ is of the second kind, then $\tau|_L$ extends to complex conjugation via the embedding e. Moreover, restricted to A, the involution τ is*

- *of the first kind and orthogonal type if and only if $A \otimes_{K,e} \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R})$,*
- *of the first kind and symplectic type if and only if $A \otimes_{K,e} \mathbb{R} \cong \mathrm{Mat}_{n/2}(\mathbb{H})$,*
- *of the second kind if and only if $A \otimes_{K,e} \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{C})$.*

Another trichotomy relates to the Frobenius–Schur indicator $\iota\chi$ for any character χ of H, defined to be

$$\iota\chi = \frac{1}{|H|} \sum_{h \in H} \chi(h^2).$$

We will be quoting some results from [JL01] where $\iota\chi$ is defined differently and only for irreducible $\mathbb{C}$-characters (over $\mathbb{C}$). However, the definitions coincide for irreducible characters (see the proof of Theorem 23.14 in [JL01]), and this is all we require.

PROPOSITION 4.4. *Continuing our notation as above, let χ be the character corresponding to the irreducible $\mathbb{Q}$-representation V of H. Then, restricted to A, the involution τ is*

- *of the first kind and orthogonal type if and only if $\iota\chi > 0$,*
- *of the first kind and symplectic type if and only if $\iota\chi < 0$,*
- *of the second kind if and only if $\iota\chi = 0$*

We start with the following elementary lemma showing that τ is the unique involution on A with a certain property.

LEMMA 4.5. *Suppose k is some field and $\psi : k[H] \to A$ is a surjective homomorphism of k-algebras. Then, there is at most one k-algebra involution ν on A such that $\nu(\psi(h))\psi(h) = \mathrm{Id}$.*

Proof. The elements $\psi(h)$ generate A as a k-vector space. □

Proof of Proposition 4.1. Suppose τ is of the first kind. Then, τ is L-linear and the involution extends to a ($\mathbb{C}$-algebra) involution $\tilde{\tau}$ of $A \otimes_L \mathbb{C}$. By Lemma 3.6, there is an isomorphism $\varphi : A \otimes_L \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C})$ such that $\nu = \varphi\tilde{\tau}\varphi^{-1}$ is the standard symplectic or orthogonal involution. If ψ is the composition $\mathbb{Q}[H] \to A \to A \otimes_L \mathbb{C}$, then it is the case that $\tilde{\tau}(\psi(h))\psi(h) = \mathrm{Id}$ and so $\nu(\varphi(\psi(h)))\ \varphi(\psi(h)) = \mathrm{Id}$. This implies $\varphi(\psi(h))$ preserves a nondegenerate symmetric bilinear form (resp. alternating form) if τ is of orthogonal (resp. symplectic) type.

Suppose that V has a non-zero H-invariant bilinear form. Then, since V is irreducible, the form must be nondegenerate because a nontrivial null space would necessarily be H-invariant. Now, let ψ be the projection $\mathbb{Q}[H] \to A$. For all $h \in H$, the adjoint involution ν associated to the form satisfies $\nu(\psi(h) \otimes 1) = (\psi(h) \otimes 1)^{-1}$. Thus, ν preserves $A = A \otimes 1$, and by Lemma 4.5 $\nu|_A = \tau$. Since ν is $\mathbb{C}$-linear, $L \otimes 1 = 1 \otimes L$, and $\nu|_{L \otimes 1} = \tau$, the involution τ is L-linear and thus of the first kind. Moreover, ν is the extension of τ, so they are of the same type and ν is of orthogonal type (resp. symplectic type) when the invariant bilinear form is symmetric (resp. alternating). □

Before moving on to the next characterization, we first prove Lemma 4.2 and a lemma about involutions when projecting $\mathbb{R}[H]$ to a simple $\mathbb{R}$-algebra.

Proof of Lemma 4.2 First we show L is a subfield of a cyclotomic field. The reduced trace (over L) is an L-linear map $\mathrm{trd}_{A/L} : A \to L$, and it is clear that it is surjective (Indeed, $\mathrm{trd}_{A/L}(L) = L$). Choose some embedding $L \to \mathbb{C}$ and an isomorphism $\varphi : A \otimes_L \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C})$, and let $r : \mathbb{Q}[H] \to A$ be the projection. Some power of the image $\varphi(r(h) \otimes 1)$ is the identity, and so its trace (which is $\mathrm{trd}_{A/L}(r(h))$ by definition) is a sum of roots of unity. The composition $\mathrm{trd}_{A/L} \circ r$ is $\mathbb{Q}$-linear and H spans the image L as a $\mathbb{Q}$-vector space. It is clear from this that L is a subfield of a cyclotomic field. The second claim follows from the fact that subfields of cyclotomic fields are all Galois extensions of $\mathbb{Q}$. □

LEMMA 4.6. *Suppose there is a surjection of $\mathbb{R}$-algebras $\psi : \mathbb{R}[H] \to B$ where B is simple. There is an $\mathbb{R}$-linear involution ν on B such that $\nu(\psi(h))\psi(h) = \mathrm{Id}$ for every $h \in H$ and*

- *ν is of the first kind and orthogonal type if and only if $B \cong \mathrm{Mat}_m(\mathbb{R})$ for some $m \in \mathbb{N}$,*
- *ν is of the first kind and symplectic type if and only if $B \cong \mathrm{Mat}_m(\mathbb{H})$ for some $m \in \mathbb{N}$,*
- *ν is of second kind if and only if $B \cong \mathrm{Mat}_m(\mathbb{C})$ for some $m \in \mathbb{N}$, in which case the center of B is $\mathbb{C}$ and $\mathbb{C}^\nu = \mathbb{R}$.*

Proof. First, note that since the only finite-dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$, and $\mathbb{H}$, it follows that B is isomorphic to one of $\mathrm{Mat}_m(\mathbb{R}), \mathrm{Mat}_m(\mathbb{C}), \mathrm{Mat}_m(\mathbb{H})$ for some $m \in \mathbb{N}$. Let respectively D be one of $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$. We can, without loss of generality, identify B with $\mathrm{Mat}_m(D)$, and thus obtain a corresponding action on D^m.

In the cases of $D = \mathbb{R}, \mathbb{C}$, we can average the standard inner or Hermitian product on D^m under H to obtain an H-invariant inner or Hermitian product. In the case of $\mathbb{H}$, there is also a standard Hermitian product, namely $v \cdot w = \sum_{i=1}^m v_i \overline{w_i}$ where $\overline{w}$ is the involution on $\mathbb{H}$ given by $\overline{a + bi + cj + dk} = a - bi - cj - dk$. In this case also, averaging the standard Hermitian product yields an H-invariant Hermitian product. In each case $v \cdot v > 0$ for nonzero v and the average has the same property. By a D-linear change of basis via Gram-Schmidt, we may assume the H-invariant inner or Hermitian products are the standard ones. We can take $\nu(b) = b^t$ in the case of $D = \mathbb{R}$ and $\nu(b) = \overline{b}^t$ in the cases of $D = \mathbb{C}, \mathbb{H}$. This involution is easily checked to satisfy the claimed properties. Uniqueness of ν by Lemma 4.5 allows us to conclude the "only if" in each of the three statements. □

Proof of Proposition 4.3. Let $K' = e^{-1}(\mathbb{R})$. Implicitly, when we tensor over K' or L, we will do it via the map e. If $K' \neq L$, then we have an isomorphism $e' : L \otimes_{K'} \mathbb{R} \to \mathbb{C}$ satisfying $e'(\ell \otimes \lambda) = e(\ell)\lambda$, and so by associativity of tensor products, there are isomorphisms

$$A \otimes_{K'} \mathbb{R} \cong A \otimes_L (L \otimes_{K'} \mathbb{R}) \cong A \otimes_L \mathbb{C}.$$

In either case ($L = K'$ or $L \neq K'$), $A \otimes_{K'} \mathbb{R}$ is isomorphic to A tensored over its center L with a simple $\mathbb{R}$-algebra ($\mathbb{R}$ or $\mathbb{C}$) and hence is simple. We have $A \otimes_{K'} \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R}), \mathrm{Mat}_n(\mathbb{C})$, or $\mathrm{Mat}_{n/2}(\mathbb{H})$.

Let $\varphi : \mathbb{Q}[H] \to A$ be the projection. There is an induced homomorphism $\mathbb{R}[H] = \mathbb{Q}[H] \otimes_{\mathbb{Q}} \mathbb{R} \to A \otimes_{K'} \mathbb{R}$, and since the image of H generates A over $\mathbb{Q}$ (and K'), this map is surjective. Let ν be the involution on $A \otimes_{K'} \mathbb{R}$ as in Lemma 4.6, which is unique by Lemma 4.5. Since $\nu(\varphi(h)) = \varphi(h)^{-1}$ and $\varphi(h) \in A \otimes 1$, the involution ν restricts to an involution on $A = A \otimes 1$ which is K'-linear (hence $\mathbb{Q}$-linear). By uniqueness (Lemma 4.5), $\nu|_A = \tau$. By Lemma 4.6, the ν-fixed subfield of the center in all cases is $\mathbb{R}$ whose intersection with $e(L)$ is $e(K')$, and agreement of ν and τ on A implies $K' = K$.

The above argument implies that if $L = K$, then all embeddings of L in $\mathbb{C}$ are real-valued; consequently, $A \otimes_K \mathbb{R}$ has an involution of the first kind and orthogonal or symplectic type and so $A \otimes_K \mathbb{R}$ is isomorphic to either $\mathrm{Mat}_n(\mathbb{R})$ or $\mathrm{Mat}_{n/2}(\mathbb{H})$ respectively. Conversely, if $A \otimes_K \mathbb{R}$ is either $\mathrm{Mat}_n(\mathbb{R})$ or $\mathrm{Mat}_{n/2}(\mathbb{H})$, then ν fixes the center and so fixes L which implies τ is of the first kind. The remaining cases are $L \neq K$ and $A \otimes_K \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{C})$ and so they coincide. □

To prove Proposition 4.4, we first establish some facts for $\iota\chi$ when χ is an irreducible $\mathbb{C}$-character. We recall some theorems relating $\iota\chi$ to the existence of certain

invariant bilinear forms on irreducible representations and translate them into facts about involutions. We will then bootstrap the results to $\mathbb{Q}$ to prove the proposition. We recall Theorem 23.16 from [JL01] with some mild modification. Note that for irreducible characters (over $\mathbb{C}$), $\iota\chi$ takes only values in $\{-1, 0, 1\}$.

Theorem 4.7. *Suppose V is an irreducible $\mathbb{C}[H]$-module with character χ. Then $\iota\chi \neq 0$ if and only if V admits a non-zero H-invariant bilinear form, and in this case, the form is nondegenerate. Furthermore, the form is symmetric if and only if $\iota\chi = 1$ and skew-symmetric if and only if $\iota\chi = -1$.*

Proof. This is precisely Theorem 23.16 from [JL01] except for our claim that the forms are nondegenerate (In [JL01], it only says "non-zero"). The form must be non-degenerate by Proposition 4.1. □

By Proposition 4.1, proving Proposition 4.4 requires only that we translate information about complex traces to rational ones. Recall that A is a simple factor in the decomposition of $\mathbb{Q}[H]$. Let W be the corresponding irreducible $\mathbb{Q}$-representation. Let $\mathcal{A} = A \otimes_L \mathbb{C}$. We have a surjection $\mathbb{C}[H] \cong \mathbb{Q}[H] \otimes_{\mathbb{Q}} \mathbb{C} \to \mathcal{A} \cong \mathrm{Mat}_n(\mathbb{C})$ and a corresponding irreducible $\mathbb{C}$-representation V. Unfortunately, it is not always the case that V is W tensored with $\mathbb{C}$, so we must expend some effort to relate the characters.

First, we recall the definitions of various traces for algebras over fields and some well-known facts relating them. Suppose A is a finite-dimensional $\mathbb{Q}$-algebra with center L. Then, A acts on itself by left multiplication and this gives a representation $\eta_\ell : A \to \mathrm{End}_L(A)$. Define the trace of $a \in A$ over L to be

$$\mathrm{Tr}_{A/L}(a) = \mathrm{tr}(\eta_\ell(a)).$$

Furthermore, for any field k contained in L, left multiplication by a is k-linear and we can consider the trace as a k-linear map on the k-vector space A. Denote this new trace $\mathrm{Tr}_{A/k}(a)$.

If k is a subfield of L, then as for A, we can view elements in L as k-linear maps on L by left multiplication. As before we have $\mathrm{Tr}_{L/k}(\alpha)$ for $\alpha \in L$. We recall the following elementary fact about traces [R75, Section 9]. In particular, for the algebra A, we have $\mathrm{Tr}_{A/k}(a) = \mathrm{Tr}_{L/k}(\mathrm{Tr}_{A/L}(a))$.

Lemma 4.8. *Suppose V is an L-vector space and $T : V \to V$ is L-linear. Let T_k be T viewed as a k-linear map on the k-vector space V. Then,*

$$\mathrm{tr}(T_k) = \mathrm{Tr}_{L/k}(\mathrm{tr}(T)).$$

We relate the trace $\mathrm{Tr}_{A/L}$ and the corresponding character for irreducible representations.

LEMMA 4.9. *Suppose V is k-vector space and $H \to \mathrm{GL}(V)$ is an irreducible k-representation and suppose A is the corresponding simple k-algebra in the decomposition of $k[H]$. Let χ be the character of V. Then, for $a \in A$,*

$$m\chi(a) = \mathrm{Tr}_{A/k}(a)$$

where $A \cong V^m$ as $k[H]$-modules.

Proof. By definition of character, $\chi(a)$ is the trace of a via the action of $k[H]$, and hence A, on V. The action of A on itself block-diagonalizes as m copies of its action on V and the result easily follows. □

Recall the reduced trace $\mathrm{trd}_{A/L}$ for a central simple L-algebra A from Section 3.4. In addition to the properties discussed in that section, we have that $\mathrm{Tr}_{A/L} = n\,\mathrm{trd}_{A/L}$ where $n^2 = \dim_L(A)$ (see [R75, Section 9]). Now, we have the tools to prove Proposition 4.4.

Proof of Proposition 4.4. As above, set $\mathcal{A} = A \otimes_L \mathbb{C}$ which has an isomorphism $\varphi : \mathcal{A} \to \mathrm{Mat}_n(\mathbb{C})$, and let V be the corresponding irreducible $\mathbb{C}$-representation of H. Let ψ be the corresponding character. Proposition 4.1 and Theorem 4.7 imply that it is sufficient to show that $\iota\psi$ and $\iota\chi$ are positive multiples of each other.

Now suppose $\eta_A : H \to A^\times$ is the representation from H to the invertible elements of A and $\eta_{\mathcal{A}} : H \to \mathcal{A}^\times$ is the composition of η_A with the canonical $A \to A \otimes_L \mathbb{C} = \mathcal{A}$. Note that for all $h \in H$, by definition, $\psi(h)$ is the trace of $\eta_{\mathcal{A}}(h)$ which is the reduced trace (over L) of $\eta_A(h)$. Thus,

$$|H|\iota\psi = \sum_{h\in H} \psi(h^2) = \sum_{h\in H} \mathrm{trd}_{A/L}(\eta_A(h^2)).$$

By the properties of reduced trace,

$$\sum_{h\in H} \mathrm{trd}_{A/L}(\eta_A(h^2)) = \frac{1}{n} \sum_{h\in H} \mathrm{Tr}_{A/L}(\eta_A(h^2)).$$

Now, suppose m is such that $A \cong V^m$ where V is the irreducible representation corresponding to A. Since $\iota\psi \in \{-1, 0, 1\}$, we further have that if $d = \dim_{\mathbb{Q}}(L)$,

$$\begin{aligned} |H|\iota\psi &= \frac{|H|}{d} \mathrm{Tr}_{L/\mathbb{Q}}(\iota\psi) = \frac{1}{nd} \mathrm{Tr}_{L/\mathbb{Q}} \left(\sum_{h\in H} \mathrm{Tr}_{A/L}(\eta_A(h^2)) \right) \\ &= \frac{1}{nd} \sum_{h\in H} \mathrm{Tr}_{A/\mathbb{Q}}(\eta_A(h^2)) = \frac{m}{nd} \sum_{h\in H} \chi(h^2) = \frac{|H|m}{nd} \iota\chi. \end{aligned}$$

where the fourth equality follows from Lemma 4.9. □

We now prove Theorem 1.7. As we have been doing, we drop the subscript i in our proof.

