Arithmetic representations of mapping class groups

EDUARD LOOIJENGA

Arithmetic representations of mapping class groups

EDUARD LOOIJENGA

Let S be a closed oriented surface and G a finite group of orientation-preserving automorphisms of S whose orbit space has genus at least two. There is a natural group homomorphism from the G-centralizer in $\mathrm{Diff}^+(S)$ to the G-centralizer in $\mathrm{Sp}(H_1(S))$. We give a sufficient condition for its image to be a subgroup of finite index.

1 Introduction and statement of the main result

Let S be a closed connected oriented surface of genus ≥ 2. The group $\mathrm{Diff}^+(S)$ of orientation-preserving diffeomorphisms of S acts on $H_1(S)$ via its connected component group $\pi_0(\mathrm{Diff}^+(S))$, known as the *mapping class group* of S, and it is a classical fact that the image of this representation is the full symplectic group $\mathrm{Sp}(H_1(S))$ of integral linear transformations which preserve the intersection form on $H_1(S)$. This paper concerns an equivariant version, where it is assumed that we are given a finite subgroup $G \subset \mathrm{Diff}^+(S)$. The centralizer $\mathrm{Diff}^+(S)^G$ of G in $\mathrm{Diff}^+(S)$ lands under the above symplectic representation in $\mathrm{Sp}(H_1(S))^G$ and the question we address here is how much smaller the image is. Besides its intrinsic interest, the answer has consequences for understanding the mapping class group of the G-orbit space of S. We shall regard the latter as an orbifold surface and denote it by S_G; the regular orbits then define an open subset $S_G^\circ \subset S_G$ with finite complement. This punctured surface S_G° has negative Euler characteristic. The image of $\mathrm{Diff}^+(S)^G$ in the mapping class group of the punctured surface S_G° is of finite index and thus makes $\mathrm{Sp}(H_1(S))$ a "virtual representation" of that mapping class group.

The work of Putman and Wieland [6] relates our question to the Ivanov conjecture as follows. Let us say that the G-action on S has the *Putman–Wieland property* if $\mathrm{Diff}^+(S)^G$ has no finite orbit in $H_1(S) \smallsetminus \{0\}$. These authors prove that if that property holds for a given genus h of S_G (no matter what S and G are), then every finite-index subgroup of a mapping class group of a connected oriented surface of finite type of genus $> h$ has zero first Betti number. The first part of our main result is about that property.

Theorem 1.1 *Let $S \to S_G$ be a G-cover as above.*

(i) *If this cover is trivial over a compact genus-one subsurface of S_G° with connected boundary, then the action of $\mathrm{Diff}^+(S)^G$ on $H_1(S)$ has no nonzero finite orbits.*

(ii) *If this cover is trivial over a compact genus-two subsurface of S_G° with connected boundary, then the image of $\mathrm{Diff}^+(S)^G$ in $\mathrm{Sp}(H_1(S))^G$ is of finite index.*

We will also obtain an arithmeticity property in the setting of (i). See the discussion and the end of this introduction as well as Remark 5.6.

Remark 1.2 In either case the cover over the complement of such a subsurface of S_G must be connected (for the subsurface has a connected boundary and S is connected). Since this complement has a boundary component over which the covering is trivial, we may contract that component (and each of the components lying over it) to obtain a G-covering $S' \to S_G'$, where the genus of S_G' is now one (resp. two) less than that of S_G. As this covering represents all the topological input, we may paraphrase our main theorem as saying that the Putman–Wieland property (resp. the arithmeticity property) holds after a "stabilization" by taking a connected sum of the base orbifold with a closed surface of genus one (resp. two).

We will prove this theorem under the apparently weaker assumption that there exists a closed one-dimensional submanifold nonempty $A \subset S_G^\circ$, so a disjoint union of say $k \geq 1$ embedded circles (with $k = 1$ in case (i) and $k = 2$ in case (ii)) such that $S \to S_G$ is trivial over A and connected over $S_G \smallsetminus A$. This looks as if this is a more general result, because it is easy to find in the respective cases such an A inside the postulated subsurface with the property that its complement is connected. But we will see that this generalization is only apparent.

There is also a useful geometric interpretation for this last formulation: given such an A, then we can obtain the G-covering $S' \to S_G'$ as above by regarding $S_G \smallsetminus A$ as a punctured surface (so with two punctures for each component of A) and letting $S_G' \supset S_G \smallsetminus A$ be the closed orbifold obtained by filling in these punctures as nonorbifold points. Our assumptions say that S_G' is a closed connected surface (the genus drop is the number of connected components of A) and that the given G-covering $S \to S_G$ arises from a G-covering $S' \to S_G'$ with, for each component of A, an identification of the fibers of this covering over the two associated points (as principal G-sets). If we give S_G a complex structure and thus turn it into a smooth complex-projective curve with an orbifold structure, then an algebraic geometer might be tempted to regard this orbifold curve as being in its moduli space near the Deligne–Mumford stratum where the orbifold acquires k nodes, but for which the G-covering stays irreducible and does not ramify over the nodes. The covering $S' \to S_G'$ then appears as the normalization of such a degeneration. No algebraic geometry is used in the proof, though, for the topological part of this paper uses methods that directly generalize those of Looijenga [3].

Let us compare the above theorem with the work of Grunewald, Larsen, Lubotzky and Malestein [1], whose main motivation was to construct, via the virtual isomorphism mentioned above, new arithmetic quotients of the mapping class group of S_G. They assume that G acts freely so that $S_G = S_G^\circ$ and impose another, more technical condition, which in our setup translates into requiring that we are in the context of (i) and demanding that the covering $S' \to S_G'$ is of "handlebody type", in the sense that it extends to a handlebody that has S_G' as boundary. They prove that the image of $\mathrm{Diff}^+(S)^G$ in each simple factor of $\mathrm{Sp}(H^1(S, \mathbb{Q}))^G$ is arithmetic. Our approach differs from theirs in several aspects, but mostly in our direct and relatively simple way of constructing G-equivariant mapping classes.

When speaking of arithmetic subgroups of $\mathrm{Sp}(H^1(S, \mathbb{Q}))^G$, it is of course tacitly understood that the latter can be regarded as the group of rational points of an algebraic group defined over $\mathbb{Q}$. Let us make this explicit.

Denote by $X(\mathbb{Q}G)$ the set of irreducible characters of $\mathbb{Q}G$ and choose for every $\chi \in X(\mathbb{Q}G)$ a representing irreducible (left) $\mathbb{Q}G$-module V_χ. We also fix on every V_χ a G-invariant inner product $s_\chi : V_\chi \times V_\chi \to \mathbb{Q}$ (which can be obtained as the G-average of an arbitrary inner product). This exhibits V_χ as a self-dual $\mathbb{Q}G$-module. Then $\mathrm{End}_{\mathbb{Q}G}(V_\chi)$ is a skew field which is of finite $\mathbb{Q}$-dimension. We denote its opposite by D_χ (meaning that the underling $\mathbb{Q}$-vector space is $\mathrm{End}_{\mathbb{Q}G}(V_\chi)$, but that composition is taken in opposite order) so that V_χ is now a right D_χ-module. Adopting as a convention that D_χ used as superscript (resp. subscript) indicates that we are dealing with right (resp. left) D_χ-module endomorphisms, then the natural map

$$\mathbb{Q}G \cong \prod_{\chi \in X(\mathbb{Q}G)} \mathrm{End}^{D_\chi}(V_\chi)$$

is an isomorphism of $\mathbb{Q}$-algebras. This is in fact the Wedderburn decomposition of $\mathbb{Q}G$, as each factor is a minimal two-sided ideal.

The group algebra $\mathbb{Q}G$ comes with an anti-involution $r \mapsto r^\dagger$ which takes each basis element e_g for $g \in G$ to the basis element $e_{g^{-1}}$. This identifies $\mathbb{Q}G$ with its opposite. Since V_χ is self-dual, in the above decomposition the involution leaves each factor $\mathrm{End}^{D_\chi}(V_\chi)$ invariant and induces one in the skew-field D_χ: the involution on $\mathrm{End}^{D_\chi}(V_\chi)$ is given by taking the s_χ-adjoint, given by $s_\chi(\sigma v, v') = s_\chi(v, \sigma^\dagger v')$. Since we have D_χ acting on V_χ on the right, this means that $s_\chi(v\lambda, v') = s_\chi(v, v'\lambda^\dagger)$. (We note in passing that any other G-invariant inner product s'_χ on V_χ is of the form $s_\chi(v\lambda, v')$ for some nonzero λ with $\lambda^\dagger = \lambda$; the associated anti-involution of D_χ is then a conjugate of $\dagger$.) The center of D_χ, which we denote by L_χ, is a number field, and the fixed-point set of $\dagger$ in L_χ is a subfield $K_\chi \subset L_\chi$ with $[L_\chi : K_\chi] \le 2$.

For a finitely generated $\mathbb{Q}G$-module H, denote by $H[\chi]$ the associated χ-isogeny space $\mathrm{Hom}_{\mathbb{Q}G}(V_\chi, H)$. The right D_χ-module structure on V_χ determines a left D_χ-module structure on $H[\chi]$ and the *isotypical decomposition* of H is the assertion that the natural map

$$\bigoplus_{\chi \in X(\mathbb{Q}G)} V_\chi \otimes_{D_\chi} H[\chi] \to H, \quad v \otimes_{D_\chi} u \in V_\chi \otimes_{D_\chi} H[\chi] \mapsto u(v),$$

is an isomorphism of $\mathbb{Q}G$-modules. So the *χ-isotypical subspace* of H, ie the image H_χ of $V_\chi \otimes_{D_\chi} H[\chi]$ in V, has the structure of a K_χ-vector space.