Proof of Theorem 1.7 Recall that $\mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle)$, and that σ is the adjoint involution defined on $B = \mathrm{Mat}_{2g-2}(A^{op})$ and associated to $\langle -, - \rangle$. Extend σ (uniquely) to a $\mathbb{C}$-linear involution $\tilde{\sigma}$ on $B \underset{K}{\otimes} \mathbb{C}$ and let

$$G = \left\{ C \in B \underset{K}{\otimes} \mathbb{C} \mid \tilde{\sigma}(C)C = I \right\}.$$

Then, G is a K-defined algebraic group whose K-points are $\mathcal{G}$. Let $n^2 = \dim_L(A)$.

First, suppose that τ is of the first kind. By Lemma 3.6, there is an isomorphism $\varphi : B \otimes_K \mathbb{C} \to \mathrm{Mat}_{(2g-2)n}(\mathbb{C})$ such that $\nu = \varphi\tilde{\sigma}\varphi^{-1}$ is either involution (1) or (2). The involution ν has the same type as $\tilde{\sigma}$ and σ, which, by Lemma 3.5, have the opposite type of τ. Thus φ maps G isomorphically onto $\mathrm{Sp}_{(2g-2)n}(\mathbb{C})$ if τ is of orthogonal type and onto $\mathrm{O}_{(2g-2)n}(\mathbb{C})$ otherwise.

If τ is of the second kind, then there is an isomorphism $\varphi : B \otimes_K \mathbb{C} \to \mathrm{Mat}_{(2g-2)n}(\mathbb{C}) \times \mathrm{Mat}_{(2g-2)n}(\mathbb{C})$ such that $\nu = \varphi\tilde{\sigma}\varphi^{-1}$ is the involution (3). Arguments similar to the above show $G \cong \mathrm{GL}_{(2g-2)n}(\mathbb{C})$. The remaining equivalences follow from Propositions 4.1 and 4.3. □

5 Submodules of M_i

In this section we analyze further the structure of $\hat{R}$, when p is ϕ-redundant. In this case, we show that $\hat{R}$ decomposes into two isomorphic totally isotropic submodules. Later, in Section 6, we will see that the image of the handlebody group under ρ preserves one of the submodules and thus has a block uppertriangular form. Moreover, we will show that when p is ϕ-redundant, there is an explicit rank two $\mathbb{Q}[H]$-submodule of $\hat{R}$ which allows us (in Section 6) to produce two tightly controlled unipotent elements in the image of $\rho_{H,p}$.

Recall that if $\phi : T_g \to F_g$ is a surjective homomorphism, we say that an epimorphism $p : T_g \to H$ is ϕ-redundant if p factors through an epimorphism $p' : F_g \to H$ which is redundant (i.e. the kernel contains a free generator). As mentioned in the introduction, every epimorphism $\phi : T_g \to F_g$ arises as follows [J69, Theorem 5.2]. Let $\mathcal{H} = \mathcal{H}_g$ be a genus g handlebody and pick some identification of $\partial\mathcal{H}$ with Σ_g. The inclusion $\Sigma_g \hookrightarrow \mathcal{H}$ induces a map on the fundamental groups which is surjective. Since the fundamental group of $\mathcal{H}$ is a free group, this induces a surjective map $\phi : T_g \to F_g = \pi_1(\mathcal{H})$ where F_g is the free group of rank g. Henceforth, we will simply refer to $\pi_1(\mathcal{H})$ as F_g.

Now fix some $\phi : T_g \to F_g$ arising from an identification $\Sigma \cong \partial\mathcal{H}$, fix some ϕ-redundant p, and set $S = \ker p'$ for the corresponding $p' : F_g \to H$. Let $\tilde{\Sigma} \to \Sigma$ be the cover corresponding to p.

5.1 The handlebody group and $\mathrm{Aut}(F_g)$. In this section, we recall a basic fact about handlebody groups. Let $*$ be some point on the boundary of $\mathcal{H}$. The handlebody group with fixed point, $\mathrm{Map}(\mathcal{H}, *)$, is the subgroup of those mapping

classes in $\mathrm{Mod}(\Sigma, *)$ which contain a representative homeomorphism extending to a homeomorphism of $\mathcal{H}$. Recall that the handlebody group (without fixed point) $\mathrm{Map}(\mathcal{H})$ is the similarly defined subgroup of $\mathrm{Mod}(\Sigma)$.

Theorem 5.1 [Z62, G64, M63]. *The natural homomorphisms* $\mathrm{Map}(\mathcal{H}, *) \to \mathrm{Aut}(F_g)$ *and* $\mathrm{Map}(\mathcal{H}) \to \mathrm{Out}(F_g)$ *are surjective.*

5.2 Free submodule of rank two. We start by finding a special torus with one boundary component embedded in Σ. Let $* \in \Sigma = \partial\mathcal{H}$ be a basepoint for the fundamental groups of both $\mathcal{H}$ and Σ.

LEMMA 5.2. *Let* $p : T_g \to H$ *be* ϕ*-redundant and* $p' : F_g \to H$ *the induced map. Then,* Σ *contains a subsurface* Σ' *homeomorphic to a torus with one boundary component such that the image of* $\pi_1(\Sigma', *)$ *in* $\pi_1(\Sigma, *) = T_g$ *lies in the kernel of* p*. Moreover, there are simple closed curves* a, b *in* Σ' *such that*

- a *and* b *intersect once, and* $\langle a, b\rangle_{\mathrm{Sp}} = 1$,
- *the homology classes of* a,b *generate* $\mathrm{H}_1(\Sigma', \mathbb{Q})$,
- b *bounds a disc in* $\mathcal{H}$,
- a, b *avoid* $*$.

Proof. Let α be a free basis element of F_g lying in the kernel of p'. This exists by the assumption that p is ϕ-redundant. We first show that the homotopy class α contains some simple closed curve a supported on Σ. Moreover, we show that there is an oriented simple closed curve b on Σ passing through $*$ such that b intersects a transversely at one point and the based homotopy class of b lies in the kernel of ϕ (Note that since we define $\mathrm{Mod}(\Sigma)$ as $\mathrm{Homeo}^+(\Sigma)/\mathrm{Homeo}_0(\Sigma)$, we are implicitly working in the category of topological spaces and so "transverse intersection" strictly speaking has no meaning. However, $\mathrm{Mod}(\Sigma)$ is also $\mathrm{Diff}^+(\Sigma)/\mathrm{Diff}_0(\Sigma)$, and we can just as well work in the smooth category). To see all this, note that by assumption there is some free basis $\alpha = \alpha_1, \ldots, \alpha_g$ of F_g. Recall that $\phi : T_g \to F_g$ is the natural map on fundamental groups. By explicit construction, one can find a (potentially different) free basis $\alpha'_1, \ldots, \alpha'_g$ of F_g such that each homotopy class α'_i contains a simple closed curve a'_i on Σ; moreover, we can ensure there is some oriented simple closed curve b' passing through $*$ such that a'_1 and b intersect once transversely and b' bounds a disc in $\mathcal{H}$ (so b' lies in the kernel of ϕ). See Figure 1.

Since $\mathrm{Map}(\mathcal{H}, *) \to \mathrm{Aut}(F_g)$ is surjective (Theorem 5.1), there is some homeomorphism φ of the handlebody fixing $*$ and mapping α'_1 to α. Let $a = \varphi(a')$ and $b = \varphi(b')$. Note that b bounds a disc in $\mathcal{H}$ as well.

Since a and b intersect once transversely, a regular neighborhood Σ' of a and b in Σ is a torus with one boundary component and with fundamental group generated by the homotopy classes of a and b. Since (the homotopy classes of) a and b both lie in the kernel of p, it follows that (the image of) $\pi_1(\Sigma', *)$ lies in the kernel.

As it stands, the curves a, b satisfy the first three properties required by the lemma but a and b do not avoid $*$. This is easily fixed by an isotopy of the curves. □

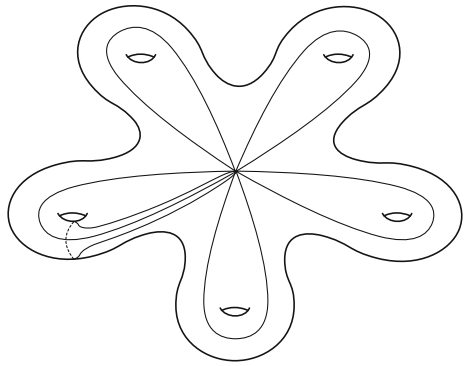

Figure 1: The curves $a'_1, \dots, a'_g$ and b' in the proof of Lemma 5.2 for $g = 5$

Let Σ', a, b be as in the lemma. Then, the preimage of Σ' under the cover $\tilde{\Sigma} \to \Sigma$ consists of $|H|$ disjoint homeomorphic copies of Σ'. Label these surfaces as $\tilde{\Sigma}'_h$ as h ranges over H so that $d_h(\tilde{\Sigma}'_{1_H}) = \tilde{\Sigma}'_h$ where d_h is the deck transformation induced by $h \in H$.

Similar to Σ', the preimages of a and b each consist of $|H|$ simple closed curves which project homeomorphically to a and b via the covering map. Call the preimages $\tilde{a}_h$ and $\tilde{b}_h$ as h ranges over H so that a_h, b_h lie in $\tilde{\Sigma}'_h$. Then, $a_h = d_h(a_{1_H})$ and $b_h = d_h(b_{1_H})$. For a simple closed curve c, we denote its homology class by $[c]$.

LEMMA 5.3. *Let notation be as above. Then* $[\tilde{a}_{1_H}]$ (*similarly* $[\tilde{b}_{1_H}]$) *generates a submodule of* $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$ *isomorphic to* $\mathbb{Q}[H]$. *Together,* $[\tilde{a}_{1_H}]$ *and* $[\tilde{b}_{1_H}]$ *generate a submodule isomorphic to* $\mathbb{Q}[H]^2$. *Moreover,* $\langle [\tilde{a}_{1_H}], [\tilde{b}_{1_H}] \rangle = 1$.

Proof. Consider the disjoint union $\tilde{\Sigma}' = \cup_{h \in H} \Sigma'_h$. From the Mayer–Vietoris sequence, one can deduce that $\mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q})$ is a direct summand as a $\mathbb{Q}$-vector space of $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$. Since the action of H preserves $\tilde{\Sigma}'$ and its complement, $\mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q})$ is a summand as a $\mathbb{Q}[H]$-module. As $\tilde{\Sigma}'$ is the disjoint union of the $\tilde{\Sigma}'_h$, it follows that $\mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q}) \cong \bigoplus_{h \in H} \mathrm{H}_1(\tilde{\Sigma}'_h, \mathbb{Q})$. Each $\mathrm{H}_1(\tilde{\Sigma}'_h, \mathbb{Q})$ is 2-dimensional so $\dim_{\mathbb{Q}} \mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q}) = 2|H|$.

Now, we know that for each $h \in H$, the classes $[\tilde{a}_h]$ and $[\tilde{b}_h]$ generate $\mathrm{H}_1(\tilde{\Sigma}'_h, \mathbb{Q})$, and so $[\tilde{a}_{1_H}], [\tilde{b}_{1_H}]$ generate $\mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q})$ as a $\mathbb{Q}[H]$-module. Because of dimension, we must have $[\tilde{a}_{1_H}], [\tilde{b}_{1_H}]$ freely generate, and $\mathrm{H}_1(\tilde{\Sigma}', \mathbb{Q}) \cong \mathbb{Q}[H]^2$. It follows that each of $[\tilde{a}_{1_H}]$ and $[\tilde{b}_{1_H}]$ generate a module isomorphic to $\mathbb{Q}[H]$. For the last claim, recall that by definition,

$$\langle [\tilde{a}_{1_H}], [\tilde{b}_{1_H}] \rangle = \sum_{h \in H} \langle [\tilde{a}_{1_H}], h \cdot [\tilde{b}_{1_H}] \rangle_{\mathrm{Sp}} h.$$

Since $h \cdot [\tilde{b}_{1_H}] = [\tilde{b}_h]$ is disjoint from $\tilde{a}_{1_H}$, the only term which survives is that for $h = 1_H$. Since $\langle [\tilde{a}_{1_H}], [\tilde{b}_{1_H}] \rangle_{\mathrm{Sp}} = \langle [a], [b] \rangle_{\mathrm{Sp}} = 1$, the claim follows. □

5.3 Totally isotropic subspaces. The inclusion $\Sigma_g \hookrightarrow \mathcal{H}$ induces a surjective map $\mathrm{H}_1(\Sigma_g, \mathbb{Q}) \to \mathrm{H}_1(\mathcal{H}, \mathbb{Q})$. It follows that the action of a homeomorphism of the handlebody preserves the kernel. It is easy to see that the kernel of this map is *totally isotropic* relative to the alternating intersection form $\langle -, - \rangle_{\mathrm{Sp}}$. I.e. for any two elements β, β' in the kernel, $\langle \beta, \beta' \rangle_{\mathrm{Sp}} = 0$. Moreover, this subspace has a complementary totally isotropic subspace which projects onto $\mathrm{H}_1(\mathcal{H}, \mathbb{Q})$. We want to show similarly that $\hat{R} = \mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$ has an isotropic submodule and decomposition.

Now, let $\hat{S} = (S/[S,S]) \otimes_{\mathbb{Z}} \mathbb{Q}$ which is naturally identified with $\mathrm{H}_1(\tilde{\mathcal{H}}, \mathbb{Q})$, the rational first homology of the cover $\tilde{\mathcal{H}} \to \mathcal{H}$ corresponding to the inclusion $S \to F_g$. Let $\hat{P}$ be the kernel of the map $\hat{\phi}_R : \hat{R} \to \hat{S}$ induced by ϕ. Note that this kernel is equivalent to the kernel of the map $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q}) \to \mathrm{H}_1(\tilde{\mathcal{H}}, \mathbb{Q})$.

LEMMA 5.4. *The subspace $\hat{P}$ is a $\mathbb{Q}[H]$-submodule which is totally isotropic relative to the sesquilinear form $\langle -, - \rangle$. Moreover, as $\mathbb{Q}[H]$-modules, $\hat{R} \cong \hat{P} \oplus \hat{S}$ and both $\hat{P}$ and $\hat{S}$ are isomorphic to $\mathbb{Q}[H]^{g-1} \oplus \mathbb{Q}$.*

We remark that below we show that the isomorphism $\hat{P} \oplus \hat{S} \cong \hat{R}$ can be chosen such that the image of $\hat{S}$ is totally isotropic relative to $\langle -, - \rangle$.

Proof. As mentioned above, the map $\mathrm{H}_1(\Sigma, \mathbb{Q}) \to \mathrm{H}_1(\mathcal{H}, \mathbb{Q})$ has totally isotropic kernel relative to the alternating intersection form. Applying the same fact to the map on the covers $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q}) \to \mathrm{H}_1(\tilde{\mathcal{H}}, \mathbb{Q})$ implies that $\hat{P}$ is totally isotropic relative to $\langle -, - \rangle_{\mathrm{Sp}}$. Since the sesquilinear form is defined as a sum with coefficients in terms of $\langle -, - \rangle_{\mathrm{Sp}}$, it follows that $\hat{P}$ is also totally isotropic relative to the sesquilinear form.