Assume now that H comes equipped with a nondegenerate G-invariant symplectic form $(a, b) \in H \times H \mapsto a \cdot b \in \mathbb{Q}$. Then the isotypical decomposition of H is symplectic, so that we also have a decomposition $\mathrm{Sp}(H)^G = \prod_{\chi \in X(\mathbb{Q}G)} \mathrm{Sp}(H_\chi)^G$. Every factor $\mathrm{Sp}(H_\chi)^G$ can be understood with the help of the skew-hermitian form

$$(f, f') \in H[\chi] \times H[\chi] \mapsto \langle f, f' \rangle_\chi \in D_\chi,$$

which is characterized by the property that for all $v, v' \in V_\chi$,

$$f(v) \cdot f'(v') = s_\chi(v \langle f, f' \rangle_\chi, v')$$

(*skew-hermitian* means that the form is D_χ-linear in the first variable and $\langle f', f \rangle_\chi = -\langle f, f' \rangle_\chi^\dagger$). Indeed, for fixed f and f', the map $(v, v') \in V_\chi \times V_\chi \mapsto f(v) \cdot f'(v') \in \mathbb{Q}$ is a bilinear form on V_χ. Since $s_\chi \colon V_\chi \times V_\chi \to \mathbb{Q}$ is nondegenerate, there exists a unique $\mathbb{Q}$-linear endomorphism σ of V_χ such that $f(v) \cdot f'(v') = s_\chi(\sigma(v), v')$. The G-invariance of both bilinear forms implies that σ is G-equivariant, ie is an element of $\mathrm{End}_{\mathbb{Q}G}(V_\chi)$. We prefer to regard it as an element of its opposite D_χ, so that $f(v) \cdot f'(v') = s_\chi(v\sigma, v')$. This σ is evidently $\mathbb{Q}$-linear in both f and f', and that is why we denote it by $\langle f, f' \rangle_\chi \in D_\chi$. It is then a little exercise to check that $\langle , \rangle_\chi$ is skew-hermitian. This form is nondegenerate in an obvious sense. The group of automorphisms $H[\chi]$ that preserve this form is a generalized unitary group, and therefore written as $U(H[\chi])$.

Any element of $\mathrm{Sp}(H_\chi)^G$ acts via the isomorphism $H_\chi \cong V_\chi \otimes_{D_\chi} H[\chi]$ as an element of the form $1_{V_\chi} \otimes u$ with $u \in U(H[\chi])$, and this identifies $\mathrm{Sp}(H_\chi)^G$ with $U(H[\chi])$. The group $U(H[\chi])$ is the group of K_χ-points of a reductive algebraic group defined over K_χ, whereas $\mathrm{Sp}(H_\chi)^G$ is the group of $\mathbb{Q}$-points of an algebraic group defined over $\mathbb{Q}$. Indeed, the latter is obtained from the former by the restriction of scalars $K_\chi | \mathbb{Q}$.

Theorem 1.1 then amounts to the assertion that the image of $\mathrm{Diff}^+(S)^G$ in the product of unitary groups $\prod_{\chi \in X(\mathbb{Q}G)} U(H_1(S; \mathbb{Q})[\chi])$ is arithmetic. We use this decomposition to prove the theorem, since we first prove arithmeticity for a single factor. This leads to a somewhat stronger result, for we show that in the setting of (i) of our main theorem (so when $S \to S_G$ is trivial over a genus-one subsurface) the image of $\mathrm{Diff}^+(S)^G$ in $U(H_1(S; \mathbb{Q})[\chi])$ is almost always arithmetic (see Remark 5.6).

Structure Of the four sections, only the last one is topological, but in order to put the constructions given there to work, we need a considerable amount of algebra and that explains the nature of the preceding sections.

Section 2 collects useful (and essentially known) algebraic proprieties of constructs that we encounter in the symplectic representation theory of a finite group over $\mathbb{Q}$. So there is little or no claim of originality here, although it was (for us) a bit of an effort to extract this material from the literature. In Section 3 we introduce and study what we might regard as the basic symplectic module associated to an irreducible $\mathbb{Q}G$-module, where G is a finite group. The main result is Proposition 3.1, which states an arithmeticity property and also lists the (few) cases for which this arithmetic group has real rank ≤ 1. This prepares us for stating and proving the arithmeticity criterion Theorem 4.2 in Section 4, which furnishes the main algebraic input for Section 5. As mentioned, this last section is essentially topological: we there construct sufficiently many G-equivariant mapping classes to ensure that we can apply said theorem to obtain our main theorem, Theorem 1.1.

2 Brief review of special unitary groups

The Albert classification In this subsection, D is a skew field of finite dimension over $\mathbb{Q}$ endowed with an anti-involution $\dagger$. We assume that the involution $\dagger$ is positive in the sense that $\lambda \in D \mapsto \operatorname{tr}_{D/\mathbb{Q}}(\lambda\lambda^{\dagger})$ is a positive-definite form. We remark that this is so for the cases that matter here, for the given anti-involution on $\mathbb{Q}G$ is evidently positive: for $r \in \mathbb{Q}G$, the $\mathbb{Q}$-trace of $rr^{\dagger}$ is $|G|$ times the coefficient of e_1 in $rr^{\dagger}$, and hence is positive definite. The same is then true for its Wedderburn factors $\operatorname{End}^{D_\chi}(V_\chi)$ and their associated skew fields D_χ.

We denote the center of D by L (so it is a number field) and denote by D_+ (resp. K) the $\dagger$-invariant part of D (resp. L). Albert's classification of such pairs $(D, \dagger)$ — see for example [5, Chapter IV, Theorem 2] — then tells us that K is totally real, so that $\mathbb{R} \otimes_{\mathbb{Q}} D = \prod_{\sigma} \mathbb{R} \otimes_{\sigma} D$, where σ runs over the distinct field embeddings $\sigma \colon K \hookrightarrow \mathbb{R}$, and that there are essentially four cases:

(I) $D = L = K$ so that $\mathbb{R} \otimes_{\sigma} D = \mathbb{R}$ for each σ,

(II) $L = K$ and for each σ there exists an isomorphism $\mathbb{R} \otimes_{\sigma} D \cong \operatorname{End}_{\mathbb{R}}(\mathbb{R}^2)$ which sends $\dagger$ to taking the transpose (so $[D : L] = 4$),

(III) $L = K$ and for each σ there exists an isomorphism $\mathbb{R} \otimes_{\sigma} D \cong \mathbb{K}$, where $\mathbb{K}$ denotes the Hamilton quaternions, which sends $\dagger$ to quaternion conjugation (so $[D : L] = 4$),

(IV) L is a purely imaginary extension of K (in other words, L is a CM field) and for each σ there exists an isomorphism $\mathbb{R} \otimes_{\sigma} D \cong \operatorname{End}_{\mathbb{C}}(\mathbb{C}^d)$, which takes $\mathbb{R} \otimes_{\sigma} L$ to $\mathbb{C}$ (so $[D : L] = d^2$) and sends $\dagger$ to taking the conjugate transpose.

Let M be a left D-module of finite rank. We write $M^{\dagger}$ for M endowed with the structure of a right D-module via the rule $a\lambda := \lambda^{\dagger}a$ for $a \in M$ and $\lambda \in D$. So if M' is another left D-module, then $M^{\dagger} \otimes_D M'$ is defined. It is a K-vector space with the property that $a \otimes_D \lambda a' = (\lambda^{\dagger}a) \otimes_D a'$ for all $\lambda \in D$, $a \in M$ and $a' \in M'$. In particular, we have in $M^{\dagger} \otimes_D M$ a K-linear involution defined by $(a \otimes_D b)' = b \otimes_D a$. We denote its fixed-point set by $u(M) \subset M^{\dagger} \otimes_D M$. As a $\mathbb{Q}$-subspace of $M^{\dagger} \otimes_D M$, it is spanned by the symmetric tensors $a \otimes_D a$.

Isotropic transvections and Eichler transformations Let $(a, b) \in M \times M \mapsto \langle a, b \rangle \in D$ be a skew-hermitian form on M. We denote its radical by M_o, so that the form descends to a nondegenerate one on $\overline{M} := M/M_o$. We define the associated unitary group $U(M)$ as the group of D-linear automorphisms of M that preserve the form and act as the identity on M_o. It is the group of K-points of an algebraic group defined over K. If the form is nondegenerate ($M_o = 0$), then $U(M)$ is what is called in [2, Section 5.2B] a *classical unitary group*.

If $c \in M$ is *isotropic* (meaning that $\langle c, c \rangle = 0$), then we have the associated *isotropic transvection* $T_c = T(c \otimes_D c) \in U(M)$ defined by $x \in M \mapsto x + \langle x, c \rangle c$ (so $c \otimes_D c$ is here understood as an element of $M^\dagger \otimes_D M$). It "generates" an abelian unipotent subgroup of $U(M)$ defined by

$$\lambda \in D_+ \mapsto T(c \otimes_D \lambda c) \in U(M), \quad T(c \otimes_D \lambda c)(x) = x + \langle x, \lambda c \rangle c.$$

Isotropic transvections are particular cases of Eichler transformations. These are defined as follows: Let $c \in M$ be isotropic, $a \in M$ perpendicular to c and $\lambda \in D$ such that $\lambda - \lambda^\dagger = \langle a, a \rangle$ (equivalently, $\lambda - \frac{1}{2}\langle a, a \rangle \in D_+$). Then the associated *Eichler transformation* is

$$E(c, a, \lambda): x \in M \mapsto x + \langle x, a \rangle c + \langle x, c \rangle a + \langle x, c \rangle \lambda c \in M.$$

It is a D-linear transformation which preserves the form. When $\lambda = \frac{1}{2}\langle a, a \rangle$, we shall write $E(c, a)$ instead. Since $T(c \otimes_D c) = E\left(\frac{1}{2}c, c\right)$, isotropic transvections are Eichler transformations, as asserted.

One checks that each Eichler transformation lies in $U(M)$ as defined above. In fact, $t \in K \mapsto E(tc, a, \lambda) = E(c, ta, t^2\lambda)$ is a closed one-parameter subgroup of $U(M)$ whose infinitesimal generator is represented by $a \otimes_D c + c \otimes_D a \in u(M)$ — or rather by its image in $u(M)/u(M_o)$, for if both a and c lie in M_o, then we get the identity. By a general property of algebraic groups [8, Corollary 2.2.7], such subgroups then generate a closed algebraic K-subgroup of $U(M)$. Following [2], we denote that group by $EU(M)$.

We note the commutator identity

(1) $$[E(c, a_1, \lambda_1), E(c, a_2, \lambda_2)] = T(c \otimes \lambda c) \quad \text{with } \lambda = \langle a_1, a_2 \rangle + \langle a_1, a_2 \rangle^\dagger.$$

It follows that if we fix c, but let a and λ vary (subject to the conditions above, so with $a \in c^\perp$), then the $E(c, a, \lambda)$ generate a unipotent group that appears as an extension of the vector group $c^\perp/(M_o + Dc)$ by the abelian subgroup of $U(M)$ defined by the $T(c \otimes_D \lambda c)$.

The group $EU(M)$ is already generated by the isotropic transvections: When $\dagger$ is nontrivial this follows from [2, (6.3.1)]. The remaining case is the one we labeled (I). This is when $D = L = K$ and $U(M)$ is a symplectic group over K, but then there is no issue, because every $a \in M$ is isotropic, and then $E(c, a) = T_{a+c} T_a^{-1} T_c^{-1}$.