It follows from the definitions that $\hat{\phi}_R$ is a $\mathbb{Q}[H]$-homomorphism, so its kernel, $\hat{P}$, is a $\mathbb{Q}[H]$-submodule. By Theorem 2.1, $\hat{S} \cong \mathbb{Q}[H]^{g-1} \oplus \mathbb{Q}$. This fact combined with Proposition 1.1 and surjectivity of $\hat{\phi}_R$ implies the rest of the Lemma since $\mathbb{Q}[H]$ is semisimple. □

Now consider the above situation projected to the ith isotypic component M_i of $\hat{R}$ using the notation of the previous sections. The above decomposition projects to a decomposition of M_i, and we can conclude a stronger statement relative to the sesquilinear form. Let M_i' be the projection of $\hat{P}$ to M_i.

LEMMA 5.5. *Let $\tilde{a}_{1_H}, \tilde{b}_{1_H}$ be as in Lemma 5.3 and $\tilde{\alpha}_i, \tilde{\beta}_i$ the projection of their homology classes to M_i. The module M_i' is totally isotropic relative to $\langle -, - \rangle$, and there is a subspace M_i'' of M_i such that*

- *M_i'' is totally isotropic relative to $\langle -, - \rangle$,*
- *$M_i = M_i' \oplus M_i''$,*
- *there are free A_i-bases $\tilde{\beta}_i = m'_{i,1}, m'_{i,2}, \ldots, m'_{i,g-1}$ (resp. $\tilde{\alpha}_i = m''_{i,1}, m''_{i,2}, \ldots, m''_{i,g-1}$) of M_i' (resp. M_i'') such that $\langle m''_{i,j}, m'_{i,k} \rangle = \delta_{j,k}$.*

Proof. The module M_i' is totally isotropic since $\hat{P}$ is. Notice that by the choice of $\tilde{b}_{1_H}$, its homology class lies in $\hat{P}$. The homology class of $\tilde{b}_{1_H}$ generates a copy of $\mathbb{Q}[H]$ in $\hat{P}$, and so $[\tilde{b}_{1_H}]$ necessarily generates a copy of A_i in M_i. Thus, $\tilde{\beta}_i$ can be

extended to some basis $\tilde{\beta}_i = m'_{i,1}, m'_{i,2}, \dots, m'_{i,g-1}$ of M'_i. Furthermore, we can ensure $\langle \tilde{\alpha}_i, m'_{i,j} \rangle = \delta_{1j}$ (If it is not already true, we can alter $m'_{i,j}$ for $j > 1$ by adding an appropriate multiple of $\tilde{\beta}_i$).

Lemma 5.4 implies that M'_i is isomorphic to A_i^{g-1}, and so we immediately have some complementary subspace N_i which is isomorphic to A_i^{g-1} (but not necessarily isotropic). Moreover, since $\tilde{\alpha}_i$ does not lie in M'_i, we can further arrange that N_i contains $\tilde{\alpha}_i$. Consider the homomorphism to the dual space of N_i

$$\begin{aligned} M'_i &\to \mathrm{Hom}_{A_i}(N_i, A_i) \\ m'_i &\mapsto \langle -, m'_i \rangle. \end{aligned} \tag{2}$$

Note that this is an A_i-module homomorphism where the (left) A_i-module structure on $\mathrm{Hom}_{A_i}(N_i, A_i)$ is given by $(a \cdot f)(n) = (f(n))\tau(a)$ for all $n \in N_i$. Since M'_i is totally isotropic and $\langle -, - \rangle$ is nondegenerate, each $m' \in M'_i$ must pair nontrivially with some element in N_i. Consequently, the map in (2) has trivial kernel, and the fact that $\mathrm{Hom}_{A_i}(N_i, A_i) \cong A_i^{g-1}$ implies (2) is an isomorphism.

There is therefore a unique basis $n_{i,1}, \dots, n_{i,g-1}$ of N_i such that $\langle n_{i,j}, m'_{i,k} \rangle = \delta_{j,k}$. Moreover, since $\tilde{\alpha}_i$ lies in N_i and $\langle \alpha_i, m'_{i,j} \rangle = \delta_{1j}$, it follows that $n_{i,1} = \tilde{\alpha}_i$. From N_i, we can construct a submodule M''_i which has the same properties as N_i but is also isotropic.

Let $c_{j,k} = \langle n_{i,j}, n_{i,k} \rangle$ for $j \neq k$, and let $c_{j,j} = \frac{1}{2}\langle n_{i,j}, n_{i,j} \rangle$. Note that since $\langle -, - \rangle$ is skew-Hermitian, $\tau(c_{j,k}) = -c_{k,j}$. Let $m''_{i,j} = n_{i,j} + \sum_{\ell \leq j} c_{j,\ell} m'_{i,\ell}$ and M''_i be the submodule generated by $m''_{i,1}, \dots, m''_{i,g-1}$. Note that $m''_{i,1} = n_{i,1} = \tilde{\alpha}_i$. It follows from the properties of the $n_{i,j}$ and the fact that M'_i is isotropic that $\langle m''_{i,j}, m'_{i,k} \rangle = \delta_{jk}$. Moreover, one computes that for all pairs $j > k$:

$$\begin{aligned} \langle m''_{i,j}, m''_{i,k} \rangle &= \langle n_{i,j}, n_{i,k} \rangle + \left\langle \sum_{\ell \leq j} c_{j,\ell} m'_{i,\ell}, n_{i,k} \right\rangle + \left\langle n_{i,j}, \sum_{\ell \leq k} c_{k,\ell} m'_{i,\ell} \right\rangle \\ &= c_{j,k} + \langle c_{j,k} m'_{i,k}, n_{i,k} \rangle = c_{j,k} - c_{j,k} = 0. \end{aligned}$$

Similarly,

$$\begin{aligned} \langle m''_{i,j}, m''_{i,j} \rangle &= \langle n_{i,j}, n_{i,j} \rangle + \langle c_{j,j} m'_{i,j}, n_{i,j} \rangle + \langle n_{i,j}, c_{j,j} m'_{i,j} \rangle \\ &= 2c_{j,j} - c_{j,j} + \tau(c_{j,j}) = 0. \end{aligned}$$

Thus, M''_i has all the desired properties. □

Corollary 5.6. *The submodule $\hat{P}$ has a complementary totally isotropic isomorphic submodule in $\hat{R}$.*

Proof. By Lemma 5.5, there is a direct sum decomposition of $\hat{R}$ as a $\mathbb{Q}[H]$-module:

$$\hat{R} = \mathbb{Q}^{2g} \oplus \bigoplus_{i=1}^{\ell} M_i = \mathbb{Q}^{2g} \oplus \bigoplus_{i=1}^{\ell} (M'_i \oplus M''_i)$$

where M_i' and M_i'' are isotropic and $M_i' = \hat{P} \cap M_i$. Similarly, $\mathbb{Q}^{2g} \cap \hat{P} \cong \mathbb{Q}^g$ and there is a complimentary isotropic subspace B isomorphic to $\mathbb{Q}^g$. The submodule complementary to $\hat{P}$ is $B \oplus (\bigoplus_{i=1}^{\ell} M_i'')$. □

6 The Representation ρ and the Image of the Handlebody Group

We now provide more details about the representations $\rho_{H,p}$. As mentioned in the introduction, we will work with $\mathrm{Aut}(T_g)^+ = \mathrm{Mod}(\Sigma_g, *)$ instead of $\mathrm{Mod}(\Sigma_g)$, and at the end (Section 8.2) we will use (virtual) arithmetic quotients of the former to obtain (virtual) arithmetic quotients of the latter. As in the previous section, let $p : T_g \to H$ be a ϕ-redundant surjective homomorphism, and let S be the kernel of the induced map $p' : F_g \to H$. We have the following commutative diagram and short exact sequences.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R & \longrightarrow & T_g & \xrightarrow{p} & H & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \| & & \\ 1 & \longrightarrow & S & \longrightarrow & F_g & \xrightarrow{p'} & H & \longrightarrow & 1 \end{array}$$

We set

$$\Gamma_{H,p} = \{f \in \mathrm{Aut}(T_g)^+ \mid p \circ f = p\}.$$

Note that if $f \in \Gamma_{H,p}$, then it follows automatically that $f(R) = R$. For such f, we can restrict the automorphism to R and then project to an automorphism of the abelianization $\overline{R}$. This, in turn, induces an automorphism of $\hat{R}$. Denote this map as $\rho_{H,p} : \Gamma_{H,p} \to \mathrm{Aut}(\hat{R})$. For the remainder of this section, we will suppress the subscripts H and p, so henceforth we fix some p and H, and set $\rho = \rho_{H,p}$ and $\Gamma = \Gamma_{H,p}$.

As we have seen, $\hat{R}$ has a $\mathbb{Q}[H]$-module structure, and this is preserved by such f.

LEMMA 6.1. *The image $\rho(\Gamma)$ lies in $\mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R})$.*

Proof. Let $f \in \Gamma$, and let $\overline{f}$ be the induced action of f on $\overline{R}$. It suffices to check that $\overline{f}$ commutes with the action of H. Suppose $r \in R$ and $\overline{r} \in \overline{R}$ is its image in the quotient. For any $h \in H$, the action on $\overline{f}(\overline{r}) = \overline{f(r)}$ is $h \cdot \overline{f}(\overline{r}) = \overline{hf(r)h^{-1}}$. Since $f \in \Gamma$, it follows that f is a trivial automorphism mod R, and so $r_0 f(h) = h$ for some $r_0 \in R$ and

$$\overline{hf(r)h^{-1}} = \overline{r_0 f(hrh^{-1}) r_0^{-1}} = \overline{f(hrh^{-1})} = \overline{f}(h \cdot \overline{r}).$$ □

To show that $\rho(f)$ additionally preserves the form $\langle -, - \rangle$, we appeal to a topological reformulation. Interpreted in a topological setting, the homomorphism can be viewed as lifting the homeomorphisms to the cover and using the induced action

on the first homology group. Let us be more precise. Suppose $\tilde{*}$ is a point in the fiber over $* \in \Sigma$ for the cover $\tilde{\Sigma} \to \Sigma$. For a homeomorphism $\varphi \in \mathrm{Homeo}(\Sigma, *)$, the lift of φ is the homeomorphism $\tilde{\varphi}$ fixing $\tilde{*}$ such that $\Pi \circ \tilde{\varphi} = \varphi \circ \Pi$ where $\Pi : \tilde{\Sigma} \to \Sigma$ is the covering map. The homeomorphism φ will lift precisely when the induced action of φ on $\pi_1(\Sigma, *)$ preserves $R = \pi_1(\tilde{\Sigma}, \tilde{*})$, i.e. its mapping class is an element of Γ. Moreover, this lifting induces a well-defined homomorphism $\Gamma \to \mathrm{Mod}(\tilde{\Sigma}, \tilde{*})$. Recall that $\hat{R}$ is naturally identified with $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$. If $f \in \Gamma$ and $\tilde{f} \in \mathrm{Mod}(\tilde{\Sigma}, \tilde{*})$ is its lift, then $\rho(f) = \tilde{f}_*$ where $\tilde{f}_*$ is the induced action on $\mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$. We can now establish the following.

LEMMA 6.2. *The action of $\rho(f)$ preserves the sesquilinear form $\langle -, - \rangle$ for all $f \in \Gamma$.*

Proof. By the above discussion, $\rho(f)$ is equivalent to $\tilde{f}_*$ which is the action induced by the orientation-preserving mapping class $\tilde{f}$. Since such a homomorphism preserves $\langle -, - \rangle_{\mathrm{Sp}}$, and, in addition, $\rho(f)$ acts by a $\mathbb{Q}[H]$-automorphism by Lemma 6.1, it must preserve $\langle -, - \rangle$.

Since the image acts by $\mathbb{Q}[H]$-automorphisms, it decomposes into actions on each isotypic component. Consequently, we obtain representations

$$\rho_i = \rho_{H,p,i} : \Gamma \to \mathrm{Aut}_{A_i}(M_i, \langle -, - \rangle)$$

by projecting the action.

6.1 Previous results for automorphisms of a free group. Here, we recall a theorem from [GL09] which describes the image of $\mathrm{Aut}(F_n)$ for a representation analogous to ρ. We will use this result to show that the image of the handlebody group maps (virtually) onto the $\mathfrak{O}$-points of the Levi factor of a parabolic subgroup of $\mathrm{Aut}_{A_i}(A_i^{2g-2}, \langle -, - \rangle)$. The essential connection between the two is that $\mathrm{Map}(\mathcal{H}, *)$ surjects onto $\mathrm{Aut}(F_g)$ via the action on its fundamental group.

We set up some additional notation and define some new terms. For any group X and subgroup Y, we set

$$\mathrm{Aut}(X|Y) = \{f \in \mathrm{Aut}(X) \mid f(Y) = Y\}.$$

Moreover, for Y normal, let $\mathrm{Aut}^t(X|Y)$ be the subgroup of $\mathrm{Aut}(X|Y)$ consisting of automorphisms acting trivially on X/Y. Note that in this notation $\Gamma = \mathrm{Aut}(T_g)^+ \cap \mathrm{Aut}^t(T_g|R)$. We have a homomorphism $\eta = \eta_{H,p} : \mathrm{Aut}^t(F_g|S) \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{S})$ defined similarly to ρ; namely restrict the automorphism to S, project to the abelianization $\overline{S}$, and take the induced map on $\hat{S} = \overline{S} \otimes_{\mathbb{Z}} \mathbb{Q}$.

By Gaschütz's theorem (Theorem 2.1), $\hat{S} \cong \mathbb{Q}[H]^{g-1} \oplus \mathbb{Q}$. Consequently, for each i, we obtain, via projection, a representation

$$\eta_i : \mathrm{Aut}^t(F_g|S) \to \mathrm{Aut}_{A_i}(A_i^{g-1}) = \mathrm{GL}_{g-1}(A_i^{op}).$$

Recall that A_i is simple and isomorphic to $\mathrm{Mat}_{m_i}(D_i)$ for some division algebra D_i and integer m_i. Thus, we can furthermore identify the target space as follows.

$$\mathrm{GL}_{g-1}(A_i^{op}) \cong \mathrm{GL}_{g-1}(\mathrm{Mat}_{m_i}(D_i)^{op}) \cong \mathrm{GL}_{(g-1)m_i}(D_i^{op}).$$

The special linear group $\mathrm{SL}_{(g-1)m_i}(D_i^{op})$ is the group of matrices C satisfying $\mathrm{nrd}_{B/L}(C) = 1$ for $B = \mathrm{End}_{D_i}(D_i^{m_i(g-1)})$.

Now, suppose K is some number field, and suppose D is a finite-dimensional K-algebra. Then a subring $\mathcal{R} \subseteq D$ is an *order* if it contains a K-basis of D and it is a finitely generated $\mathbb{Z}$-module. Recall that A_i is finite-dimensional over K_i, (the τ-fixed subfield of its center), and so D_i is a finite-dimensional K_i-algebra. The next theorem is a direct consequence of Theorem 5.5 of [GL09].

Theorem 6.3 (Grunewald–Lubotzky). *Keeping notation as above, if $g \geq 4$, then there exists an order $\mathcal{R}_i$ of D_i^{op} such that the intersection $\eta_i(\mathrm{Aut}^t(F_g|S)) \cap \mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$ is of finite index in $\mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$.*

Remark 6.4. Theorem 5.5 in [GL09] is proved for $g \geq 4$. However, as explained on page 1592 there, it is also true when $g = 3$ in many cases, e.g. if $m_i > 1$. Moreover, even if $m_i = 1$, the image of η_i contains finite index subgroups of the upper and lower unitriangular subgroups of $\mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$. The issue is that it is not clear there that these unitriangular subgroups generate $\mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$. But in any event, they generate a Zariski dense subgroup.