Unipotent radical and Levi quotient If the form is nondegenerate (ie $M_o = \{0\}$), then $EU(M)$ is a K-form of a classical semisimple algebraic group, and hence has finite center. To be precise, it is a group of symplectic type in cases (I) and (II), of orthogonal type in case (III) and of special linear type in case (IV).

If M_o is possibly nonzero, then per convention, the elements of $U(M)$ act trivially on M_o. The natural map $U(M) \to U(\overline{M})$ is evidently onto. Its kernel consists of the transformations that act trivially on both M_o and M/M_o, and is therefore the unipotent radical $R_u(U(M))$ of $U(M)$ — recall that $U(\overline{M})$ is reductive. We have an exact sequence

$$1 \to R_u(U(M)) \to U(M) \to U(\overline{M}) \to 1.$$

The elements of $R_u(U(M))$ are the Eichler transformations $E(c,a)$ with $c \in M_o$ and $a \in M$ arbitrary. In this case $E(c,a)$ only depends on the image of $c \otimes_{\mathbb{Z}} a$ in $M_o^\dagger \otimes_D \overline{M}$), so that the resulting map

$$M_0^\dagger \otimes_D \overline{M} \to R_u(U(M))$$

is an isomorphism. So $R_u(U(M))$ is a vector group over K (ie a K-vector space regarded as the group of K-points of a K-algebraic group of additive type). Since $EU(\overline{M})$ is a normal semisimple subgroup of $U(M)$, it has the same unipotent radical: $R_u(EU(M)) = R_u(U(M))$.

The relation between $EU(M)$ and $U(M)$ Since in what follows the notion of the real rank of an algebraic group shows up, let us begin with reviewing this concept briefly.

Let $\mathcal{G}$ be a reductive algebraic group. Suppose first that $\mathcal{G}$ is defined over $\mathbb{R}$. Then the real rank $\mathrm{rk}_{\mathbb{R}}(\mathcal{G})$ of $\mathcal{G}$ is by definition the dimension of a Cartan subgroup of $\mathcal{G}$ defined over $\mathbb{R}$. For example, if $\mathcal{G}$ is the orthogonal group of a nondegenerate quadratic form over $\mathbb{R}$, then its real rank is the Witt index of this form: the dimension of a maximal isotropic subspace defined over $\mathbb{R}$. If $\mathcal{G}$ is defined over a number field k, then we restrict scalars à la Weil so that $\mathrm{Res}_{k|\mathbb{Q}}\, \mathcal{G}$ is a group defined over $\mathbb{Q}$. We then regard $\mathrm{Res}_{k|\mathbb{Q}}\, \mathcal{G}$ (by base change) as a group over $\mathbb{R}$, and define the real rank of $\mathcal{G}$ to be the real rank of the latter. Concretely, if $\sigma_1, \ldots, \sigma_r$ are the real embeddings of k in $\mathbb{R}$ and $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$ are the remaining distinct (complex) embeddings (they come in complex conjugate pairs), then the definition comes down to

$$\mathrm{rk}_{\mathbb{R}}(\mathcal{G}) = \sum_{i=1}^{r} \mathrm{rk}_{\mathbb{R}}(\mathcal{G}_{\sigma_i}) + \sum_{i=1}^{s} \mathrm{rk}_{\mathbb{C}}(\mathcal{G}_{\tau_i})$$

(this is also the sum over all the archimedean valuations of k, taking as general term the real rank of the corresponding completion of $\mathcal{G}(k)$). The Dirichlet unit theorem often gives lower bounds for the rank. For example, if the skew field D is as in the Albert classification, the group of units $D^\times$ is a reductive group defined over K, and its group of real points and its real rank are then as follows, putting $e := [K : \mathbb{Q}]$:

(I) $\mathrm{Res}_{K|\mathbb{Q}}\, D^\times(\mathbb{R})$ is open in $(\mathbb{R}^\times)^e$; the real rank of $D^\times$ is e,

(II) $\mathrm{Res}_{K|\mathbb{Q}}\, D^\times(\mathbb{R})$ is open in $\mathrm{GL}_2(\mathbb{R})^e$; the real rank of $D^\times$ is $2e$,

(III) $\mathrm{Res}_{K|\mathbb{Q}}\, D^\times(\mathbb{R})$ is open in $(\mathbb{K}^\times)^e$; the real rank of $D^\times$ is e,

(IV) $\mathrm{Res}_{K|\mathbb{Q}}\, D^\times(\mathbb{R})$ is open in $\mathrm{GL}_d(\mathbb{C})^e$; the real rank of $D^\times$ is de.

So $D^\times$ has real rank ≥ 2, unless D equals $\mathbb{Q}$ (I), is a definite quaternion algebra with center $\mathbb{Q}$ (III) or is an imaginary quadratic extension of $\mathbb{Q}$.

It is clear that $\mathrm{EU}(M)$ is a normal subgroup of $U(M)$. We already noticed that it is closed in $U(M)$, and hence the quotient $U(M)/\mathrm{EU}(M)$ is also an algebraic group. Note however that if $\overline{M}$ has no nonzero isotropic vectors, then $\mathrm{EU}(\overline{M})$ is trivial. We mention for future reference a consequence of a theorem of G E Wall [10]:

Lemma 2.1 *If M is nondegenerate and contains a nonzero isotropic vector, then $U(M)/\mathrm{EU}(M)$ is anisotropic (all its real forms are compact). So $\mathrm{EU}(M)$ and $U(M)$ have the same real rank, and any arithmetic subgroup of $U(M)$ will have finite image in $U(M)/\mathrm{EU}(M)$.*

Proof Theorem 1 of [10] identifies $U(M)/\mathrm{EU}(M)$ as a quotient of $D^{\times}$ by a normal subgroup which contains $D^{\times} \cap D_{+}$. It is easy to check that in all four cases (I)–(IV) in the Albert classification such a quotient must be anisotropic. ☐

Wall's result is more specific and tells us that $U(M)/\mathrm{EU}(M)$ is often an anisotropic torus. But this need not be so when $\dim_D M = 2$.

Lemma 2.2 *If M is nondegenerate isotropic, then the K-algebraic group $\mathrm{EU}(M)$ is almost simple (by which we mean that $\mathrm{EU}(M)$ is perfect and every proper normal subgroup is contained in its center) unless $D = K$ and $M \cong K^4$ is endowed with a nondegenerate symmetric form which admits an isotropic plane defined over K.*

Proof This follows from [2, Theorem 6.3.16 combined with Theorem 6.3.15]. ☐

The excepted case is genuine, for in that case $M \cong M_1 \otimes_K M_2$ as modules endowed with K-forms, where M_i is a two-dimensional K-vector space endowed with a nondegenerate symplectic form. The resulting map $\mathrm{SL}(M_1) \times \mathrm{SL}(M_2) \to \mathrm{GL}(M)$ has image $\mathrm{EU}(M) \cong O(M)$ and its kernel has $(-1,-1)$ as its unique nonidentity element.

Remark 2.3 The *reduced norm* is the homomorphism $N : U(M) \to L^{\times}$ characterized by the following property: if $T \in U(M)$, then for some (or equivalently, every) real embedding $\sigma : K \hookrightarrow \mathbb{R}$, the D-linear T induces a linear transformation of the $(\mathbb{R} \otimes_{\sigma} L)$-vector space $\mathbb{R} \otimes_K M$ whose determinant is $1 \otimes_{\sigma} N(T)$. The kernel of N, usually denoted by $\mathrm{SU}(M)$, contains $\mathrm{EU}(M)$ and is often equal to it. But in our context this group does not show up in a natural manner.

3 The hyperbolic module attached to a finite group

A hermitian extension Our discussion of symplectic $\mathbb{Q}G$-modules also applies to orthogonal $\mathbb{Q}G$-modules. One such module is $\mathbb{Q}G$ itself (regarded as a left module). It comes indeed with a G-invariant pairing $\mathbb{Q}G \times \mathbb{Q}G \to \mathbb{Q}$, the *trace form*, which assigns to the pair (r_1, r_2) the trace of $r_1 r_2^{\dagger}$ considered as an endomorphism of $\mathbb{Q}G$ as a $\mathbb{Q}$-vector space (this is simply $|G|$ times the coefficient of e_1). This pairing is symmetric and nondegenerate.

The Wedderburn decomposition $\mathbb{Q}G \cong \prod_\chi \mathrm{End}^{D_\chi}(V_\chi)$ is also the isotypical decomposition, for the K_χ-linear map

$$V_\chi \otimes_{D_\chi} \mathrm{Hom}^{D_\chi}(V_\chi, D_\chi) \to \mathrm{End}^{D_\chi}(V_\chi), \quad v_1 \otimes_{D_\chi} f : v \in V_\chi \mapsto v_1 f(v),$$

which assigns to $v_1 \otimes_{D_\chi} f$ the endomorphism $v \in V_\chi \mapsto v_1 f(v)$ is well defined and is an isomorphism of left $\mathbb{Q}G$-modules (and also as right $\mathbb{Q}G$-modules). This also shows that $\mathbb{Q}G[\chi] \cong \mathrm{Hom}^{D_\chi}(V_\chi, D_\chi)$ as a right D_χ-module.

We claim that $\mathrm{Hom}^{D_\chi}(V_\chi, D_\chi) \cong V_\chi^\dagger$ as left D_χ-modules. This is based on a hermitian extension of s_χ to $V_\chi^\dagger$: if we follow the same recipe as in the introduction for a symplectic representation, then we find that there is a hermitian form $h_\chi : V_\chi^\dagger \times V_\chi^\dagger \to D_\chi$ characterized by the property that for all $v, v' \in V_\chi$ and $f, f' \in V_\chi^\dagger$,

$$s_\chi(v, f') s_\chi(v', f) = s_\chi(v h_\chi(f, f'), v').$$

This formula implies that h_χ is G-invariant (we let G act on the right of $V_\chi^\dagger$). By taking $v = f = f'$, we also see that $h_\chi(f, f) = s_\chi(f, f)$, so that h_χ is a hermitian extension of s_χ. For every $v \in V_\chi^\dagger$, the expression $h_\chi(v, -)$ yields an element of $\mathrm{Hom}^{D_\chi}(V_\chi, D_\chi)$ and defines the stated isomorphism.