6.2 Structure of the image of the handlebody group. Here, we will analyze the image of the handlebody subgroup $\mathrm{Map}(\mathcal{H}, *)$ of $\mathrm{Mod}(\Sigma, *)$. The handlebody group naturally has a homomorphism to $\mathrm{Aut}(F_g)$ via the action on the fundamental group of $\mathcal{H}$. We define the finite index subgroup

$$\Lambda = \Gamma \cap \mathrm{Map}(\mathcal{H}, *).$$

We will show that the image of Λ under ρ_i block uppertriangularizes, and furthermore that the blocks on the diagonal range over a wide variety of matrices. More precisely, we have the following result. Similar to Section 3, we set $C^* = (\tau(c_{ji}))$ for any matrix $C = (c_{ij}) \in \mathrm{Mat}_m(A_i^{op})$. We define the parabolic subgroup of $\mathcal{G}$

$$\mathcal{P} = \left\{ \begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix} \mid C, E \in \mathrm{Mat}_{g-1}(A_i^{op}) \text{ and } E^*C = C^*E \right\}.$$

Let $pr : \mathcal{P} \to \mathrm{GL}_{g-1}(A_i^{op})$ be the homomorphism

$$\begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix} \mapsto C.$$

Proposition 6.5. *After identifying $\mathrm{Aut}_{A_i}(M_i)$ with $\mathrm{GL}_{2(g-1)}(A_i^{op})$ via the ordered basis $m'_{i,1}, \ldots, m'_{i,g-1}, m''_{i,1}, \ldots, m''_{i,g-1}$ from Lemma 5.5, we have*

$$\rho_i(\Lambda) \subseteq \mathcal{P}.$$

Moreover, if $g \geq 4$, then there is an order $\mathcal{R}_i$ of D_i^{op} such that $pr(\rho_i(\Lambda))$ is a finite index subgroup in $\mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$. If $g = 3$, then $pr(\rho_i(\Lambda))$ is Zariski dense in $\mathrm{SL}_{m_i(g-1)}(\mathcal{R}_i)$.

The first part of the proposition is essentially equivalent to the following lemma.

LEMMA 6.6. *The following is a well-defined commutative diagram.*

$$\begin{array}{ccc} \Lambda & \xrightarrow{\rho} & \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}|\hat{P}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}^t(F_g|S) & \xrightarrow{\eta} & \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{S}) \end{array}$$

Proof. Note that Λ can project to $\mathrm{Aut}^t(F_g|S)$ since $\mathrm{Map}(\mathcal{H},*)$ preserves $\ker(\phi)$ and Γ lies in $\mathrm{Aut}^t(T_g|R)$. In addition to commutativity, we have to establish that $\rho(\Lambda)$ preserves the subspace $\hat{P}$. We translate parts of the diagram into topological language where it becomes the following:

$$\begin{array}{ccc} \mathrm{Map}(\mathcal{H},*)\cap\Gamma & \xrightarrow{\rho} & \mathrm{Aut}_{\mathbb{Q}[H]}(\mathrm{H}_1(\tilde{\Sigma},\mathbb{Q})|\hat{P}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}^t(F_g|S) & \xrightarrow{\eta} & \mathrm{Aut}_{\mathbb{Q}[H]}(\mathrm{H}_1(\tilde{\mathcal{H}},\mathbb{Q})) \end{array} .$$

We prove commutativity in two steps. First, we can lift elements from $\mathrm{Map}(\mathcal{H},*)$ to $\mathrm{Map}(\tilde{\mathcal{H}},\tilde{*})$. and properties of lifts and the fact that $S=\pi_1(\tilde{\mathcal{H}},\tilde{*})$ implies commutativity in the following diagram.

$$\begin{array}{ccc} \mathrm{Map}(\mathcal{H},*)\cap\Gamma & \xrightarrow{\text{lift}} & \mathrm{Map}(\tilde{\mathcal{H}},\tilde{*}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}^t(F_g|S) & \longrightarrow & \mathrm{Aut}(S) \end{array}$$

Since elements of $\mathrm{Map}(\tilde{\mathcal{H}},\tilde{*})$ preserve $\hat{P}$, the following diagram is well-defined and commutative.

$$\begin{array}{ccc} \mathrm{Map}(\tilde{\mathcal{H}},\tilde{*}) & \longrightarrow & \mathrm{Aut}(\mathrm{H}_1(\tilde{\Sigma},\mathbb{Q})|\hat{P}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(S) & \longrightarrow & \mathrm{Aut}(\mathrm{H}_1(\tilde{\mathcal{H}},\mathbb{Q})) \end{array}$$

Putting the diagrams together establishes the Lemma. □

This establishes the block diagonal form claimed in Proposition 6.5. Proving Proposition 6.5 is now a matter of combining some of the above results.

Proof of Proposition 6.5. Let $\gamma\in\Lambda$. Lemma 6.6 implies that $\rho_i(\gamma)$ preserves M_i' and so $\rho_i(\gamma)$ block diagonalizes. To show that $\rho_i(\gamma)$ lies in $\mathcal{P}$ as defined, it suffices to show

that any element of $\mathcal{G}$ preserving M_i' has diagonal entries $(C^*)^{-1}, C$ for some matrix $C \in \mathrm{Mat}_{g-1}(A^{op})$. Notice that relative to the basis, (and multiplying in $\mathrm{Mat}(-^{op})$)

$$\langle (a_1,\dots,a_{2(g-1)}),(b_1,\dots,b_{2(g-1)})\rangle = (\tau(b_1)\dots\tau(b_{2(g-1)}))\begin{pmatrix} 0 & I \\ -I & 0\end{pmatrix}\begin{pmatrix} a_1 \\ \vdots \\ a_{2(g-1)}\end{pmatrix}.$$

Consequently any matrix $\begin{pmatrix} F & E \\ 0 & C\end{pmatrix}$ preserving $\langle -,-\rangle$ must satisfy

$$\begin{pmatrix} F^* & 0 \\ E^* & C^*\end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0\end{pmatrix}\begin{pmatrix} F & E \\ 0 & C\end{pmatrix} = \begin{pmatrix} 0 & I \\ -I & 0\end{pmatrix}.$$

This implies $F = (C^*)^{-1}$, and $C^*E = E^*C$.

Theorem 5.1 implies that Λ surjects onto $\mathrm{Aut}^t(F_g|S)$. Lemma 6.6 implies that $pr \circ \rho_i = \eta_i$, and so Theorem 6.3 and Remark 6.4 finish the proof. □

7 Generating Unipotents in the Image

Our goal in this section is to prove that the image of $\rho_{H,p,i}$ contains the finite index subgroups of the unipotent subgroups $\mathcal{N}^+(\mathfrak{O})$ and $\mathcal{N}^-(\mathfrak{O})$. We begin in this first subsection by finding two concrete examples of unipotents in the image of $\rho_{H,p,i}$. As before, we fix H and p and drop them from the subscripts of ρ and Γ.

7.1 Two unipotent elements. Let a, b be the simple closed curves on Σ as in Lemmas 5.2 and 5.3. The tightly controlled unipotents are the images of the Dehn twists about a and b which we denote by T_a and T_b.

LEMMA 7.1. *Let M_i', M_i'' be the modules and $m_{i,1}', \dots, m_{i,g-1}'$ and $m_{i,1}'', \dots, m_{i,g-1}''$ their respective free A_i-bases given by Lemma 5.5. Then, with respect to the ordered basis $m_{i,1}', \dots, m_{i,g-1}', m_{i,1}'', \dots, m_{i,g-1}''$,*

$$\rho_i(T_b) = \begin{pmatrix} I & e_{1,1} \\ 0 & I\end{pmatrix},$$

$$\rho_i(T_a^{-1}) = \begin{pmatrix} I & 0 \\ e_{1,1} & I\end{pmatrix},$$

where $e_{1,1} \in \mathrm{Mat}_{g-1}(A_i)$ is the matrix with 1 in the upper left corner and 0 in all other entries.

Proof. We prove it for T_a^{-1}; the proof for T_b is similar. Let φ be some representative homeomorphism of T_a which fixes $*$. The lift $\tilde{\varphi}$ is precisely the twist φ on each copy Σ_h' of Σ. I.e., the lift in $\mathrm{Mod}(\tilde{\Sigma}, \tilde{*})$ is simply the composition of twists $\prod_{h\in H} T_{a_h}$. Notice that since all the twists have mutually disjoint support, all the T_{a_h} commute with each other, so the order of composition is irrelevant. It is a standard fact (see

e.g. [FM12, Proposition 6.3]) that the action on homology $T_{\delta *}$ of a single Dehn twist T_δ on a homology class $v \in \mathrm{H}_1(\Sigma, \mathbb{Q})$ is

$$T_{\delta *}(v) = v + \langle v, [\delta] \rangle_{\mathrm{Sp}} [\delta]$$

where $[\delta]$ is the homology class of δ.

We now simply compute our action. Notice that $T_{a_h *}([a_{h'}]) = [a_{h'}]$ for all pairs $h \neq h'$ as $a_h, a_{h'}$ are disjoint, and so we do not "accumulate" any extra terms in composing. I.e. the composition of the $T_{a_h *}$ applied to any $v \in \mathrm{H}_1(\tilde{\Sigma}, \mathbb{Q})$ is

$$\begin{aligned} \textstyle\prod_{h \in H} T_{a_h *}(v) &= v + \textstyle\sum_{h \in H} \langle v, [a_h] \rangle_{\mathrm{Sp}} [a_h] \\ &= v + \textstyle\sum_{h \in H} \langle v, h \cdot [a_1] \rangle_{\mathrm{Sp}} h \cdot [a_1] \\ &= v + \langle v, [a_1] \rangle [a_1]. \end{aligned}$$

By the choice of basis, $\langle v, [a_1] \rangle$ is -1 when $v = b_1$ and is 0 when v is any other basis element. Using the inverse Dehn twist then gives us positive 1. □

7.2 The unipotent subgroups $\mathcal{N}^+$ and $\mathcal{N}^-$. We again fix some simple component $A = A_i$ of $\mathbb{Q}[H]$ and the corresponding submodule $M = M_i$ of $\hat{R}$ with its associated sesquilinear form. Also let $\rho = \rho_i = \rho_{H,p,i}$. Let us now consider the following unipotent subgroups of the corresponding group $\mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle)$ which we continue to view in terms of the basis from Lemma 5.5. Let us set $B = \mathrm{Mat}_{g-1}(A^{op})$, and for $E = (e_{ij}) \in B$, define E^* to be $(\tau(e_{ji}))$. For any matrix of the form $\begin{pmatrix} I & E \\ 0 & I \end{pmatrix}$ in $\mathcal{G}$, a straightforward computation shows that $E^* = E$. We set

$$\mathcal{N}^+ = \left\{ \begin{pmatrix} I & E \\ 0 & I \end{pmatrix} \in \mathrm{Mat}_2(B) \;\middle|\; E^* = E \right\},$$

$$\mathcal{N}^- = \left\{ \begin{pmatrix} I & 0 \\ E & I \end{pmatrix} \in \mathrm{Mat}_2(B) \;\middle|\; E^* = E \right\}.$$

In this section we show that $\rho(\Gamma)$ contains a lattice in each of these unipotent subgroups. We will produce them by conjugating the elements $\rho(T_b)$ and $\rho(T_a^{-1})$ by elements in $\rho(\Lambda)$. Recall from Proposition 6.5 that $\rho(\Lambda)$ consists of elements of the form $\begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix}$ with $E^* C = C^* E$, and note that the inverse of such a matrix is $\begin{pmatrix} C^* & E^* \\ 0 & C^{-1} \end{pmatrix}$. One can compute that

$$\begin{pmatrix} C^* & E^* \\ 0 & C^{-1} \end{pmatrix} \begin{pmatrix} I & E' \\ 0 & I \end{pmatrix} \begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix} = \begin{pmatrix} I & C^* E' C \\ 0 & I \end{pmatrix}.$$

Recall also from Proposition 6.5 that, if $g \geq 4$, for every C in a finite index subgroup of $\mathrm{SL}_{m(g-1)}(\mathcal{R})$, the image $\rho(\Lambda)$ contains a matrix of the form $\begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix}$ (and for $g = 3$, this is true for every C in some Zariski dense subgroup of $\mathrm{SL}_{m(g-1)}(\mathcal{R})$).

Hence, our interest is in the set of matrices C^*EC where $E = E^*$ and $C \in \mathrm{SL}_{m(g-1)}(\mathcal{R})$.

First, we will understand the action of $\mathrm{SL}_1(B) = \{C \in B \mid \mathrm{nrd}_{B/L}(C) = 1\}$ on $N = \{E \in B \mid E^* = E\}$ given by $C \cdot E = C^*EC$. Recall that L is the center of A and hence B, and that K is the field fixed by τ and hence by *.

LEMMA 7.2. *The above action of* $\mathrm{SL}_1(B)$ *on* N *is irreducible over* K.

Proof. Suppose τ (hence *) is of the first kind, and choose some isomorphism $\varphi : B \otimes_K \mathbb{C} \to \mathrm{Mat}_n(\mathbb{C})$ (for appropriate n) so that * goes over to the involution ν in (1) or (2) of Lemma 3.6. Applying φ to $N \otimes_K \mathbb{C}$ identifies $N \otimes_K \mathbb{C}$ with $N' = \{E \in \mathrm{Mat}_n(\mathbb{C}) \mid \nu(E) = E\}$. Let φ' be the composition of $B \to B \otimes_K \mathbb{C}$ followed by φ. Now, $\varphi'(\mathrm{SL}_1(B))$ consists of the K-points of a form of SL_n in $\mathrm{SL}_n(\mathbb{C})$, and so $\varphi'(\mathrm{SL}_1(B))$ is Zariski dense in $\mathrm{SL}_n(\mathbb{C})$ by [BS66, Theorem A] (see also [AB64] or [R57]). Thus, if $\mathrm{SL}_n(\mathbb{C})$ acts irreducibly on N', so does $\varphi'(\mathrm{SL}_1(B))$, and so $\mathrm{SL}_1(B)$ acts irreducibly on N. We will show that for any nonzero $E \in N'$, the $\mathrm{SL}_n(\mathbb{C})$-orbit spans N'. Since scaling E does not affect the span, it is equivalent to prove this for the $\mathrm{GL}_n(\mathbb{C})$-orbit.

In case (1), we have $\nu(C) = C^t$, and N' is the set of symmetric matrices and the action is $C \cdot E = C^tEC$. This action is well-known to be irreducible. In case (2), we have $\nu(C) = JC^tJ^{-1}$. Notice that $J^{-1} = J^t = -J$. The set N' consists of those matrices E such that $JE^tJ^{-1} = E$ which is equivalent to $J^{-1}E$ being skew-symmetric. Then, we have

$$J^{-1}(C \cdot E) = J^{-1}JC^tJ^{-1}EC = C^t(J^{-1}E)C.$$

Consequently, this case reduces to the fact that the action $E \to C^tEC$ on the set of skew-symmetric matrices E is irreducible. The irreducibility of this action is also well-known.

Suppose now that τ is of second kind. We use a proof very similar to the previous cases. By Lemma 3.6, there is an isomorphism $\varphi : B \otimes_K \mathbb{C} \to \mathrm{Mat}_n(\mathbb{C}) \times \mathrm{Mat}_n(\mathbb{C})$ (for appropriate n), so that * goes over to the involution ν defined by $\nu(C, D) = (D^t, C^t)$. Thus, the homomorphism φ identifies $N \otimes_K \mathbb{C}$ with $N' = \{(E, E^t) \in \mathrm{Mat}_n(\mathbb{C}) \times \mathrm{Mat}_n(\mathbb{C})\}$. Let φ' be the composition of $B \to B \otimes_K \mathbb{C}$ followed by φ. By [BS66, Theorem A], the image $\varphi'(\mathrm{SL}_1(B))$ is Zariski dense in $\mathrm{SL}_n(\mathbb{C}) \times \mathrm{SL}_n(\mathbb{C})$. Just as before, $\mathrm{SL}_1(B)$ acts irreducibly on N if $\mathrm{SL}_n(\mathbb{C}) \times \mathrm{SL}_n(\mathbb{C})$ acts irreducibly on N'. In this case, the action on N' is

$$(C, D) \cdot (E, E^t) = (C^t, D^t)(E, E^t)(D, C) = (C^tED, D^tE^tC).$$

It is clearly irreducible. □

We can now show that our image contains a finite index subgroup of $\mathcal{N}^+(\mathfrak{O}) = \mathcal{G}(\mathfrak{O}) \cap \mathcal{N}^+$.

LEMMA 7.3. *The intersection* $\rho(\Lambda) \cap \mathcal{N}^+(\mathfrak{O})$ *is of finite index in* $\mathcal{N}^+(\mathfrak{O})$.

Proof. Let $\mathcal{F} = \rho(\Lambda) \cap \mathcal{G}(\mathfrak{O})$. We show that the subgroup of the (abelian) group $\mathcal{N}^+(\mathfrak{O})$ generated by conjugates of $\begin{pmatrix} I & e_{1,1} \\ 0 & I \end{pmatrix}$ by $\mathcal{F}$ is of finite index in $\mathcal{N}^+(\mathfrak{O})$ (Note that by construction, this unipotent matrix lies in $\rho(\Lambda)$). Using Proposition 6.5, this is equivalent to the subgroup of $N(\mathfrak{O})$ generated by the orbit of $e_{1,1}$ under the action of the finite index subgroup $G = pr(\rho(\Lambda))$ of $\mathrm{SL}_{m(g-1)}(\mathcal{R})$. By Proposition 6.5, the group G is Zariski dense in $\mathrm{SL}_1(B) \cong \mathrm{SL}_{g-1}(A^{op})$. Consequently, since $\mathrm{SL}_1(B)$ acts irreducibly by Lemma 7.2, so does G, and thus the group generated by the G-orbit of $e_{1,1}$ is of finite index in $\mathcal{N}^+(\mathfrak{O})$.

Using this lemma, we can now see that $\rho(\Lambda)$ contains block diagonal matrices. In fact, we can show the following.

LEMMA 7.4. *Assume $g \geq 4$. The image $\rho(\Lambda)$ contains a finite index subgroup of the following group*:

$$\left\{ \begin{pmatrix} (C^*)^{-1} & 0 \\ 0 & C \end{pmatrix} \in \mathrm{Mat}_2(B) \mid C \in \mathrm{SL}_{m(g-1)}(\mathcal{R}) \right\}$$

where $\mathcal{R}$ is the order from Theorem 6.3.

Proof. Let $\mathcal{F} = \rho(\Lambda) \cap \mathcal{G}(\mathfrak{O})$ which necessarily lies in $\mathcal{P}(\mathfrak{O}) = \mathcal{P} \cap \mathcal{G}(\mathfrak{O})$ by Proposition 6.5. Recall that unipotent subgroups have the congruence subgroup property, so, by Lemma 7.3, there is some ideal $\mathfrak{a}$ of $\mathfrak{O}$ such that $\rho(\Lambda) \cap \mathcal{N}^+(\mathfrak{O})$ contains $\mathcal{N}^+(\mathfrak{a})$ (see e.g. page 303 of [R04]). After passing to a finite index subgroup $\mathcal{F}'$ of $\mathcal{F}$, we can ensure that if $\begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix} \in \mathcal{F}'$, then $\begin{pmatrix} I & E \\ 0 & I \end{pmatrix} \in \mathcal{N}^+(\mathfrak{a})$ and therefore $\begin{pmatrix} I & -C^*E \\ 0 & I \end{pmatrix}$ also lies in $\mathcal{N}^+(\mathfrak{a})$. The result then follows from Proposition 6.5 and the computation:

$$\begin{pmatrix} (C^*)^{-1} & E \\ 0 & C \end{pmatrix} \begin{pmatrix} I & -C^*E \\ 0 & I \end{pmatrix} = \begin{pmatrix} (C^*)^{-1} & 0 \\ 0 & C \end{pmatrix}. \qquad \square$$

REMARK 7.5. For $g = 3$, a similar argument using Remark 6.4 instead of Proposition 6.5 will show that $\rho(\Lambda)$ contains a Zariski dense subgroup of

$$\left\{ \begin{pmatrix} (C^*)^{-1} & 0 \\ 0 & C \end{pmatrix} \in \mathrm{Mat}_2(B) \mid C \in \mathrm{SL}_{m(g-1)}(\mathcal{R}) \right\}.$$

The block diagonal matrices act in similar ways on $\mathcal{N}^+(\mathfrak{O})$ and $\mathcal{N}^-(\mathfrak{O})$ by conjugation. Applying the argument of Lemma 7.3 but using the block diagonal matrices from Lemma 7.4 and Remark 7.5 in place of $\rho(\Lambda) \cap \mathcal{G}(\mathfrak{O})$, we obtain the following lemma.

LEMMA 7.6. *The intersection $\rho(\Gamma) \cap \mathcal{N}^-(\mathfrak{O})$ is of finite index in $\mathcal{N}^-(\mathfrak{O})$.*

8 The Image of the Mapping Class Group

We are now ready to finish the proof of our main technical result Theorem 1.6, and then to deduce Theorem 1.8 which outlines the general procedure of obtaining arithmetic quotients of the mapping class group. In the next section, we will apply the procedure to specific examples of H and r to deduce Theorem 1.2, its corollaries, and Theorem 1.3.

8.1 Finishing the proof of Theorem 1.6. First, let $\Gamma = \Gamma_{H,p}$, $\rho = \rho_{H,p}$, $\mathcal{G} = \mathcal{G}_{H,i}$, and $\mathcal{G}^1 = \mathcal{G}^1_{H,i}$. We can now use the results of Lemmas 7.3, 7.4, 7.6 to get the following. Let $\mathcal{G}$ be the algebraic group $\mathrm{Aut}_A(A^{2g-2}, \langle -,- \rangle)$. It is a reductive group but not necessarily semisimple. Let $\mathcal{G}^1$ be the elements of reduced norm 1 over L. This subgroup $\mathcal{G}^1$ is semisimple.

First, let us see why a finite index subgroup of Γ must map into $\mathcal{G}(\mathfrak{O}) = \mathrm{Aut}_{\mathfrak{O}}(\mathfrak{O}^{2g-2}, \langle -,- \rangle)$. Recall that ρ is originally defined by the action of $\Gamma < \mathrm{Aut}(T_g)^+$ on $\overline{R} = R/[R,R]$ which is induced by the action of Γ on $R < T_g$. After tensoring $\overline{R}$ by $\mathbb{Q}$ we obtain $\hat{R} \cong \mathbb{Q}[H]^{2g-2} \oplus \mathbb{Q}^2$ and the action of Γ projects to an action of A^{2g-2} preserving $\langle -,- \rangle$. Since Γ preserves $\overline{R} \subset \hat{R}$, it also preserves $\overline{R} \cap A^{2g-2}$ which is a lattice in the K-vector space A^{2g-2}. Thus, some finite index subgroup of Γ maps into $\mathcal{G}(\mathfrak{O})$.

Recall that $\mathcal{P}$ is the parabolic subgroup of $\mathcal{G}$ which consists of those elements preserving the submodule M' in the notation of Section 5. Let $\mathcal{P}^1 = \mathcal{P} \cap \mathcal{G}^1$. Then $\mathcal{P}^1$ is the normalizer of the unipotent subgroup $\mathcal{N}^+$. The group $\mathcal{P}^1$ is a semi-direct product of its Levi factor $\mathcal{L}$ and its unipotent radical, which is equal to $\mathcal{N}^+$. The Levi factor $\mathcal{L}$ is isomorphic to $\mathrm{GL}_{g-1}(A^{op}) \cong \mathrm{GL}_{(g-1)m}(D^{op})$. Let T be the maximal K-split torus of $\mathcal{L}$ given by diagonal matrices with entries in K; in particular, T is isomorphic to $(K^*)^{m(g-1)}$. Viewing $\mathcal{L}$ as block diagonal matrices, T is also a maximal K-split torus for $\mathcal{G}^1$. I.e. the following is a maximal K-split torus for $\mathcal{G}^1$:

$$\left\{ \begin{pmatrix} (C^*)^{-1} & 0 \\ 0 & C \end{pmatrix} \mid C \in T \right\}$$

(see classification in [T66, Table II]). Let Φ be a K-root system with respect to this torus. Then for every $\alpha \in \Phi$, the corresponding root subgroup lies either in $\mathcal{N}^+, \mathcal{N}^-$, or $\mathcal{L}$.

Now, when $g \geq 4$, Lemmas 7.3, 7.4, 7.6 imply, therefore, that for every $\alpha \in \Phi$, the intersection of $\rho(\Gamma)$ with the root subgroup is commensurable to the integral points of the K-root subgroup. Recall also that unipotent subgroups have an affirmative answer to the congruence subgroup problem [R04], and hence a finite index subgroup of the root subgroup contains a congruence subgroup of it. For $g = 3$, we can still get the same conclusion even though Lemma 7.4 is not valid, as explained in Remark 6.4.

We are now in a position to use Theorem 1.2 of [R92] which asserts that exactly in such a situation the group generated by congruence subgroups of U_α as α ranges over Φ is an arithmetic group, i.e. of finite index in $\mathcal{G}^1(\mathfrak{O})$ (the theorem requires that

the $\mathbb{Q}$-rank of $\mathcal{G}^1$ is at least 2, and this is always true when $g \geq 3$). We thus deduce that $\rho(\Gamma)$ contains a finite index subgroup of $\mathcal{G}^1(\mathfrak{O})$. By Proposition 3.9, $\mathcal{G}^1(\mathfrak{O})$ is of finite index in $\mathcal{G}(\mathfrak{O})$, and so $\rho(\Gamma)$ and $\mathcal{G}^1(\mathfrak{O})$ are commensurable.

8.2 Passing to mapping class groups without fixed point. We have so far only proven results for $\mathrm{Mod}(\Sigma, *)$. We now show how the homomorphism ρ induces a map on $\mathrm{Mod}(\Sigma)$. Let $\epsilon : \mathrm{Mod}(\Sigma, *) \to \mathrm{Mod}(\Sigma)$ be the natural map that forgets the fixed point. The following proposition says that after passing to a finite index subgroup, ρ factors through ϵ.

PROPOSITION 8.1. *Let $p : T_g \to H$ be a ϕ-redundant homomorphism and $\rho_{H,p} : \Gamma_{H,p} \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}, \langle -, - \rangle)$ the corresponding homomorphism. Then, there is a finite index subgroup $\Gamma'_{H,p} < \Gamma_{H,p}$ so that $\rho_{H,p}|_{\Gamma'_{H,p}}$ factors through ϵ.*

Proof. We recall the Birman Exact Sequence for $\mathrm{Mod}(\Sigma, *)$: ([FM12, B74])

$$1 \to T_g \xrightarrow{c} \mathrm{Mod}(\Sigma, *) \xrightarrow{\epsilon} \mathrm{Mod}(\Sigma) \to 1.$$

Here T_g maps to the "point-pushing" mapping classes and each $c(\alpha)$ for $\alpha \in T_g$ acts as conjugation by α on the fundamental group. For ρ to factor through ϵ on some subgroup $\Gamma' < \mathrm{Mod}(\Sigma, *)$, we need $\epsilon(\Gamma' \cap c(T_g))$ to act trivially on $R/[R, R]$. Hence, it suffices that $\Gamma' \cap c(T_g) \subseteq c(R)$.

Let $\alpha \in T_g$ and suppose $c(\alpha) \in \Gamma_{H,p}$. Since R is of finite index, there is some n such that $\alpha^n \in R$, and so $c(\alpha)^n$ acts trivially on $R/[R, R]$ by conjugation. Thus, $\rho(\Gamma_{H,p} \cap c(T_g))$ consists entirely of torsion elements. The image $\rho(\Gamma_{H,p})$ lies in $\mathrm{Aut}(\overline{R}, \langle -, - \rangle_{\mathrm{Sp}})$ which is isomorphic to $\mathrm{Sp}(2 + (2g-2)|H|, \mathbb{Z})$ and contains some finite index torsion-free subgroup G. Thus, $\Gamma'_{H,p} = \rho^{-1}(G) \cap \Gamma_{H,p}$ is the required subgroup. □

8.3 Producing virtual quotients from irreducible representations of finite groups. Theorem 1.6 and Section 8.2 establish Theorem 1.8 which presents a procedure to obtain arithmetic quotients and which we summarize now. This theorem will be convenient for use in Section 9 and possibly the future.

Let Σ_g be a closed surface, let H be some finite group generated by $d(H) < g$ generators, and let A be a simple component of $\mathbb{Q}[H]$. This is the required input for the theorem. By Lemma 3.2, the standard involution τ on $\mathbb{Q}[H]$ defined by $h \mapsto h^{-1}$ restricts to an involution on A which, by abuse of notation, we will also call τ.

Set $M = A^{2g-2}$ with free basis $x_1, \ldots, x_{g-1}, y_1, \ldots y_{g-1}$ and let $\langle -, - \rangle$ be the skew-Hermitian form sesquilinear relative to τ such that $\langle x_i, y_j \rangle = \delta_{ij}, \langle y_i, x_j \rangle = -\delta_{ij}, \langle x_i, x_j \rangle = 0$, and $\langle y_i, y_j \rangle = 0$. Let $\mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle)$, and set $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O}) = \mathcal{G}^1 \cap \mathrm{Aut}_{\mathfrak{O}}(\mathfrak{O}^{2g-2}, \langle -, - \rangle)$ where $\mathfrak{O}$ is the order in A which is the image of $\mathbb{Z}[H]$.

To obtain our representation, we need some ϕ-redundant homomorphism $p : T_g \to H$. Let $\phi : T_g \to F_g$ be the map on fundamental groups induced by the inclusion $\Sigma_g \hookrightarrow \mathcal{H}_g$. Since $d(H) < g$, there is some epimorphism $p' : F_g \to H$ which

maps at least one free generator to the trivial element. The composition $p = p' \circ \phi$ is ϕ-redundant. Recall that R is the kernel of p and $\overline{R} = R/[R,R]$. From the discussion in Section 6, the following subgroup of $\mathrm{Mod}(\Sigma_g, *) \cong \mathrm{Aut}(T_g)^+$

$$\Gamma = \{f \in \mathrm{Aut}(T_g)^+ \mid p \circ f = p\}$$

has a well-defined action on $\overline{R}$, hence on $\hat{R} \cong \mathbb{Q}[H]^{2g-2} \oplus \mathbb{Q}^2$, and hence on A^{2g-2}. This induces a homomorphism $\Gamma \to \mathcal{G}$ by Lemmas 6.1 and 6.2. By Theorem 1.6, there is a finite index subgroup $\Gamma' < \Gamma$ and a homomorphism $\rho : \Gamma' \to \Omega_{H,A}$ with finite index image. By Lemma 8.1, there is a finite index subgroup $\Gamma_{H,A} < \mathrm{Mod}(\Sigma_g)$ and a representation $\rho_{H,A} : \Gamma_{H,A} \to \Omega_{H,A}$ with finite index image. This establishes the theorem.

8.4 Some remarks on the uniqueness of $\rho_{H,r}$. Notice that in the above $\Omega_{H,r} = \Omega_{H,A}$ is uniquely determined by H and r, but the representation $\rho_{H,r} = \rho_{H,A}$ depends on the choice of the surjective representation $p : T_g \to H$. One way to get other epimorphisms p is via the action of the group $\mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$ by $(\psi, \varphi) \cdot p = \varphi \circ p \circ \psi^{-1}$. The corresponding induced representations ρ are "equivalent" in the following sense. Let $\mathrm{inn}(\psi) : \mathrm{Aut}(T_g) \to \mathrm{Aut}(T_g)$ denote the inner automorphism $\mathrm{inn}(\psi)(f) = \psi f \psi^{-1}$. The proof of the following lemma is elementary, so we omit it.