Isotropic transvections Henceforth we write R for the integral group ring $\mathbb{Z}G$. Let M be a finitely generated (left) R-module, free over $\mathbb{Z}$, and let $(a, b) \in M \times M \mapsto a \cdot b \in \mathbb{Z}$ be a nondegenerate (but not necessarily unimodular) G-equivariant symplectic form. We extend this in the standard manner to a form

$$(a, b) \in M \times M \mapsto \langle a, b \rangle := \sum_{g \in G} (g^{-1} a \cdot b) e_g = \sum_{g \in G} (a \cdot gb) e_g \in R.$$

This form is skew-hermitian: it is R-linear in the first variable and $\langle a, b \rangle = -\langle b, a \rangle^\dagger$. A $\mathbb{Z}$-linear automorphism of M is G-equivariant and preserves the symplectic form if and only if it is an R-module automorphism which preserves this skew-hermitian form. We denote the group of such automorphisms by $U(M)$.

Let R_+ stand for the fixed-point set of $\dagger$ in R; this is an additive subgroup of R. If $a \in M$ is R-isotropic in the sense that $\langle a, a \rangle = 0$, then for every $r \in R_+$ the isotropic transvection

(2) $$T_a(r) : x \in M \mapsto x + \langle x, a \rangle r a \in M$$

lies in $U(M)$ and $r \in R_+ \mapsto T_a(r)$ is a homomorphism from (the additively written) R_+ to (the multiplicatively written) $U(M)$. Since $T_a(r)$ only depends on $a \otimes r a \in M^\dagger \otimes_R M$, we also denote this transformation by $T(a \otimes r a)$.

The basic hyperbolic module Let A be a (not necessarily commutative) unital ring with unit endowed with an anti-involution $\dagger$. The *basic hyperbolic A-module* $\mathcal{H}^2(A)$ is the free left A-module of rank two (whose generators we denote by e and f) endowed with the skew-hermitian form defined by

$\langle e, e \rangle = \langle f, f \rangle = 0$ and $\langle e, f \rangle = 1$. It can be regarded as the A-form of the standard symplectic module $\mathbb{Z}^2$. In vector notation:

$$\left\langle \begin{pmatrix} a' \\ a'' \end{pmatrix}, \begin{pmatrix} b' \\ b'' \end{pmatrix} \right\rangle = a'b''^\dagger - a''b'^\dagger. \tag{3}$$

It is unimodular in the sense that $a \in \mathcal{H}^2(A) \mapsto \langle -, a \rangle \in \mathrm{Hom}_A(\mathcal{H}^2(A), A)$ is an antilinear isomorphism. We will write $U_2(A)$ and $\mathrm{EU}_2(A))$ for $U(\mathcal{H}^2(A))$ and $\mathrm{EU}(\mathcal{H}^2(A))$, respectively. The latter contains $\mathrm{SL}_2(\mathbb{Z})$ in an obvious manner. Let $A_+ \subset A$ be the set of $\dagger$-invariant elements. One verifies that $T_e : x \in \mathcal{H}^2(A) \mapsto x + \langle x, e \rangle e$ and the similarly defined T_f have the matrix form

$$T_e(a) = \begin{pmatrix} 1 & -\rho_a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad T_f(a) = \begin{pmatrix} 1 & 1 \\ \rho_a & 1 \end{pmatrix},$$

respectively, where ρ_a stands for right multiplication with a.

The group $\Gamma(G)$ We take $A = R(= \mathbb{Z}G)$. The elements of the form $r + r^\dagger$ with $r \in R$ make up a subgroup R_{++} of R_+ such that R_+/R_{++} is a finite-dimensional $\mathbb{F}_2$-vector space. Let $\Gamma_+(G)$ and $\Gamma_-(G)$ denote the subgroups of $\mathrm{EU}_2(R)$ generated by $T_e(R_{++})$ and $T_f(R_{++})$, respectively, and let $\Gamma_o(G) \subset \mathrm{EU}_2(R)$ stand for the subgroup generated by $\Gamma_+(G)$ and $\mathrm{SL}_2(\mathbb{Z})$. Since $\Gamma_-(G)$ is a $\mathrm{SL}_2(\mathbb{Z})$-conjugate of $\Gamma_+(G)$, the group $\Gamma_o(G)$ contains $T_f(R_{++})$. The right (inverse) action of G on $\mathcal{H}^2(R)$ defines an embedding of G in $U_2(R)$. One checks that

$$\rho_g T_e(r) \rho_{g^\dagger} = T_e(grg^{-1}),$$

and so G normalizes $\Gamma_o(G)$. We put $\Gamma(G) := \Gamma_o(G).G$.

Arithmetic nature of $\Gamma(G)$ The notion of a basic hyperbolic module generalizes in a straightforward manner to $\mathcal{H}^2(V_\chi^\dagger)$, the skew-hermitian form being given by

$$\left\langle \begin{pmatrix} v' \\ v'' \end{pmatrix}, \begin{pmatrix} w' \\ w'' \end{pmatrix} \right\rangle = h_\chi(v', w'') - h_\chi(v'', w'). \tag{4}$$

So we have defined $U_2(V_\chi^\dagger)$; it is the group of K_χ-points of a reductive algebraic group defined over K_χ. If we write an element of $U_2(V_\chi^\dagger)$ in block form $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, with A, B, C and D in $\mathrm{End}_{D_\chi}(V_\chi^\dagger)$, then the subgroup defined by $C = 0$ is parabolic. Its unipotent radical is given by requiring that in addition A and D are the identity. The corresponding subgroup is then the vector group $\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix}$ for which B is hermitian relative to h_χ. In other words, h_χ identifies B with an element of $u(V_\chi^\dagger)$ — that is, a symmetric element of $V_\chi \otimes_{D_\chi} V_\chi^\dagger$ — and hence defines an isotropic transvection. In particular, this is also the unipotent radical of the corresponding subgroup of $\mathrm{EU}_2(V_\chi^\dagger)$. An opposite parabolic subgroup is defined by $B = 0$ and has a similar description of its unipotent radical. Let us denote these unipotent radicals by $\mathcal{R}_+(U_2(V_\chi^\dagger))$ and $\mathcal{R}_-(U_2(V_\chi^\dagger))$, respectively.

We run into this when we consider the isotypical decomposition of $\mathcal{H}^2(\mathbb{Q}G)$. The isogeny space $\mathcal{H}^2(\mathbb{Q}G)[\chi] = \operatorname{Hom}_{\mathbb{Q}G}(V_\chi, \mathcal{H}^2(\mathbb{Q}G))$ is then a left D_χ-module that is naturally identified with $\mathcal{H}^2(V_\chi^\dagger)$. This gives rise to a decomposition

$$U_2(\mathbb{Q}G) = \prod_{\chi \in X(\mathbb{Q}G)} U_2(V_\chi^\dagger).$$

The image of $\Gamma_\pm(G)$ in $U_2(V_\chi^\dagger)$ clearly lands in $\mathcal{R}_\pm(U_2(V_\chi^\dagger))$. Since $\operatorname{End}_{D_\chi}(V_\chi^\dagger) = \operatorname{End}^{D_\chi}(V_\chi)$ is a Wedderburn factor of $\mathbb{Q}G$, it follows that the image of R in $\operatorname{End}_{D_\chi}(V_\chi^\dagger)$ is an order (a lattice that is also a unital algebra). This is compatible with the anti-involutions, and hence the image of R_{++} in $\operatorname{End}_{D_\chi}(V_\chi^\dagger)$ is a lattice in the subspace of hermitian matrices. So the image of $\Gamma_\pm(G)$ in $U_2(V_\chi^\dagger)$ is a lattice in $\mathcal{R}_\pm(U_2(V_\chi^\dagger))$.

It is clear that $\Gamma_o(G)$ maps to $\operatorname{EU}_2(V_\chi^\dagger)$.

Proposition 3.1 *The image of $\Gamma(G)$ in $U_2(V_\chi^\dagger)$ is an arithmetic subgroup. The real rank of $U_2(V_\chi^\dagger)$ is ≥ 2 unless $\dim_{D_\chi} V_\chi = 1$. In that last case, where we can assume that $V_\chi^\dagger = D_\chi$ with G acting on the right and mapping to its group of units, one of the following holds:*

  (i) $D_\chi = \mathbb{Q}$ *and G maps to μ_2,*
 (iia) D_χ *is the Gaussian field $\mathbb{Q}(\sqrt{-1})$ and G maps onto μ_4,*
 (iib) D_χ *is the Eisenstein field $\mathbb{Q}(\sqrt{-3})$ and G maps onto μ_3 or μ_6,*
(iiia) $D_\chi \cong \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ *and G maps onto its group of units (a binary tetrahedral group of order 24) or onto the quaternion group of order 8, or*
(iiib) $D_\chi \cong \mathbb{Q} + \mathbb{Q}\sqrt{3}i + \mathbb{Q}j + \mathbb{Q}\sqrt{3}k$ *and G maps onto the binary dihedral group of order 12.*

In all cases, $\Gamma(G)$ acts $\mathbb{Q}$-irreducibly in $\mathcal{H}^2(V_\chi^\dagger)$.

Remark 3.2 It is well known that the quaternion group appearing in [Proposition 3.1](iiia) is realized as the Galois group of a torus ramified at four points (the covering surface has genus three). This example is like a Swiss army knife for illustrating (and refuting) statements in complex dynamics, which is why that community refers to it as the *eierlegende Wollmilchsau*. We do not know whether its appearance here is just a coincidence.

For the proof we need:

Theorem 3.3 (Raghunathan [7], Venkataramana [9]) *Let $\mathcal{G}$ be an almost simple simply connected $\mathbb{Q}$-algebraic group of real rank ≥ 2. Let $\mathcal{R}_-$ and $\mathcal{R}_+$ be $\mathbb{Q}$-subgroups that contain the unipotent radicals of opposite $\mathbb{Q}$-parabolic subgroups of $\mathcal{G}$. Then for any pair of lattices $\Gamma_+ \subset \mathcal{R}_+(\mathbb{Q})$ and $\Gamma_- \subset \mathcal{R}_-(\mathbb{Q})$, the subgroup of $\mathcal{G}(\mathbb{Q})$ generated by their union $\Gamma_+ \cup \Gamma_-$ is a congruence subgroup of $\mathcal{G}(\mathbb{Q})$.*

Proof We first prove the arithmeticity property of $\Gamma_o(G)$ in $\operatorname{EU}_2(V_\chi^\dagger)$. Let us first observe that the group $\operatorname{EU}_2(V_\chi^\dagger)$ is almost simple by [Lemma 2.2](#). Indeed, this can only fail if $D_\chi = K_\chi$ and the form is symmetric (with $\dim_{K_\chi} V_\chi^\dagger = 2$), and this is clearly not the case.