LEMMA 8.2. *Suppose $p_1 : T_g \to H$ is some epimorphism and $p_2 = \varphi p_1 \psi^{-1}$ for some $(\psi, \varphi) \in \mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$. Let $R_i = \ker(p_i)$, let $\hat{R}_i = (R_i/[R_i, R_i]) \otimes_{\mathbb{Z}} \mathbb{Q}$, and let $\rho_{H,p_i} : \Gamma_{H,p_i} \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}_i, \langle -, - \rangle)$ be the corresponding representation as presented in Section 6. Then, there is an isomorphism $\epsilon : \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}_1) \to \mathrm{Aut}_{\mathbb{Q}[H]}(\hat{R}_2)$ such that $\rho_{H,p_2} = \epsilon \circ \rho_{H,p_1} \circ \mathrm{inn}(\psi)$.*

Recall that our maps $T_g \to H$ are ϕ-redundant, so a natural question is: how transitively does $\mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$ act on them? Suppose $p_1, p_2 : T_g \to H$ are respectively ϕ_1-redundant and ϕ_2-redundant, and $p_1', p_2' : F_g \to H$ are the respective induced maps. Recall from the introduction and Section 5 that all maps $\phi : T_g \to F_g$ are induced by some identification $\Sigma \cong \partial\mathcal{H}$. This fact combined with Theorem 5.1 implies that p_1 and p_2 are are in the same $\mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$-orbit if p_1' and p_2' are in the same $\mathrm{Aut}(F_g) \times \mathrm{Aut}(H)$-orbit.

The question then reduces to the transitivity of the $\mathrm{Aut}(F_g) \times \mathrm{Aut}(H)$ action on redundant homomorphisms $F_g \to H$. In [L11, Conjecture 6.3], it was conjectured that this action is transitive. This is known to be true when H is solvable [D70] and when H is simple [G77, E93] (see also [L11, Theorem 6.6]). If the conjecture is true, then our homomorphisms $\rho_{H,r}$ depend only on (H, r) up to the above equivalence.

A more general problem is to understand the $\mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$-orbits of all epimorphisms, $\mathrm{Epi}(T_g, H)$, not just those which are ϕ-redundant. One obstruction to transitivity is $\mathrm{H}_2(H, \mathbb{Z})$. Given an epimorphism $T_g \to H$, there is an induced map $\mathrm{H}_2(T_g, \mathbb{Z}) \to \mathrm{H}_2(H, \mathbb{Z})$ which specifies a well-defined element of $\mathrm{H}_2(H, \mathbb{Z})/\mathrm{Out}(H)$ up to the $\mathrm{Aut}(T_g) \times \mathrm{Aut}(H)$-action. Those epimorphisms $T_g \to H$ factoring through F_g and, in particular, ϕ-redundant homomorphisms induce the ($\mathrm{Out}(H)$-orbit of

the) trivial element in $\mathrm{H}_1(H,\mathbb{Z})/\operatorname{Out}(H)$. Theorem 6.20 of [DT06] shows that for any fixed finite group H and sufficiently large g, the $\operatorname{Aut}(T_g)\times\operatorname{Aut}(H)$-orbits of $\operatorname{Epi}(T_g,H)$ are in bijective correspondence with $\mathrm{H}_2(H,\mathbb{Z})/\operatorname{Out}(H)$. We make the following conjecture.

CONJECTURE. *If H is finite and $g > d(H)$, then the $\operatorname{Aut}(T_g)\times\operatorname{Aut}(H)$-orbits of $\operatorname{Epi}(T_g,H)$ are in one-to-one correspondence with $\mathrm{H}_2(H,\mathbb{Z})/\operatorname{Out}(H)$.*

Note that for any surjective homomorphism $p : T_g \to H$ and irreducible $\mathbb{Q}$-representation r of H, there is an associated representation $\rho_{H,r}$ even if p is not ϕ-redundant. The assumption that p is ϕ-redundant is only necessary for us to establish that the image is arithmetic. If the above conjecture is true, then, up to the natural equivalence, $\rho_{H,r}$ is uniquely determined by the pair (H,r) and an element of $\mathrm{H}_2(H,\mathbb{Z})/\operatorname{Out}(H)$.

8.5 Remarks on property (*T*) and Theorem 1.6 for the case $g = 2$. Another remark which seems to be worth mentioning is that, except for the case $g = 2$, all the virtual arithmetic quotients we obtain for $\operatorname{Mod}(\Sigma_g)$ are lattices in higher-rank semisimple Lie groups (whose simple factors are of $\mathbb{R}$-rank ≥ 2) and hence have Kazhdan's property (T). We do not know if this is the case for the analogous virtual quotient of $\operatorname{Aut}(F_n)$ constructed in [GL09]. There it is possible that the image has an infinite abelian quotient. See [GL09] for a detailed discussion.

8.6 Image of subgroups in the Johnson filtration. As promised in the introduction, we show that the groups in the Johnson filtration are "very different" from the new Torelli groups we define here. Precisely, we prove the following.

PROPOSITION 8.3. *Assume $g \geq 3$. Let H be a nontrivial finite group, r a nontrivial irreducible $\mathbb{Q}$-representation of H, and let $\Gamma = \Gamma_{H,r}$ and $\rho = \rho_{H,r}$ be as in Theorem 1.8. Let $\mathfrak{T} = \mathfrak{T}_{H,r} = \ker(\rho_{H,r})$ and $\mathfrak{I}$ any element in the Johnson filtration of $\operatorname{Mod}(\Sigma)$. Then $\mathfrak{I}\cdot\mathfrak{T}$ is of finite index in $\operatorname{Mod}(\Sigma)$.*

Before proving the proposition, note that this implies $\rho_{H,r}(\mathfrak{I})$ has finite index image in $\Omega_{H,r}$ when H is nontrivial. Thus, our main results imply also that the classical Torelli group and the subgroups in the Johnson filtration have a rich collection of arithmetic quotients.

Proof. First, suppose that $\mathfrak{I}$ is the classical Torelli group, i.e. the kernel of the standard homomorphism $\operatorname{Mod}(\Sigma)\to\operatorname{Sp}(2g,\mathbb{Z})$. Let $\mathfrak{I}' = \mathfrak{I}\cap\Gamma$. Then $\mathfrak{I}'$ and $\mathfrak{T}$ are both normal in Γ. Consider $\mathfrak{I}\cdot\mathfrak{T}/\mathfrak{I}$ which is a normal subgroup of $\Gamma/\mathfrak{I}$, a finite index subgroup of $\operatorname{Sp}(2g,\mathbb{Z})$. By Margulis' normal subgroup theorem [M91, Theorem (4')], it is either finite or of finite index. In the latter case, it follows that $\mathfrak{I}\cdot\mathfrak{T}$ is of finite index in $\operatorname{Mod}(\Sigma)$.

Suppose then that $\mathfrak{I}\cdot\mathfrak{T}/\mathfrak{I}$ is finite. Then $\hat{\mathfrak{T}} = \mathfrak{I}\cap\mathfrak{T}$ is of finite index in $\mathfrak{T}$. Consider now $\hat{\mathfrak{T}}\mathfrak{I}/\hat{\mathfrak{T}}$ in $\Gamma/\hat{\mathfrak{T}}$. The latter group is commensurable to a higher rank lattice, so as above $\hat{\mathfrak{T}}\mathfrak{I}/\hat{\mathfrak{T}}$ is finite or of finite index. If the latter holds, we are done. If the former

holds, then $\mathfrak{I} \cap \hat{\mathfrak{T}}$ is of finite index in $\mathfrak{I}$, and so $\mathfrak{T}$ and $\mathfrak{I}$ are commensurable, but that is impossible.

Now, let $\mathfrak{I}$ be any group in the Johnson filtration and let $\mathfrak{I}_0$ be the classical Torelli group. Let $\mathfrak{I}_0' = \Gamma \cap \mathfrak{I}_0$ and $\mathfrak{I}' = \Gamma \cap \mathfrak{I}$. The quotient $\mathfrak{I}_0/\mathfrak{I}$ is nilpotent, and thus $\mathfrak{I}_0'/\mathfrak{I}'$ is nilpotent. Let $\Pi : \Gamma \to \Gamma/\mathfrak{T}$ be the quotient map. The above two paragraphs show that $\Pi(\mathfrak{I}_0')$ is of finite index in $\Gamma/\mathfrak{T}$. Thus, $\Pi(\mathfrak{I}_0')/\Pi(\mathfrak{I}')$ is a nilpotent quotient of a higher rank lattice and hence finite. This implies that $\mathfrak{I} \cdot \mathfrak{T}$ is of finite index in $\mathrm{Mod}(\Sigma)$. □

9 Finite Groups and Arithmetic Quotients

As explained in the introduction, our main result gives us a way to associate a virtual epimorphism ρ from $\mathrm{Mod}(\Sigma)$ to an arithmetic group Ω from the choice of a finite group H and irreducible $\mathbb{Q}$-representation r or, equivalently, a simple component A of $\mathbb{Q}[H]$. In this section, we present various kinds of arithmetic groups which arise as we vary H and r.

In the first section, we prove Corollary 1.4. While this is formally a corollary of Theorem 1.2 as stated, our actual proof must proceed by deducing the corollary directly. Then, for genus 2, the various examples in Theorem 1.2 actually follow from the "corollary". Note, then, that for genus 2, we do *not* obtain these virtual arithmetic quotients of $\mathrm{Mod}(\Sigma_2)$ by various representations $\rho_{H,p}$. In the next few sections, we prove Theorem 1.2 by listing the finite groups H and irreducible representations r, establishing the requisite properties and determining the arithmetic group $\Omega_{H,A}$ with the use of results in Section 4 when necessary. We then prove Corollary 1.5 using example (a) of Theorem 1.2. In the final section, we discuss more generally the question of what simple $\mathbb{Q}$-algebras with involution can arise as factors of $\mathbb{Q}[H]$ and deduce Theorem 1.3.

9.1 Proof of Corollary 1.4 and Theorem 1.2 for $g = 2$. We set $H = \mathbb{Z}/2\mathbb{Z}$ and we let $p : T_2 \to \mathbb{Z}/2\mathbb{Z}$ be some surjective ϕ-redundant map. Here, $\mathbb{Q}[H] \cong \mathbb{Q} \oplus A$ where $A \cong \mathbb{Q}$ as a $\mathbb{Q}$-algebra and where as a $\mathbb{Q}[H]$ module, the nontrivial element of H acts on A by multiplication by -1. Note that the standard involution τ on $\mathbb{Q}[H]$ is trivial, and hence its restriction to A is trivial. Thus, $\mathrm{Aut}(A^{2g-2}, \langle -, - \rangle) = \mathrm{Sp}(2, \mathbb{Q}) = \mathrm{SL}(2, \mathbb{Q})$. From Lemma 7.1, it follows directly that $\rho(\Gamma)$ contains the generating elements

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Moreover, as $\rho(\Gamma_{H,p})$ preserves $\overline{R} \subseteq \hat{R}$, there is some finite index subgroup of $\Gamma_{H,p}$ whose image is $\mathrm{Sp}(2, \mathbb{Z})$.

Because of the corollary, $\mathrm{Mod}(\Sigma_2)$ virtually surjects onto a finitely generated free group, and thus onto all free groups of finite rank. Since all the arithmetic groups in Theorem 1.2 are finitely generated, $\mathrm{Mod}(\Sigma_2)$ virtually surjects onto them.

9.2 The symmetric and alternating groups. In this section, we describe an irreducible representation for the symmetric group and alternating group. Let $\mathrm{Sym}(m+1)$ denote the symmetric group on $m+1$ letters and $\mathrm{Alt}(m+1)$ the alternating group on $m+1$ letters. The symmetric group has an irreducible representation (sometimes called the standard representation) defined as follows. There is an obvious action of $\mathrm{Sym}(m+1)$ on $\mathbb{Q}^{m+1}$ acting by the permutation matrices. The vector $w = (1, 1, \ldots, 1)$ is a fixed vector, but $\mathrm{Sym}(m+1)$ acts irreducibly on the orthogonal complement $V = w^{\perp}$. The representation $r : \mathrm{Sym}(m+1) \to \mathrm{GL}(V)$ is irreducible and moreover, the induced homomorphism $\tilde{r} : \mathbb{Q}[\mathrm{Sym}(m+1)] \to \mathrm{End}_{\mathbb{Q}}(V)$ is surjective, and so the corresponding simple factor in $\mathbb{Q}[\mathrm{Sym}(m+1)]$ is $A \cong \mathrm{Mat}_m(\mathbb{Q})$. Since the center is $L = \mathbb{Q}$, the fixed field K under τ is $K = L = \mathbb{Q}$. Since $A \otimes_K \mathbb{R} = A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{Mat}_m(\mathbb{R})$, by Proposition 4.3, τ is of first kind and orthogonal type.

For $m \geq 3$, the restriction $r : \mathrm{Alt}(m+1) \to \mathrm{GL}(V)$ is irreducible, so $A = \mathrm{Mat}_m(\mathbb{Q})$ is a simple component of $\mathbb{Q}[\mathrm{Alt}(m+1)]$ also. For the same reasons as above, the induced involution τ on A is of first kind and orthogonal type. For all $m \geq 2$, a 3-cycle γ and m-cycle δ for m odd (resp. $m+1$-cycle δ for m even) generate $\mathrm{Alt}(m+1)$; moreover, we can choose δ, γ such that $\mathrm{Alt}(m+1)$ is generated by all elements of the form $\delta^k \gamma \delta^{-k}$.

9.3 Example (a) of Theorem 1.2. In this section, we establish example (a) of Theorem 1.2 for genus $g \geq 3$. Here and in the following three sections, we use our main result, Theorem 1.8, and so here, and in the following sections, we generally present the following:

- the finite group H and a demonstration that $d(H) \leq 2 < g$,
- an irreducible representation r of H and/or the corresponding simple factor A of $\mathbb{Q}[H]$,
- an identification of a finite index subgroup of the arithmetic group $\Omega_{H,A}$.

For example (a), let $H = \mathrm{Sym}(m+1)$. It is well-known that $\mathrm{Sym}(m+1)$ is generated by two elements. We take r to be the standard representation, so the corresponding simple factor A is $\mathrm{Mat}_m(\mathbb{Q})$ as explained in Section 9.2.

We now describe $\Omega_{H,A}$. Let $\mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle)$, and let σ be the involution of $\mathrm{End}_A(A^{2g-2})$ associated to $\langle -, - \rangle$. Since τ is of orthogonal type, the involution σ associated to $\langle -, - \rangle$ is of symplectic type by Lemma 3.5. The endomorphism ring $\mathrm{End}_A(A^{2g-2})$ is isomorphic to $\mathrm{Mat}_{2(g-1)}(A^{op}) \cong \mathrm{Mat}_{2m(g-1)}(\mathbb{Q})$. Over fields K of characteristic 0, all symplectic involutions of $\mathrm{Mat}_{2(g-1)}(K)$ are equivalent, and so there is an isomorphism $\varphi : \mathrm{End}_A(A^{2g-2}) \to \mathrm{Mat}_{2m(g-1)}(\mathbb{Q})$ sending σ to the standard symplectic involution. The intersection of $\varphi(\mathcal{G}^1(\mathfrak{O}))$ and $\mathrm{Sp}(2m(g-1), \mathbb{Z})$ is of finite index in the latter. By Theorem 1.8, there is a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O})$ which, up to finite index, is isomorphic to $\mathrm{Sp}(2m(g-1), \mathbb{Z})$. This establishes example (a) in Theorem 1.2.

9.4 Example (b) of Theorem 1.2. The required finite group will be $H = \mathrm{Dih}(2n)$ for $m = 1$ and $H = \mathrm{Alt}(m+1) \times \mathrm{Dih}(2n)$ for $m \geq 3$ where $\mathrm{Dih}(2n)$ is the dihedral group of order $2n$ which has presentation

$$\mathrm{Dih}(2n) = \langle x, y \mid x^n = 1,\ y^2 = 1,\ yxy^{-1} = x^{-1} \rangle.$$

For $m = 2$, we require a group containing $\mathrm{Dih}(2n)$ which we will describe below (We remark that for $g \geq 4$, one can use $H = \mathrm{Sym}(m+1) \times \mathrm{Dih}(2n)$ for all m; however this choice is not suitable for $g = 3$ as the group is not generated by two elements for n even).