If the real rank of $EU_2(V_\chi^\dagger)$ is ≥ 2, then the theorem of Raghunathan and Venkataramana applies and we conclude that $\Gamma_o(\chi)$ is an arithmetic subgroup of $EU_2(V_\chi^\dagger)$. It is then also easy to see that $\Gamma(G)$ acts $\mathbb{Q}$-irreducibly in $\mathcal{H}^2(V_\chi^\dagger)$.

Since the real rank of $EU_2(V_\chi^\dagger)$ is $\geq \dim_{D_\chi} V_\chi^\dagger$, it remains to treat the case when $\dim_{D_\chi} V_\chi^\dagger = 1$. In other words, we can assume that $V_\chi^\dagger = D_\chi$. The real rank of $EU_2(D_\chi)$ is then still ≥ 2 most of the time. As we saw above, the exceptions are the cases for which $K_\chi = \mathbb{Q}$ and D_χ is either $\mathbb{Q}$, a definite quaternion algebra over $\mathbb{Q}$ with center $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. Since D_χ is also an irreducible $\mathbb{Q}G$-module, we have a homomorphism $\rho: G \to D_\chi^\times$ whose image contains a $\mathbb{Q}$-basis of D_χ. In particular, D is generated over $\mathbb{Q}$ by its units. So if D_χ is an imaginary quadratic extension of $\mathbb{Q}$, then D_χ is either $\mathbb{Q}$, the Gaussian field or the Eisenstein field. In the definite quaternion case, $D_\chi^\times(\mathbb{R})$ is the group of unit quaternions, and hence $\rho(G)$ is one of the subgroups classified by Klein: this group must be binary tetrahedral, binary octahedral, binary icosahedral or binary dihedral (of order $4n$). In these cases $\rho(\mathbb{Q}G) \cap \mathbb{R}$ equals $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\cos(\pi/n))$, respectively. Since we want this intersection to be $\mathbb{Q}$, only the two groups listed have that property.

Note that in each of these exceptional cases, $D_{\chi,+} = K_\chi = \mathbb{Q}$. The isotropic subspaces in $\mathcal{H}^2(D_\chi)$ are defined over $\mathbb{Q}$, and hence $EU_2(D_\chi) \cong SL_2(\mathbb{Q})$. The group $\Gamma_o(\chi)$ is then a copy of $SL_2(\mathbb{Z})$. So $\Gamma_o(G)$ is arithmetic in $EU_2(V_\chi^\dagger)$. In view of Lemma 2.1 this also implies the arithmeticity of $\Gamma(G)$ in $U_2(V_\chi^\dagger)$. The actions of G (on the right) and $SL_2(\mathbb{Z})$ (on the left) on $\mathcal{H}^2(V_\chi^\dagger)$ commute and make $\mathcal{H}^2(V_\chi^\dagger)$ an exterior tensor product of irreducible $\mathbb{Q}$-representations: it is the right $\mathbb{Q}G$-module $V_\chi^\dagger$ tensored with the tautological representation of $SL_2(\mathbb{Z})$ on $\mathbb{Q}^2$ (which is absolutely irreducible). Hence $\mathcal{H}^2(V_\chi^\dagger)$ is irreducible as a representation of $SL_2(\mathbb{Z}) \times G$. This implies that $\mathcal{H}^2(V_\chi^\dagger)$ is irreducible as a $\Gamma(G)$-module. $\square$

4 An arithmeticity criterion

In this section we fix a rational character $\chi \in X(\mathbb{Q}G)$. We therefore suppress the subscript χ and write D for D_χ and V for V_χ.

Proposition 3.1 tells us that $\Gamma(G) \subset U_2(V^\dagger)$ is an arithmetic subgroup which acts $\mathbb{Q}$-irreducibly on $\mathcal{H}^2(V^\dagger)$ and that, with a few exceptions, the group $U_2(V^\dagger)$ is of real rank ≥ 2.

Eichler transformations revisited Let M be (left) D-module of finite rank endowed with a nondegenerate skew-hermitian form $\langle -, - \rangle: M \times M \to D$. Given a D-submodule $N \subset M$, we denote by $U_M(N)$ the subgroup of the group of transformations that act trivially on $N^\perp$. This group preserves N and acts trivially on its radical $N_o = N \cap N^\perp$. Hence "restriction to N" defines a homomorphism $U_M(N) \to U(N)$. This homomorphism is easily shown to be onto. Its kernel consists of the unitary transformations that act trivially on $N + N^\perp$, and one checks that this is the image of $u(N_o)$ under T. We saw that the homomorphism $U(N) \to U(\overline{N})$ is also onto, and we identified its kernel with the vector

group $N_o^\dagger \otimes \overline{N}$. So the Levi quotient of $U_M(N)$ is $U(\overline{N})$ and its unipotent radical $R_u(U_M(N))$ is an extension of vector groups:

$$1 \to u(N_o) \xrightarrow{T} R_u(U_M(N)) \to N_o^\dagger \otimes_D \overline{N} \to 0.$$

As is clear from (1), this extension is usually nontrivial. If N_o is spanned by a single element c, then we can write this sequence as

(5) $$0 \to c \otimes D_+ c \xrightarrow{T} R_u(U_M(N)) \to c \otimes \overline{N} \to 0.$$

Any element of $R_u(U_M(N))$ is an Eichler transformation $E(c, a, \lambda)$ whose image in $c \otimes \overline{N}$ is $c \otimes \bar{a}$ (where $\bar{a} \in \overline{N}$ is the image of a). We will often use the following lemma:

Lemma 4.1 *Let $\Gamma \subset U_M(N)$ be a discrete subgroup whose image in $U(\overline{N})$ is arithmetic and which acts $\mathbb{Q}$-irreducibly in $\overline{N}$. If $\Gamma \cap R_u(U_M(N))$ contains an Eichler transformation $E(c, a, \lambda)$ with $a \in N \smallsetminus D_+ c$, then $\Gamma \cap U_M(N)$ is arithmetic in $U_M(N)$.*

Proof We are given that in the exact sequence of algebraic groups

$$1 \to R_u(U_M(N)) \to U_M(N) \to U(\overline{N}) \to 1,$$

the image $\overline{\Gamma}$ of Γ in $U(\overline{N})$ is arithmetic. Hence for Γ to be arithmetic, it suffices that $\Gamma \cap R_u(\mathrm{EU}_M(N))$ be a lattice. For this we turn to the exact sequence (5). The Eichler transformation $E(c, a, \lambda)$ has image $c \otimes \bar{a}$ in $c \otimes \overline{N}$, and this image is nonzero by assumption. The image of the Γ-conjugacy class of $E(c, a, \lambda)$ in $c \otimes \overline{N}$ is equal to $c \otimes \overline{\Gamma} \bar{a}$. Since our assumptions also imply that $\overline{\Gamma}$ acts $\mathbb{Q}$-irreducibly in $\overline{N}$, it follows that the image of $\Gamma \cap R_u(U_M(N))$ in $c \otimes \overline{N}$ is a lattice in $c \otimes \overline{N}$.

Next observe that if $E(c, a_1, \lambda_1)$ and $E(c, a_2, \lambda_2)$ lie in $\Gamma \cap R_u(U_M(N))$, then so does their commutator, which by the identity (1) is $T(c \otimes \lambda c)$ with $\lambda = \langle a_1, a_2 \rangle + \langle a_1, a_2 \rangle^\dagger$. Since the $\langle a_1, a_2 \rangle$ generate a lattice in D, it follows that the λ generate a lattice in D_+. In other words, the preimage of $\Gamma \cap R_u(U_M(N))$ in $c \otimes D_+ c$ is also a lattice. Hence $\Gamma \cap R_u(U_M(N))$ is a lattice. $\square$

Hyperbolic submodules If $j : \mathcal{H}^2(V^\dagger) \hookrightarrow M$ is an embedding of hermitian D-modules, then M is the orthogonal direct sum of the image of j and its perp (for $\mathcal{H}^2(V^\dagger)$ is nondegenerate), so that j gives rise to an injective homomorphism of groups $j_* : U_2(V^\dagger) \hookrightarrow U(M)$. Let us refer to such an embedding as a $V^\dagger$-*hyperbolic summand* in M.

The following criterion for arithmeticity will be central to our argument:

Theorem 4.2 *Let M be a nondegenerate skew-hermitian D-module of finite rank, and*

$$a : V^\dagger \hookrightarrow M, \quad \{b : V^\dagger \hookrightarrow M\}_{b \in \mathcal{B}}$$

*a collection of D-linear embeddings (with $\mathcal{B}$ finite and nonempty) whose images span M over D and are such that for each $b \in \mathcal{B}$, the pair (a, b) defines a hyperbolic summand of M. If $\dim_D V^\dagger = 1$ **and** $\dim_D M > 2$, assume in addition that there exist $b_1, b_2 \in \mathcal{B}$ for which $b_1(V^\dagger)$ and $b_2(V^\dagger)$ are perpendicular.*

Then the subgroup Γ of $U(M)$ generated by $\{(a, b)_* \Gamma(G)\}_{b \in \mathcal{B}}$ is an arithmetic subgroup of $U(M)$ which acts $\mathbb{Q}$-irreducibly in M.

The proof will be by induction on $\dim_D M$. As may be inferred from the statement of the theorem, the case when $\dim_D V^\dagger = 1$ is a bit more delicate. Indeed, the first induction step then requires special care and so we do that case first. Once we have dealt with it, we indicate how to modify the arguments in order to obtain a proof of the unrestricted version of Theorem 4.2.

Let us say that a D-subspace $N \subset M$ is Γ-*arithmetic* if $\Gamma \cap U_M(N)$ is arithmetic in $U_M(N)$ and acts $\mathbb{Q}$-irreducibly in $\overline{N}$ (the last property is a consequence of the first if the real rank of $U_M(N)$ is ≥ 2).

The case $\dim_D V^\dagger = 1$ We then identify $V^\dagger$ with D and a and each $b \in \mathcal{B}$ with the image of $1 \in D$ under these embeddings, so that $\langle a, b \rangle = 1$ for all $b \in \mathcal{B}$. Note that $\{a\} \cup \mathcal{B} \subset M$ consists of isotropic elements and generates M over D. We write $\Gamma(a, b)$ for the image of $\Gamma(G)$ under (a, b), so that Γ is generated by $\{\Gamma(a, b)\}_{b \in \mathcal{B}}$. As any $b \in \mathcal{B}$ lies in $\Gamma(a, b)a$, it follows that $\{a\} \cup \mathcal{B} \subset \Gamma a$.