We first establish (b) in the case of $m \geq 3$. The group H is generated by (γ, y) and (δ, x) for the following reasons. Both $(\gamma, 1)$ and $(1, y)$ are powers of (γ, y). By conjugating $(\gamma, 1)$ by powers of (δ, x), we obtain all elements of the form $(\delta^k \gamma \delta^{-k}, 1)$. From this, we generate $\mathrm{Alt}(m+1) \times 1$, and then clearly (γ, y) and (δ, x) generate H.

We next describe an irreducible representation of $\mathrm{Dih}(2n)$. Let ζ be a primitive nth root of unity, and let $\alpha \to \overline{\alpha}$ denote the order 2 automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta \mapsto \zeta^{-1}$. Set

$$B = \left\{ \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{Q}(\zeta) \right\}.$$

The group ring $\mathbb{Q}[H]$ surjects onto the $\mathbb{Q}$-algebra B via the homomorphism $\tilde{s}$ defined by

$$\tilde{s}(x) = \begin{pmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{pmatrix} \quad \tilde{s}(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The center L of B is equal to the subfield of $\mathbb{Q}(\zeta)$ invariant under $^-$, i.e. $L = \mathbb{Q}(\zeta)^+$. Recall that the induced involution, call it ν, on B is the unique involution satisfying $\nu(\tilde{s}(z)) = \tilde{s}(z)^{-1}$ for all $z \in \mathrm{Dih}(2n)$. It follows that the involution is the one given by conjugate transpose of the matrix, and so ν is of first kind. Moreover, $\dim_L(B) = 4$ and the ν-fixed vector subspace is 3-dimensional, so ν is of orthogonal type.

We can describe B further. Recall that B is a matrix ring over a division algebra with center L. Notice, however, that B is not a division algebra, and since it has dimension 4 over L, it follows that $B \cong \mathrm{Mat}_2(L)$.

We now describe the simple factor A of $\mathbb{Q}[H]$ and the involution τ. Let $\tilde{s}' : \mathbb{Q}[\mathrm{Alt}(m+1)] \to \mathrm{Mat}_m(\mathbb{Q})$ be the standard representation from Section 9.2, and let ν' be the involution of $\mathrm{Mat}_m(\mathbb{Q})$ induced by the standard involution of $\mathbb{Q}[\mathrm{Alt}(m+1)]$. Set $A = \mathrm{Mat}_m(\mathbb{Q}) \otimes_{\mathbb{Q}} B$. There is a surjective homomorphism $\tilde{r} : \mathbb{Q}[H] \to A$ defined by $\tilde{r}(z, w) = \tilde{s}'(z) \otimes \tilde{s}(w)$ on $(z, w) \in H = \mathrm{Alt}(m+1) \times \mathrm{Dih}(2n)$. The involution τ of A induced by the standard involution of $\mathbb{Q}[H]$ satisfies

$$\tau(x \otimes b) = \nu'(x) \otimes \nu(b).$$

It is straightforward to check that τ is of first kind. Let V^+, V^- (resp. W^+, W^-) be the $+1$- and -1-eigenspace of ν' (resp. ν). Then, the $+1$-eigenspace of τ is $V^+ \otimes$

$W^+ + V^- \otimes W^-$, and, after counting dimension, one finds that this eigenspace is more than half the dimension of A. Consequently, τ is of orthogonal type.

In total, there is a surjective homomorphism $s : \mathbb{Q}[H] \to A \cong \mathrm{Mat}_m(B) \cong \mathrm{Mat}_{2m}(L)$ with induced orthogonal involution on $\mathrm{Mat}_{2m}(L)$. Arguing as in the Section 9.2, we find that, up to finite index, $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O})$ is isomorphic to $\mathrm{Sp}(2 \cdot (2m)(g-1), \mathcal{O}) = \mathrm{Sp}(4m(g-1), \mathcal{O})$. Thus, there is a virtual epimorphism $\mathrm{Mod}(\Sigma_g)$ onto $\mathrm{Sp}(4m(g-1), \mathcal{O})$.

For $m = 1$, the simple factor of $\mathbb{Q}[H]$ is $A = B$, and clearly $d(H) = 2$. The analysis above applies mutatis mutandis to establish that $\mathcal{G}^1(\mathfrak{O})$, up to finite index, is $\mathrm{Sp}(4(g-1), \mathcal{O})$ and there is a virtual epimorphism $\mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}(4(g-1), \mathcal{O})$.

Now suppose $m = 2$. We construct H as a subgroup of the units in $\mathrm{Mat}_2(B)$. Namely, let $X = \tilde{s}(x) \in B$ and $Y = \tilde{s}(y) \in B$, and set

$$H = \left\{ \begin{pmatrix} X^{2k}Z & 0 \\ 0 & Z \end{pmatrix}, \begin{pmatrix} 0 & X^{2k+1}Z \\ Z & 0 \end{pmatrix} \in \mathrm{Mat}_2(B) \mid Z \in s(\mathrm{Dih}(2n)), k \in \mathbb{Z} \right\}.$$

This is a group which is finite and generated by the following two elements

$$\begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} \quad \begin{pmatrix} 0 & X \\ I & 0 \end{pmatrix}.$$

The inclusion $H \to \mathrm{Mat}_2(B)$ induces a homomorphism $\mathbb{Q}[H] \to \mathrm{Mat}_2(B) \stackrel{\mathrm{def}}{=} A$ which is surjective. The induced involution τ satisfies $\tau((b_{ij})) = (\nu(b_{ji}))$. Using arguments similar to the above, we find that $\mathcal{G}^1(\mathfrak{O})$ is, up to finite index, $\mathrm{Sp}(8(g-1), \mathcal{O})$ and there is a virtual epimorphism $\mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}(8(g-1), \mathcal{O})$.

9.5 Example (c) of Theorem 1.2. Here, we use the finite group $H = \mathrm{Sym}(m+1) \times \mathrm{Cyc}(n)$ for $m \geq 2$ and $H = \mathrm{Cyc}(n)$ for $m = 1$ where $\mathrm{Cyc}(n) = \mathbb{Z}/n\mathbb{Z}$. We first describe an irreducible representation of $\mathrm{Cyc}(n)$. Namely, there is an irreducible representation $\mathrm{Cyc}(n) \to \mathbb{Q}(\zeta)^\times$ sending the generator of $\mathrm{Cyc}(n)$ to ζ, a primitive nth root of unity. The corresponding map $\mathbb{Q}[\mathrm{Cyc}(n)] \to \mathbb{Q}(\zeta)$ is surjective. The induced involution, ν on $L = \mathbb{Q}(\zeta)$ is the unique one sending ζ to ζ^{-1} which is an involution of the second kind with fixed field $K = \mathbb{Q}(\zeta)^+$.

Suppose now that $m \geq 2$. The group $\mathrm{Sym}(m+1) \times \mathrm{Cyc}(n)$ has generators $(\gamma, 0)$ and $(\delta, 1)$ where γ is a transposition and δ is an $m+1$-cycle. The conjugates of $(\gamma, 0)$ by $(\delta, 1)$ generate $\mathrm{Sym}(m+1) \times 0$, and from there it is obvious that H is generated by both elements.

Via an argument similar to the one used in Section 9.4, we have a surjective homomorphism $\mathbb{Q}[H] \to \mathrm{Mat}_m(\mathbb{Q}) \otimes \mathbb{Q}(\zeta) \cong \mathrm{Mat}_m(\mathbb{Q}(\zeta)) = A$. Since the center is $L = \mathbb{Q}(\zeta)$, the induced involution on A is of second kind by Proposition 4.3. The τ-fixed subfield K is $\mathbb{Q}(\zeta)^+$.

It only remains to describe $\Omega_{H,A}$. From the description of $\langle -, - \rangle$, it is clear that a matrix E is the adjoint of $C \in \mathrm{Mat}_{2g-2}(A^{op})$ if and only if

$$E^* \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} C$$

where E^* is the map defined by $(e_{ij})^* = (\tau(e_{ji}))$. Thus, the adjoint involution for $\langle -, - \rangle$ is

$$\sigma(C) = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}^{-1} C^* \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Since $\mathrm{Mat}_{2g-2}(A^{op}) \cong \mathrm{Mat}_{2m(g-1)}(\mathbb{Q}(\zeta))$, the involution σ is also the adjoint involution for a nondegenerate $\mathbb{Q}(\zeta)$-valued Hermitian form $\langle -, - \rangle_0$ on $\mathbb{Q}(\zeta)^{2m(g-1)}$ ([K98, Theorem 4.2]). From the fact that $\langle -, - \rangle$ has a maximal isotropic submodule, one can deduce that $\langle -, - \rangle_0$ has a maximal isotropic subspace (i.e. of $\mathbb{Q}(\zeta)$-dimension $m(g-1)$) as well. All Hermitian forms on $\mathbb{Q}(\zeta)^{2m(g-1)}$ with a maximal isotropic subspace are equivalent (e.g. one can apply the same arguments as in Lemma 5.5), and so the form $\langle -, - \rangle_0$ is equivalent to the form defining $U(m(g-1), m(g-1), \mathbb{Q}(\zeta))$.

Thus, there is an isomorphism from a finite index subgroup of $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O})$ to a finite index subgroup of $\mathrm{SU}(m(g-1), m(g-1), \mathcal{O})$ where $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\zeta)$. By Theorem 1.8, there is a virtual epimorphism from $\mathrm{Mod}(\Sigma_g)$ onto $\mathrm{SU}(m(g-1), m(g-1), \mathcal{O})$.

For the case $m = 1$, a simplified version of the above argument applies, and so there is a virtual epimorphism $\mathrm{Mod}(\Sigma_g)$ onto $\mathrm{SU}((g-1), (g-1), \mathcal{O})$.

9.6 Example (d) of Theorem 1.2. For these examples, we use the finite group $H = \mathrm{Alt}(m+1) \times \mathrm{Dic}(4n)$ for $m \geq 3$ and $\mathrm{Dic}(4n)$ for $m = 1$ where $\mathrm{Dic}(4n)$ is the dicyclic group of order $4n$. The group $\mathrm{Dic}(4n)$ has the following presentation:

$$\mathrm{Dic}(4n) = \langle x, y \mid x^{2n} = 1, y^2 = x^n, y^{-1}xy = x^{-1} \rangle.$$

For $m = 2$, we use a group containing $\mathrm{Dic}(4n)$ which we will describe below and which has a construction similar to that for example (b).

We begin with the case $m \geq 3$. The group $H = \mathrm{Alt}(m+1) \times \mathrm{Dic}(4n)$ is generated by the two elements (γ, y) and (δ, x). This follows verbatim from the same argument for $\mathrm{Alt}(m+1) \times \mathrm{Dih}(2n)$.

The group ring $\mathbb{Q}[\mathrm{Dic}(4n)]$ has a representation onto a division algebra D defined as follows. Let ζ be the primitive $2n$th root of unity, and let $^-$ denote the unique order 2 automorphism of $\mathbb{Q}(\zeta)$ sending $\zeta \mapsto \zeta^{-1}$. The division algebra is

$$D = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Q}(\zeta)) \mid \alpha, \beta \in \mathbb{Q}(\zeta) \right\}.$$

The center L of D is $\mathbb{Q}(\zeta)^+$, and the epimorphism $\tilde{s} : \mathbb{Q}[\mathrm{Dic}(4n)] \to D$ is defined on the generators by

$$\tilde{s}(x) = \begin{pmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{pmatrix} \quad \tilde{s}(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The induced involution, call it ν, on D is that involution satisfying $\nu(\tilde{s}(z)) = \tilde{s}(z)^{-1}$ for all $z \in \mathrm{Dic}(4n)$. Thus, in terms of the matrices, ν is conjugate transpose, and

it is of first kind (on D). The fixed subspace of ν has L-dimension 1 and D has L-dimension 4, so ν is of symplectic type.

We describe the simple factor A of $\mathbb{Q}[H]$. Let $\tilde{s}' : \mathbb{Q}[\mathrm{Alt}(m+1)] \to \mathrm{Mat}_m(\mathbb{Q})$ be the homomorphism from Section 9.2, and let ν' be the involution of $\mathrm{Mat}_m(\mathbb{Q})$ induced by the standard involution of $\mathbb{Q}[\mathrm{Alt}(m+1)]$. Let $A = \mathrm{Mat}_m(\mathbb{Q}) \otimes_{\mathbb{Q}} D \cong \mathrm{Mat}_m(D)$. There is a surjective homomorphism $\tilde{r} : \mathbb{Q}[H] \to A$ defined by $\tilde{r}(z,w) = \tilde{s}'(z) \otimes \tilde{s}(w)$ on $(z,w) \in H$. The induced involution, τ, on A is equal to $\nu' \otimes \nu$. By an argument similar to the one in Section 9.4, one can show τ is of first kind and symplectic type. By Theorem 1.7, $\mathcal{G} = \mathrm{Aut}_A(A^{2g-2}, \langle -, - \rangle)$ is the L-points ($K = L$ here) of an L-defined algebraic group whose real form is $\mathrm{SO}(2m(g-1), 2m(g-1), \mathbb{R})$. Thus, there is a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto $\Omega_{H,A} = \mathcal{G}^1(\mathfrak{O})$, an arithmetic subgroup of $\mathrm{SO}(2m(g-1), 2m(g-1), \mathbb{R})$.

For $m = 1$, it is clear that $H = \mathrm{Dih}(2n)$ is generated by two elements, and the above arguments apply mutatis mutandis to show that there is a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto an arithmetic subgroup of $\mathrm{SO}(2(g-1), 2(g-1), \mathbb{R})$.

For $m = 2$, we construct H as a subgroup of the units of $\mathrm{Mat}_2(D)$. Namely, let $X = s(x) \in D$ and $Y = s(y) \in D$, and set

$$H = \left\{ \begin{pmatrix} X^{2k} Z & 0 \\ 0 & Z \end{pmatrix}, \begin{pmatrix} 0 & X^{2k+1} Z \\ Z & 0 \end{pmatrix} \in \mathrm{Mat}_2(D) \mid Z \in s(\mathrm{Dic}(4n)), k \in \mathbb{Z} \right\}.$$

Like the group H for $m = 2$ in Section 9.4, H here is generated by two elements, and the inclusion $H \to \mathrm{Mat}_2(D)$ induces a homomorphism $\mathbb{Q}[H] \to \mathrm{Mat}_2(D) \stackrel{\mathrm{def}}{=} A$ which is surjective. The induced involution τ satisfies $\tau((b_{ij})) = (\nu(b_{ji}))$, and so τ is of symplectic type. Using arguments similar to the above, we find a virtual epimorphism onto an arithmetic subgroup of $\mathrm{SO}(4(g-1), 4(g-1), \mathbb{R})$.

9.7 Proof of Corollary 1.5. This follows rather quickly from example (a) of Theorem 1.2. A finite index subgroup of $\mathrm{Sp}(2m(g-1), \mathbb{Z})$ is mapped onto $\mathrm{Sp}(2m(g-1), \mathbb{Z}/p\mathbb{Z})$ for almost all primes p. The latter contains $\mathrm{SL}(m(g-1), \mathbb{Z}/p\mathbb{Z})$ and hence contains $\mathrm{Sym}(m(g-1)-1)$. Now, every finite group G embeds in $\mathrm{Sym}(m(g-1)-1)$ for sufficiently large m. Thus, $\mathrm{Mod}(\Sigma_g)$ has a finite index subgroup which is mapped onto G.

9.8 Simple components of $\mathbb{Q}[H]$ in general. From Theorem 1.8, given a finite group H with $d(H) < g$ and a simple factor A of $\mathbb{Q}[H]$, there is a corresponding arithmetic group $\Omega_{H,A}$ which is a virtual quotient of $\mathrm{Mod}(\Sigma_g)$. It is therefore of interest to understand what kinds of algebras with involution (A, τ) are obtained in this way. This seems to be an open problem in general.

We start with some basic properties of the pairs (A, τ). Recall that A is isomorphic to $\mathrm{Mat}_m(D)$ for some integer m and some division algebra D with a number field L as center. Recall from Lemma 4.2 that L must be a subfield of a cyclotomic field. This is equivalent to L being an abelian extension of $\mathbb{Q}$. Recall, moreover, from Proposition 4.3 that L is totally real if and only if τ is of first kind and L is totally imaginary if and only if τ is of second kind.