By Proposition 3.1, $Da + Db$ is Γ-arithmetic for every $b \in \mathcal{B}$. We therefore assume that M is not of the form $Da + Db$. So there exist $b_1, b_2 \in \mathcal{B}$ with $b_2 \notin Da + Db_1$ such that $\langle b_1, b_2 \rangle = 0$.

Lemma 4.3 *Put $N := Da + Db_1$. Then $N' := N + Db_2$ is Γ-arithmetic.*

Proof We verify that the assumptions of Lemma 4.1 are satisfied by $\Gamma \cap U_M(N')$. It is clear that the radical of N' is spanned by $c := b_2 - b_1$, so that $\overline{N}'$ is the isomorphic image of N. We know that N is Γ-arithmetic and so Γ has arithmetic image in $U(\overline{N}')$. Since T_{b_1} and T_{b_2} lie in Γ, so does $T_{b_2} T_{b_1}^{-1}$. We check that

$$T_{b_2} T_{b_1}^{-1}(x) = x - \langle x, b_1 \rangle + \langle x, b_1 + c \rangle (b_1 + c) = E(c, b_1, 1)(x).$$

So the image of $\Gamma \cap R_u(U_M(N'))$ in $c \otimes \overline{N}'$ contains $c \otimes b_1$. Now apply Lemma 4.1. $\qquad\square$

From this point onward the argument will be inductive. The union of Lemmas 4.4 and 4.5 will establish the theorem in the case $\dim_D V^\dagger = 1$.

Lemma 4.4 *Let $N \subsetneq M$ be a D-subspace which contains a, b_1 and b_2, and whose radical is of D-dimension one. If N is Γ-arithmetic, then there exists a $b \in \mathcal{B}$ such that $N' := N + Db$ is nondegenerate and Γ-arithmetic, and the real rank of $U(N')$ is ≥ 2.*

Proof Let $c \in N$ span the radical of N. Since M is nondegenerate and D-spanned by $\{a\} \cup \mathcal{B}$, there must exist a $b \in \mathcal{B}$ such that c is not in the radical of $N' := N + Db$. Then it is easily seen that N' is nondegenerate, so that $U_M(N') \cong U(N')$. In the case $N = Da + Db_1 + Db_2$ (where we can take $c = b_2 - b_1$), one checks that N is the perpendicular sum of two copies of $\mathcal{H}^2(D)$. Otherwise, N' contains such a sum. This implies that $U(N')$ has real rank ≥ 2.

The $U(N')$-stabilizer $U(N')_c$ of c is equal to $U_M(N)$ and hence contains $\Gamma \cap U(N')_c$ as an arithmetic subgroup. Observe that $c' := T_b(c) = c + \langle c, b \rangle b$ is another isotropic element with $\langle c', c \rangle = \langle c, b \rangle \langle b, c \rangle \neq 0$, and so $Dc + Dc' \cong \mathcal{H}^2(D)$. The two $U(N')$-stabilizers of Dc and Dc' are opposite parabolic subgroups of $U(N')$ whose unipotent radicals are contained in $U(N')_c$ and $U(N')_{c'}$, respectively. Since $U(N')_{c'}$ is a Γ-conjugate of $U(N')_c$, it follows that $\Gamma \cap U(N')_{c'}$ is an arithmetic subgroup of $U(N')_{c'}$. We have thus satisfied the hypotheses of Theorem 3.3 and we conclude that $\Gamma \cap U(N')$ is arithmetic in $U(N')$. The fact that $\Gamma \cap U(N')$ acts $\mathbb{Q}$-irreducibly in N' follows from the fact that $\Gamma \cap U(N)$ has this property in N, for the $(\Gamma \cap U(N'))$-translates of N span N' over $\mathbb{Q}$, but do not decompose N'. $\square$

Lemma 4.5 *Let $N \subsetneq M$ be a proper nondegenerate D-subspace of dimension ≥ 4 and contain a, b_1 and b_2. If N is Γ-arithmetic, then so is $N' := N + Db'$ for every $b' \in \mathcal{B} \smallsetminus N$.*

Proof when N' is degenerate We verify that the assumptions of Lemma 4.1 are satisfied by $\Gamma \cap U_M(N')$. The radical of N' is necessarily spanned by an element of the form $c := b' - b$, where $b \in N$ is characterized by the property that $\langle x, b \rangle = \langle x, b' \rangle$ for all $x \in N$. So N maps isomorphically onto $N'/Dc = \overline{N}'$. In particular, the natural map $U(N) \to U(\overline{N}')$ is an isomorphism, and hence $\Gamma \cap U_M(N')$ maps onto an arithmetic subgroup of $U(\overline{N}')$.

Let n be a positive integer such that $T_b^n \in \Gamma$. Then

$$T_{b'}^n T_b^{-n}(x) = x - n\langle x, b \rangle b + n\langle x, b' \rangle b' = x + n\langle x, b \rangle c + n\langle x, c \rangle b + n\langle x, c \rangle c = E(c, nb, n)(x).$$

So $E(c, nb, n) \in \Gamma \cap R_u(U_M(N'))$ and this element has image $c \otimes nb$ in $c \otimes \overline{N}'$. It then follows from Lemma 4.1 that N' is Γ-arithmetic. $\square$

Proof when N' is nondegenerate Then $N_1' := N' \cap b'^\perp$ is degenerate with radical spanned by b'. We first prove that N_1' is Γ-arithmetic by verifying the assumptions of Lemma 4.1. The subspace $N_1 := N \cap b'^\perp$ supplements b' in N_1'. It is therefore nondegenerate and maps isomorphically onto $\overline{N}_1' = N_1'/Db'$. This enables us to regard $U(N_1)$ as a subgroup of $U_M(N_1')$ that acts trivially on both b' and its orthogonal projection in N.

Since $\Gamma \cap U_M(N)$ is arithmetic in $U_M(N)$, its subgroup $\Gamma \cap U(N_1)$ is arithmetic in $U(N_1)$ and has arithmetic image in $U(\overline{N}_1')$. We show that $E(b', c') \in \Gamma$ for some $c' \in N_1' \smallsetminus Db'$. Then Lemma 4.1 will imply that N_1' is Γ-arithmetic.

For this we recall that $c := b_2 - b_1$ is perpendicular to b_1 and has nonzero image in $Db_1^\perp/Db_1$. Let $\gamma \in \Gamma(a, b')\Gamma(a, b_1) \subset \Gamma(N')$ take b_1 to b'. Since c is perpendicular to b_1, $c' := \gamma(c) \in N'$ is perpendicular to $\gamma(b_1) = b'$ (so lies in N_1') and has nonzero image $[c']$ in $\overline{N}_1' \cong N_1$. Since $E(b', c') = E(c', b')^{-1}$ is a Γ-conjugate of $E(c, b_1)^{-1}$, it lies in Γ.

Now $U(N')_{b'} = U(N' \cap b'^\perp)$ and so $\Gamma \cap U(N')_{b'}$ is arithmetic in $U(N')_{b'}$. As $a \in \Gamma b'$, the same is true for $\Gamma \cap U(N')_a$. Since a and b' span a copy of $\mathcal{H}^2(D)$, their $U(N')$-stabilizers contain the unipotent radicals of opposite parabolic subgroups of $U(N')$. The real rank of $U(N')$ is ≥ 2, so Theorem 3.3 applies and tells us that N' is Γ-arithmetic. $\square$

The case when $\dim_D V^{\dagger} > 1$ The same scheme works when $\dim_D V^{\dagger} > 1$. The difference is that we deal with larger hyperbolic packets, to wit, the images of hyperbolic embeddings $(a, b) : \mathcal{H}^2(V^{\dagger}) \hookrightarrow M$. The essential difference is that we start off in a better position, since we begin with a $V^{\dagger}$-hyperbolic embedding $j : \mathcal{H}^2(V^{\dagger}) \hookrightarrow M$ and we already know that its image N is Γ-arithmetic and that $U_M(N) \cong U(N)$ has real rank ≥ 2.

5   Finding liftable mapping classes

In this section the G-covering $S \to S_G$ is as in the introduction and $A \subset S_G^{\circ}$ is a nonempty closed one-submanifold such that the covering is trivial over A and is connected over $S \smallsetminus A$. We also choose a connected component α of A, so that $A' := A \smallsetminus \alpha$ might be empty. We orient α and regard it as the oriented image of an embedding of the circle in S_G°. We will see that this gives rise to enough copies of $\Gamma(G)$ in the representation of the G-equivariant mapping classes as to satisfy the hypotheses of our arithmeticity criterion, Theorem 4.2.

We denote by $S_G(\alpha)$ the singular surface obtained from S_G by contracting α to a point (that we will denote by ∞). Its topological normalization is a closed connected surface, denoted by $\hat{S}_G(\alpha)$, whose genus is one less than that of S_G. The surface $\hat{S}_G(\alpha)$ comes with two points over ∞ and the orientation of α enables us to tell them apart: we let p_- be "to the left" of α and p_+ be "to the right" of α. If we regard A' also as a submanifold of $\hat{S}_G^{\circ}(\alpha)$, then the surjection $\hat{S}_G^{\circ}(\alpha) \to S_G^{\circ}(\alpha)$ defines a map from the set $\Pi(\hat{S}_G^{\circ}(\alpha) \smallsetminus A'; p_-, p_+)$ of path homotopy classes in $\hat{S}_G^{\circ}(\alpha) \smallsetminus A'$ from p_- to p_+ to the fundamental group $\pi_1(S_G^{\circ}(\alpha), \infty)$. This map is injective. We do the same (in a G-equivariant manner) for the preimage of $S_G \smallsetminus \alpha$ in S, and thus get G-covers $S(\alpha) \to S_G(\alpha)$ and $\hat{S}^{\circ}(\alpha) \to \hat{S}_G(\alpha)$, and G-orbits $P_{\infty} \subset S(\alpha)^{\circ}$ and $P_{\pm} \subset \hat{S}^{\circ}(\alpha)$, so that we end up with the diagram below (in which the vertical maps are G-coverings):
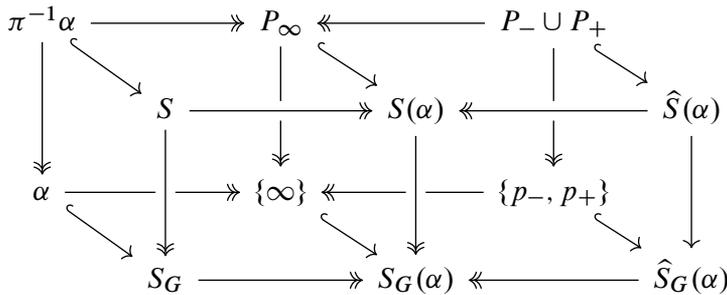
This construction comes with G-equivariant bijections $P_- \cong P_{\infty} \cong P_+$. Our assumption on the covering $S \to S_G$ amounts to the properties that $\hat{S}(\alpha)$ is connected and stays so if we remove the preimage of A', and the three G-orbits P_{∞} and $P_{\pm}$ are regular. So the choice of a point in P_{∞} (which is equivalent to the choice of a lift $\tilde{\alpha}$ of α) identifies these G-sets with G (on which G acts by left translation). In particular, we thus identify $\mathrm{Iso}_G(P_-, P_+) \cong \mathrm{Aut}_G(P_{\infty})$ with G (where $g \in G$ acts on G by right translation over g^{-1}).
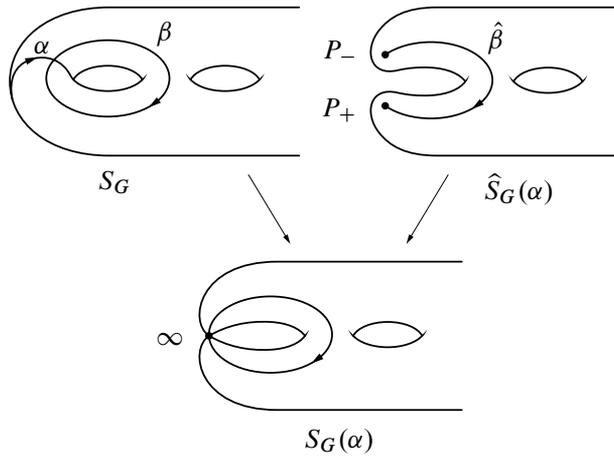
Figure 1: The surface S_G, its quotient $S_G(\alpha)$ and the normalization $\widehat{S}_G(\alpha)$.

For any path in $\widehat{S}_G^\circ(\alpha) \smallsetminus A'$ from p_- to p_+, the G covering is trivial over it, so that we have an associated G-bijection $P_- \cong P_+$. Since the G-covering over $\widehat{S}_G^\circ(\alpha) \smallsetminus A'$ is connected, the resulting map

$$\Pi(\widehat{S}_G^\circ(\alpha) \smallsetminus A'; p_-, p_+) \to \mathrm{Iso}_G(P_-, P_+) \cong \mathrm{Aut}_G(P_\infty)$$

is onto by standard covering theory. We will say that an element of $\Pi(\widehat{S}_G^\circ(\alpha) \smallsetminus A'; p_-, p_+)$ is *G-trivial* if its image in $\mathrm{Aut}_G(P_\infty)$ under the above map is the identity. Such elements make up a coset for the kernel of the natural homomorphism $\pi_1(\widehat{S}_G^\circ(\alpha) \smallsetminus A', p_-) \to G$.

Lemma 5.1 *Every element of $\Pi(\widehat{S}_G^\circ(\alpha) \smallsetminus A'; p_-, p_+)$ is representable by some arc (ie some embedded unit interval) in $\widehat{S}_G^\circ(\alpha) \smallsetminus A'$ from p_- to p_+. We can arrange that this arc lifts to an embedding of the circle $\mathbb{R}/\mathbb{Z}$ in S_G° which meets α in a single point with intersection number one. In particular, every element of $\mathrm{Aut}_G(P)$ is realized by the monodromy along an embedded circle β which does not meet A', and meets α in one point only and does so transversally with intersection number one.*

Proof We first represent the homotopy class by an immersion of the unit interval with only transverse self-intersections. That number of self-intersections is finite and if this number is positive, we lower it by moving the last point of self-intersection towards p_+ and then slide the path over p_+. By iterating this procedure we obtain a representative which is an embedding. It is clear that we can make this arc lift to an embedded circle. The second assertion then follows. $\qquad\square$

We choose a lift $\tilde{\alpha}$ of α and write $a \in H_1(S)$ for its homology class. Since Ra is an isotropic sublattice of $H_1(S)$, we have that $\langle a, a \rangle = 0$. We let $I \subset H_1(S)$ be the homology supported by the preimage of A'; this is a free R-submodule (where as before, $R = \mathbb{Z}G$) with a generator for every connected component of A'. It is clear that $Ra + I$ is isotropic. We saw that the lift $\tilde{\alpha}$ identifies $\mathrm{Aut}_G(P)$ with the group G with G acting on itself by right translations. Lemma 5.1 above shows that all such elements are obtained from a loop of the type described there. From that lemma we also derive:

Corollary 5.2 *Let $b \in I^{\perp}$ be such that $a \cdot b = 1$ and $ga \cdot b = 0$ for $g \in G \smallsetminus \{1\}$. Then some $b' \in b + Ra$ can be represented by a lift of an embedded circle β in $S_G^{\circ} \smallsetminus A'$ which meets α transversally at a unique point (and for which necessarily $\alpha \cdot \beta = 1$). In particular, b' is R-isotropic and the R-linear map defined by*

$$\mathcal{H}^2(R) \to I^{\perp}, \qquad \boldsymbol{e} \mapsto a, \quad \boldsymbol{f} \mapsto b',$$

is an embedding of skew-hermitian R-modules whose orthogonal complement supplements its image; we obtain a basic hyperbolic summand of the R-module $H_1(S)$.

Proof It is not difficult to see that the homology class b is representable by a map from the circle to S° which meets the preimage of α exactly once (and hence in a point of $\tilde{\alpha}$) and does not meet the preimage of A'. We apply Lemma 5.1 to its image in $S_G^{\circ} \smallsetminus A'$, or rather to the resulting arc in $\hat{S}_G^{\circ}(\alpha) \smallsetminus A'$ which connects p_- with p_+; this then produces an embedding β of the circle in $S_G^{\circ} \smallsetminus A'$ which meets α only once and with intersection number one over which the G-covering is trivial. The lift $\tilde{\beta}$ of β which meets $\tilde{\alpha}$ defines a homology class b' which differs from b by a class supported by the preimage of α, that is, an element of Ra.

The proof of the last paragraph is straightforward.   □

Let us call an ordered pair (a, b) in $H_1(S)$ *R-hyperbolic* if $\langle a, a \rangle = \langle b, b \rangle = 0$ and $\langle a, b \rangle = 1$. Such a pair defines a basic hyperbolic summand $Ra + Rb \subset H_1(S)$ and gives rise to an embedding of $\Gamma(G)$ in $\mathrm{Sp}(H_1(S))^G$. We shall denote the latter's image by $\Gamma(a, b)$ and the image of $\Gamma_o(G)$ by $\Gamma_o(a, b)$. We write $\mathcal{B}_a$ for the set of $b \in H_1(S)$ for which the pair (a, b) is R-hyperbolic, and $\Gamma_o(a)$ and $\Gamma(a)$ for the subgroups of $\mathrm{Sp}(H_1(S))^G$ generated by its subgroups $\Gamma_o(a, b)$ and $\Gamma(a, b)$, respectively, with $b \in \mathcal{B}_a$.

Fix a basepoint p on α and write $\tilde{p}$ for its preimage in $\tilde{\alpha}$.

Let $h \in G$ and regard h as an element of $\mathrm{Aut}_G(P)$. Let β be as in Lemma 5.1, which we may (and will) assume to meet α in p such that the lift $\tilde{\beta}$ of β (as an arc) begins in $\tilde{p}$ ends in $h\tilde{p}$. Let S_G^{β} be a closed regular neighborhood of $\alpha \cup \beta$ in $S_G^{\circ} \smallsetminus A'$. This is a compact genus-one surface whose boundary ∂S_G^{β} is connected. The homotopy class of this boundary (with its natural orientation) is in the free homotopy class of the commutator $[\beta]^{-1}[\alpha]^{-1}[\beta][\alpha]$ — we write path composition functorially, so the order of travel is read from right to left. This commutator has trivial image in G (since $[\alpha]$ has), and so the G-covering $S \to S_G$ is trivial over ∂S_G^{β}. The preimage of ∂S_G^{β} in S is the boundary of the preimage S^{β} of S_G^{β} and the Dehn twist along ∂S_G^{β} lifts in a G-equivariant manner to a multi-Dehn twist D^{β} along that boundary. The following lemma generalizes one of the constructions given in [3] for the case when G is cyclic (in that paper they are depicted as Figures 2 and 3).

Lemma 5.3 *The multi-Dehn twist D^{β} acts on $H_1(S)$ as $T_a(2 - e_h - e_h^{\dagger})$ (where we use formula (2), noting that $2 - e_h - e_h^{\dagger} \in R_+$).*

Proof The lift of the commutator $[\beta]^{-1}[\alpha]^{-1}[\beta][\alpha]$ that passes through $\tilde{p}$ first traverses the embedded circle $\tilde{\alpha}$, then traverses $\tilde{\beta}$, then traverses the circle $h\tilde{\alpha}$ in the opposite direction and then returns via the inverse of $\tilde{\beta}$ to $\tilde{p}$. So the homology class of this lift of the commutator (and hence of the corresponding lift of ∂S_G^β) is $a - ha$. If we replace $\tilde{p}$ by $g\tilde{p}$ with $g \in G$, then this replaces a by ga and h by ghg^{-1}, so that the corresponding class is $ga - gha = g(1-h)a$. By a standard formula, the resulting action on $H_1(S)$ is given by

$$D_*^\beta(x) = x + \sum_{g \in G} (x \cdot g(1-h)a)g(1-h)a$$

$$= x + \sum_{g \in G} ((x \cdot ga)ga - (x \cdot gha)ga - (x \cdot ga)gha + (x \cdot gha)gha)$$

$$= x + 2\langle x, a \rangle a - \langle x, ha \rangle a - \langle x, a \rangle ha = T_a(2 - e_h - e_h^\dagger)(x). \qquad \square$$

Proposition 5.4 Let $b \in H_1(S)$ be such that (a, b) is an R-hyperbolic pair. Then the image of $\mathrm{Diff}^+(S)^G \to \mathrm{Sp}(H_1(S))^G$ contains $\Gamma(a, b)$.

Proof We first show this for $\Gamma_0(a, b)$. Let β be as in Corollary 5.2 (and thus represent an element of $b + Ra$). The diffeomorphisms of S_G with support in the interior of S_G^β have, as their image in the mapping class group of S_G, a centrally extended copy of $\mathrm{SL}(2, \mathbb{Z})$ with the central subgroup generated by the Dehn twist along the boundary of S_G^β. This Dehn twist acts trivially on $H_1(S_G^\beta)$. These diffeomorphisms lift to diffeomorphisms of S with support in S^β with the central subgroup acting trivially on $H_1(S)$. We thus obtain in the image of $\mathrm{Diff}^+(S)^G \to \mathrm{Sp}(H_1(S))^G$ a copy of $\mathrm{SL}_2(\mathbb{Z})$.