We will not say much about the involution τ. However, in the case where τ is of first kind, the division algebra D is considerably restricted. The following proposition is essentially the Brauer–Speiser Theorem, and the proof we give is basically that given by Fields in [F71]. Recall that the degree d of a division algebra D is the integer satisfying $d^2 = \dim_L(D)$ where L is the center of D.

PROPOSITION 9.1. *If $A = \mathrm{Mat}_m(D)$ has an involution of the first kind, then the degree of D is at most 2, i.e. D is the field L or a quaternion algebra over L.*

Proof. If τ is an involution of the first kind, then τ is an isomorphism $A \cong A^{op}$ as L-algebras. Thus $A \otimes_L A \cong A \otimes_L A^{op} \cong \mathrm{Mat}_n(L)$ where $n = \dim_L(A)$ [FD93, Proposition 3.12]. Thus, the class defined by A in the Brauer group of L has order 1 or 2 (see below for the definition of the Brauer group and [FD93] for more details). For number fields L, the exponent of $\mathrm{Mat}_m(D)$ in the Brauer group of L is equal to the degree of D [R75, Theorem 32.19]. □

Let us consider, now, the simpler question of which algebras A appear as simple components of $\mathbb{Q}[H]$ or what division algebras D appear in such an $A \cong \mathrm{Mat}_m(D)$ regardless of m. Notice that, by using $\mathrm{Sym}(\ell+1)$ and its standard representation, given any algebra $A = \mathrm{Mat}_m(D)$ which is a simple part of $\mathbb{Q}[H]$, we can also obtain $\mathrm{Mat}_{\ell m}(D)$ as a simple part of $\mathbb{Q}[H \times \mathrm{Sym}(\ell+1)]$. One can show that this increases the requisite number of generators of the finite group by at most 1 except when H is trivial. For $D = L$ a field, the algebra $\mathrm{Mat}_m(D)$ is a simple component of $\mathbb{Q}[H]$ for some H precisely when L is a subfield of a cyclotomic field (see e.g. [M78, Theorem 3.2]). This leads to the proof of Theorem 1.3.

Proof of Theorem 1.3. We use Theorem 1.8 and follow a similar program as for Theorem 1.2. From the above discussion, it follows that for some $s_L \in \mathbb{N}$, there is a finite group H such that $\mathrm{Mat}_{s_L}(L)$ is a simple component of $\mathbb{Q}[H]$. Consequently, using arguments similar to those for Theorem 1.2, $\mathrm{Mat}_{ms_L}(L)$ is a simple part of $\mathbb{Q}[H \times \mathrm{Sym}(m+1)]$. Let $N = d(H \times \mathrm{Sym}(m+1)) + 1$.

Suppose L is a totally real field. By Proposition 4.3, τ is of first kind and $K = L$. By the same proposition, since $\mathrm{Mat}_{ms_L}(L) \otimes_K \mathbb{R} = \mathrm{Mat}_{ms_L}(K) \otimes_K \mathbb{R} = \mathrm{Mat}_{ms_L}(\mathbb{R})$, the involution τ is of orthogonal type. Arguing as for example (b) of Theorem 1.2, we find a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto $\mathrm{Sp}(2ms_L(g-1), \mathcal{O})$ where $\mathcal{O}$ is the ring of integers in L.

Suppose L is a totally imaginary field. By Proposition 4.3, τ is of second kind. Arguing as for example (c) of Theorem 1.2, we find a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto $\mathrm{SU}(ms_L(g-1), ms_L(g-1), \mathcal{O})$ where $\mathcal{O}$ is the ring of integers in L. □

If we ask only what division algebras D appear regardless of m, then we can appeal to results on the Schur subgroup, $S(L)$, of the Brauer group, $B(L)$, for a finite abelian extension L of $\mathbb{Q}$. The elements of the Brauer group are equivalence classes of central simple L-algebras where A_1 and A_2 are equivalent if they are isomorphic, respectively, to $\mathrm{Mat}_{m_1}(D)$ and $\mathrm{Mat}_{m_2}(D)$ for some division algebra D.

The group operation is $\otimes_L$. The Schur group consists of those classes $[A]$ where A is a simple component of some $L[H]$. In the case where L is a finite abelian extension of $\mathbb{Q}$, the Schur subgroup is also the set of those classes $[A]$ where A is a simple component of some $\mathbb{Q}[H]$ (This seems to be well-known among experts, but is also a consequence of the stronger [M78, Theorem 3.2]).

We mention some of the easier-to-state theorems in the literature. One basic question that can be answered is what possible degree d of a division algebra D is possible. I.e. for what d is $\dim_L(D) = d^2$ for some division algebra D in the Schur group of L? It follows from [BS72] that, for L containing a primitive dth root of unity, there are infinitely many elements $[D]$ in $S(L)$ where D has degree d. In particular, in combination with our theorems, this implies that for each of these infinitely many division algebras D, some m and sufficiently large g (depending on D), there is a virtual epimorphism of $\mathrm{Mod}(\Sigma_g)$ onto the arithmetic group $\mathcal{G}^1(\mathfrak{O})$, i.e. the elements of reduced norm 1 in $\mathrm{Aut}_{\mathfrak{O}}(\mathfrak{O}^{2g-2}, \langle -, - \rangle)$ where $\mathfrak{O}$ is an order in $\mathrm{Mat}_m(D)$.

In the opposite direction, a result due to Schacher and Fein (independently) tells us that infinitely many division algebras D are unattainable regardless of m [S72]. In the special case of $L = \mathbb{Q}$, it has been shown that $S(\mathbb{Q})$ and $B(\mathbb{Q})$ are equal when restricting to classes $[D]$ where the degree of D is 2 [B71, F71]. Some other papers characterize $S(L)$ for certain subclasses of fields in cyclotomic fields (e.g.[BS72, J75]). We refrain from going into further detail and refer the interested reader to the literature.

Acknowledgments

The authors acknowledge useful discussions with Ursula Hamenstädt and Sebastian Hensel on the handlebody groups and with V. Venkataramana on generators of arithmetic groups. We are also grateful to Andrei Rapinchuk, Eli Eljadeff, and Uriah First for various discussions on algebras and arithmetic groups. The work of the 3rd and 4th authors is supported by the ERC, and the work of the 2nd and 3rd authors by the NSF and BSF.

References

[AB64] M. Artin, J.E. Bertin, M. Demazure, P. Gabriel, A. Grothendieck, M. Raynaud and J.-P. Serre. *Schémas en groupes. Fasc. 4: Exposés 12 à 14*, volume 1963/64 of *Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques*. Institut des Hautes Études Scientifiques, Paris (1964).

[B71] M. Benard. Quaternion constituents of group algebras. *Proc. Amer. Math. Soc.*, 30 (1971), 217–219. ISSN 0002-9939.

[BS72] M. Benard and M.M. Schacher. The Schur subgroup. II. *J. Algebra*, 22(1972), 378–385. ISSN 0021-8693.

[B74] J.S. Birman. *Braids, links, and mapping class groups*. Princeton University Press, Princeton, N.J. (1974). Annals of Mathematics Studies, No. 82.

[BS66] A. Borel and T.A. Springer. Rationality properties of linear algebraic groups. In: *Algebraic Groups and Discontinuous Subgroups* (*Proc. Sympos. Pure Math., Boulder, Colo., 1965*). Amer. Math. Soc., Providence, R.I. (1966), pp. 26–32.

[B89] H. Burkhardt. Grundzüge einer allgemeinen Systematik der hyperelliptischen Functionen I. Ordnung. *Math. Ann.*, (1–2)35 (1889), 198–296. ISSN 0025-5831. doi:10.1007/BF01443877.

[CW34] C. Chevalley and A. Weil. Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abh. Math. Sem. Univ. Hamburg*, 10 (1934), 358–361

[DT06] N.M. Dunfield and W.P. Thurston. Finite covers of random 3-manifolds. *Invent. Math.*, (3)166 (2006), 457–521. ISSN 0020-9910. doi:10.1007/s00222-006-0001-6.

[D70] M.J. Dunwoody. Nielsen transformations. In: *Computational Problems in Abstract Algebra* (*Proc. Conf., Oxford, 1967*). Pergamon, Oxford (1970), pp. 45–46.

[E93] M.J. Evans. T-systems of certain finite simple groups. *Math. Proc. Cambridge Philos. Soc.*, (1)113 (1993), 9–22. ISSN 0305-0041. doi:10.1017/S0305004100075745.

[FD93] B. Farb and R.K. Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York (1993). ISBN 0-387-94057-X. doi:10.1007/978-1-4612-0889-1.

[FM12] B. Farb and D. Margalit. *A primer on mapping class groups*, volume 49 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ (2012). ISBN 978-0-691-14794-9.

[F71] K.L. Fields. On the Brauer-Speiser theorem. *Bull. Amer. Math. Soc.*, 77 (1971), 223. ISSN 0002-9904.

[G77] R. Gilman. Finite quotients of the automorphism group of a free group. *Canad. J. Math.*, (3)29 (1977), 541–551. ISSN 0008-414X.

[G64] H.B. Griffiths. Automorphisms of a 3-dimensional handlebody. *Abh. Math. Sem. Univ. Hamburg*, Vol. 26 (1963/1964). pp. 191–210. ISSN 0025-5858.

[GL09] F. Grunewald and A. Lubotzky. Linear representations of the automorphism group of a free group. *Geom. Funct. Anal.*, (5)18 (2009), 1564–1608. ISSN 1016-443X. doi:10.1007/s00039-009-0702-2.

[HH12] U. Hamenstädt and S. Hensel. The geometry of the handlebody groups I: distortion. *J. Topol. Anal.*, (1)4 (2012), 71–97. ISSN 1793-5253. doi:10.1142/S1793525312500070.

[HH13] U. Hamenstädt and S. Hensel. Isoperimetric inequalities for the handlebody groups. *Trans. Amer. Math. Soc.*, (10)365 (2013), 5313–5327. ISSN 0002-9947. doi:10.1090/S0002-9947-2012-05808-9.

[H83] J. Hempel. Intersection calculus on surfaces with applications to 3-manifolds. *Mem. Amer. Math. Soc.*, (282)43 (1983), vi+48. ISSN 0065-9266. doi:10.1090/memo/0282.

[J69] W. Jaco. Heegaard splittings and splitting homomorphisms. *Trans. Amer. Math. Soc.*, 144 (1969), 365–379. ISSN 0002-9947.

[JL01] G. James and M. Liebeck. *Representations and characters of groups*. Cambridge University Press, New York, second edition (2001). ISBN 0-521-00392-X.

[J75] G.J. Janusz. The Schur group of cyclotomic fields. *J. Number Theory*, (3)7 (1975), 345–352. ISSN 0022-314X.

[K98] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*.

American Mathematical Society, Providence, RI (1998). ISBN 0-8218-0904-0. With a preface in French by J. Tits.

[K12] T. Koberda. Asymptotic linearity of the mapping class group and a homological version of the Nielsen-Thurston classification. *Geom. Dedicata*, 156 (2012), 13–30. ISSN 0046-5755. doi:10.1007/s10711-011-9587-y.

[K03] M. Korkmaz. On cofinite subgroups of mapping class groups. *Turkish J. Math.*, (1)27 (2003), 115–123. ISSN 1300-0098.

[L97] E. Looijenga. Prym representations of mapping class groups. *Geom. Dedicata*, (1)64 (1997), 69–83. ISSN 0046-5755. doi:10.1023/A:1004909416648.

[L11] A. Lubotzky. Dynamics of $\mathrm{Aut}(F_N)$ actions on group presentations and representations. In: *Geometry, rigidity, and group actions*. Chicago Lectures in Math. Univ. Chicago Press, Chicago, IL (2011), pp. 609–643.

[LM12] A. Lubotzky and C. Meiri. Sieve methods in group theory II: the mapping class group. *Geom. Dedicata*, 159 (2012), 327–336. ISSN 0046-5755. doi:10.1007/s10711-011-9662-4.

[MS13] J. Malestein and J. Souto. On genericity of pseudo-Anosovs in the Torelli group. *Int. Math. Res. Not. IMRN*, (6) 2013, 1434–1449. ISSN 1073-7928.

[M91] G.A. Margulis. *Discrete subgroups of semisimple Lie groups, volume 17 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin (1991). ISBN 3-540-12179-X.

[MR12] G. Masbaum and A.W. Reid. All finite groups are involved in the mapping class group. *Geom. Topol.*, (3)16 (2012), 1393–1411. ISSN 1465-3060. doi:10.2140/gt.2012.16.1393.

[M01] J.D. McCarthy. On the first cohomology group of cofinite subgroups in surface mapping class groups. *Topology*, (2)40 (2001), 401–418. ISSN 0040-9383. doi:10.1016/S0040-9383(99)00066-X.

[M63] D.R. McMillan, Jr. Homeomorphisms on a solid torus. *Proc. Amer. Math. Soc.*, 14 (1963), 386–390. ISSN 0002-9939.

[M78] R. Mollin. The Schur group of a field of characteristic zero. *Pacific J. Math.*, (2)76 (1978), 471–478. ISSN 0030-8730. URL http://projecteuclid.org/getRecord?id=euclid.pjm/1102806834.

[PR94] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA (1994). ISBN 0-12-558180-7. Translated from the 1991 Russian original by Rachel Rowen.

[PW13] A. Putman and B. Wieland. Abelian quotients of subgroups of the mappings class group and higher Prym representations. *J. Lond. Math. Soc. (2)*, (1) 88 (2013), 79–96. ISSN 0024-6107. doi:10.1112/jlms/jdt001.

[R92] M.S. Raghunathan. A note on generators for arithmetic subgroups of algebraic groups. *Pacific J. Math., (2)* 152 (1992), 365–373. ISSN 0030-8730. URL http://projecteuclid.org/getRecord?id=euclid.pjm/1102636172.

[R04] M.S. Raghunathan. The congruence subgroup problem. *Proc. Indian Acad. Sci. Math. Sci.*, (4) 114 (2004), 299–308. ISSN 0253-4142. doi:10.1007/BF02829437.

[R34] K. Reidemeister. Homotopiegruppen von komplexen. *Abh. Math. Sem. Univ. Hamburg*, (1) 10 (1934), 211–215. ISSN 0025-5858. doi:10.1007/BF02940675.

[R75] I. Reiner. *Maximal orders*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York (1975). London Mathematical Society Monographs, No. 5.

[R57] M. Rosenlicht. Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl.* (4)43 (1957), 25–50. ISSN 0003-4622.

[S72] M.M. Schacher. More on the Schur subgroup. *Proc. Amer. Math. Soc.*, 31 (1972), 15–17. ISSN 0002-9939.

[T66] J. Tits. Classification of algebraic semisimple groups. In: *Algebraic Groups and Discontinuous Subgroups* (*Proc. Sympos. Pure Math., Boulder, Colo., 1965*). Amer. Math. Soc., Providence, R.I. (1966), pp. 33–62.

[V94] T.N. Venkataramana. On systems of generators of arithmetic subgroups of higher rank groups. *Pacific J. Math.*, (1)1661994, 193–212. ISSN 0030-8730. URL http://projecteuclid.org/getRecord?id=euclid.pjm/1102621249.

[Z62] H. Zieschang. Über einfache Kurven auf Vollbrezeln. *Abh. Math. Sem. Univ. Hamburg*, 25 (1961/1962), 231–250. ISSN 0025-5858

Fritz Grunewald, Mathematisches Institut der Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany

Michael Larsen, Department of Mathematics, Indiana University, Bloomington, IN, 47405, USA. mjlarsen@indiana.edu

Alexander Lubotzky, Einstein Institute of Mathematics, The Hebrew University of Jerusalem, 91904, Jerusalem, Israel. alex.lubotzky@mail.huji.ac.il

Justin Malestein, Department of Mathematics, University of Oklahoma, 601 Elm Avenue, Norman OK, 73019, USA jmalestein@math.ou.edu

Received: February 20, 2014
Accepted: August 25, 2014