The multi-Dehn twist associated to α acts on $H_1(S)$ as $x \mapsto x + \sum_{g \in G} (x \cdot ga)ga = x + \langle x, a \rangle a = T_a(1)(x)$. By Lemma 5.3 the image of $\mathrm{Diff}^+(S)^G \to \mathrm{Sp}(H_1(S))^G$ also contains the transvections $T_a(2 - e_h - e_h^\dagger)$ for all $h \in G$. Hence that image contains all of $T_a(R_{++})$. This proves that the image of $\mathrm{Diff}^+(S)^G \to \mathrm{Sp}(H_1(S))^G$ contains $\Gamma_o(a, b)$.
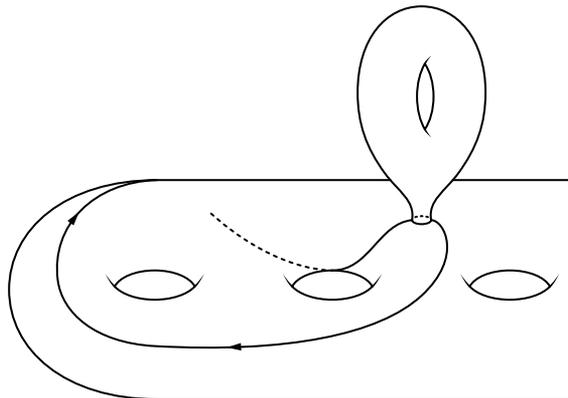
Figure 2: Point pushing (or rather, "small circle pushing") the genus-one surface S^β along S_G/S_G^β.

So it remains to show that the image of G in $\Gamma(a,b)$ is realized by $\mathrm{Diff}^+(S)^G$. For this we use mapping classes of *push type*. Consider the smooth surface S_G/S_G^β that is obtained as a quotient of S_G by contracting S_G^β to a point (that we shall call q). If we do the same for the connected components of S^β in G we get a G-cover $S/\!/S^\beta \to S_G/S_G^\beta$ fitting in the commutative diagram

$$
\begin{array}{ccc}
S & \longrightarrow & S/\!/S^\beta \\
{\scriptstyle G}\downarrow & & \downarrow{\scriptstyle G} \\
S_G & \longrightarrow & S_G/S_G^\beta
\end{array}
$$

The covering on the right does not branch over q, and so its preimage Q in $S/\!/S^\beta$ is a regular G-orbit. For every $g \in G$ there is a closed loop γ of S_G/S_G^β based at q which avoids branch points and induces in Q right multiplication by g. The corresponding point-pushing map on S_G/S_G^β (chosen to fix branch points) lifts to a G-equivariant diffeomorphism φ of $S/\!/S^\beta$ that extends this permutation.

Such a point-pushing map is isotopic to the identity on S_G/S_G^β, and hence the same is true for its lift φ. In particular, φ acts trivially on $H_1(S/\!/S^\beta)$. It is not difficult to see that the point-pushing map and its lift φ can be "lifted" to S and S_G by "small circle pushing". Since $H_1(S\smallsetminus S^\beta, \partial(S\smallsetminus S^\beta)) \to H^1(S/\!/S^\beta)$ is an isomorphism, the action on $H_1(S\smallsetminus S^\beta, \partial(S\smallsetminus S^\beta))$ will be trivial. Clearly the components of S_β will be permuted according to the right action of g, and thus $g \in \Gamma(a,b)$ is realized in the image of $\mathrm{Diff}^+(S)^G$. □

Part (ii) of the corollary below establishes the Putman–Wieland property of Theorem 1.1.

Corollary 5.5 (hyperbolic generation) *The following properties hold*:

(i) *The subset $\{a\} \cup \mathcal{B}_a$ of $H_1(S;\mathbb{Q})$ spans the latter over $\mathbb{Q}G$.*

(ii) *The subgroup $\Gamma_o(a)$ of $\mathrm{Sp}(H_1(S))$ generated by the subgroups $\Gamma_o(a,b)$ with $b \in \mathcal{B}_a$ (and hence $\mathrm{Diff}^+(S)^G$) has no nonzero finite orbit in $H_1(S)$.*

Proof Let $c \in H_1(S;\mathbb{Q})$ be perpendicular to $\{a\}\cup\mathcal{B}_a$. We prove that c is then perpendicular to every $x \in H_1(S)$; since the intersection form is nondegenerate, this will imply that $c = 0$ and hence that the $\mathbb{Z}G$-submodule of $H_1(S)$ generated by $\{a\}\cup\mathcal{B}_a$ is of finite index. To this end, let $b \in \mathcal{B}_a$. Then $x' := (1 + \langle x,a\rangle)b + x$ has the property that $\langle a, x'\rangle = 1$. By Corollary 5.2 (a,x'') is a hyperbolic pair for some $x'' \in x' + Ra$, so that $0 = \langle x'', c\rangle = \langle x, c\rangle$.

For (ii) it suffices to show that for every finite-index subgroup $\Gamma \subset \Gamma_o(a)$, the fixed part $H_1(S)^\Gamma$ is trivial. Note that $H_1(S)^{\Gamma_o(a,b)}$ is the perp of $Ra + Rb$ in $H_1(S)$ with respect to the intersection pairing. The $\Gamma_o(a,b)$-invariant part of $H_1(S)$ is not changed if we replace $\Gamma_o(a,b)$ by the finite-index subgroup $\Gamma \cap \Gamma_o(a,b)$, and hence $H_1(S)^\Gamma$ is perpendicular to $Ra + Rb$. As this is true for all $b \in \mathcal{B}_a$ and $\{a\}\cup\mathcal{B}_a$ generates $H_1(S)$ as an R-module, it follows that $H_1(S)^\Gamma$ must be trivial. □

We can now finish the proof of our main theorem.

Proof of Theorem 1.1 Let us denote the image of $\mathrm{Diff}^+(M)^G$ in $\mathrm{Sp}(H_1(S;\mathbb{Q}))^G$ by Γ and the image of the latter in the factor $U(H_1(S)[\chi])$ of $\mathrm{Sp}(H_1(S;\mathbb{Q}))^G = \prod_\chi U(H_1(S)[\chi])$ by Γ_χ. By combining Corollary 5.5 with Theorem 4.2, we see that under the assumptions of (ii), Γ_χ is an arithmetic subgroup of $U(H_1(S)[\chi])$.

Note that $\Gamma^\chi := \Gamma \cap \mathrm{EU}(H_1(S)[\chi])$ is a normal subgroup of Γ_χ. It remains to see that Γ^χ is of finite index in Γ_χ. Since $\mathrm{EU}(H_1(S)[\chi])$ is almost simple and of real rank ≥ 2, it follows from a general result of Margulis [4, Assertion (A), Chapter VIII] that this is the case unless Γ^χ meets $\mathrm{EU}(H_1(S)[\chi])$ in the center. But Proposition 5.4 shows that Γ^χ contains a subgroup isomorphic to $\Gamma_o(\chi)$, and so this last possibility does not occur. $\square$

Remark 5.6 This argument shows that if we are in the setting of (i) (triviality of the cover over a genus-one subsurface of S_G), then Γ_χ is an arithmetic subgroup of $U(H_1(S)[\chi])$, unless $V_\chi^\dagger \cong D_\chi$ and the image of G in V_χ is of the type given in Proposition 3.1. Denote that image by G_χ and let G^χ stand for the kernel of $G \to G_\chi$. Since $H_1(S)[\chi]$ already arises on the G_χ-cover $S_{G^\chi} \to S_G$ in the sense that $H_1(S)[\chi] = H_1(S_{G^\chi})[\chi]$, we may for the arithmeticity question just as well focus on this intermediate cover.

In Proposition 3.1(i)–(ii), that is, when D_χ equals $\mathbb{Q}$, the Gaussian field or the Eisenstein field, then G_χ is a group of roots of unity and hence cyclic. When the genus of S_G is at least three, we can always find a closed subsurface of genus two over which the covering $S_{G^\chi} \to S_G$ is trivial, and so Γ_χ is then arithmetic. In the remaining cases, G_χ is a particular kind of Kleinian group. It might well be that a G_χ-cover is then also trivial over the complement of a genus-two subsurface of the quotient surface when the genus of the latter is ≥ 3. If true, then it would follow that Γ would always be arithmetic if the genus of S_G is at least three and the covering is trivial over a genus-one subsurface of S_G.

References

[1] **F Grunewald**, **M Larsen**, **A Lubotzky**, **J Malestein**, *Arithmetic quotients of the mapping class group*, Geom. Funct. Anal. 25 (2015) 1493–1542 MR Zbl

[2] **A J Hahn**, **O T O'Meara**, *The classical groups and K-theory*, Grundl. Math. Wissen. 291, Springer (1989) MR Zbl

[3] **E Looijenga**, *Prym representations of mapping class groups*, Geom. Dedicata 64 (1997) 69–83 MR Zbl

[4] **G A Margulis**, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Math. 17, Springer (1991) MR Zbl

[5] **D Mumford**, *Abelian varieties*, Tata Inst. Fund. Res. Stud. Math. 5, Oxford Univ. Press (1970) MR Zbl

[6] **A Putman**, **B Wieland**, *Abelian quotients of subgroups of the mappings class group and higher Prym representations*, J. Lond. Math. Soc. 88 (2013) 79–96 MR Zbl

[7] **M S Raghunathan**, *A note on generators for arithmetic subgroups of algebraic groups*, Pacific J. Math. 152 (1992) 365–373 MR Zbl

[8]   **T A Springer**, *Linear algebraic groups*, 2nd edition, Progr. Math. 9, Birkhäuser, Boston, MA (1998)   MR Zbl

[9]   **T N Venkataramana**, *On systems of generators of arithmetic subgroups of higher rank groups*, Pacific J. Math. 166 (1994) 193–212   MR   Zbl

[10]   **G E Wall**, *The structure of a unitary factor group*, Inst. Hautes Études Sci. Publ. Math. 1 (1959) 23   MR Zbl

Mathematics Department, University of Chicago
Chicago, IL, United States

Mathematisch Instituut, Universiteit Utrecht
Utrecht, Netherlands

`e.j.n.looijenga@uu.nl`

ALGEBRAIC & GEOMETRIC TOPOLOGY

msp.org/agt