Geometry & Topology 16 (2012) 1393–1411 **1393**

All finite groups are involved in the mapping class group

GREGOR MASBAUM
ALAN W REID

Let Γ_g denote the orientation-preserving mapping class group of the genus $g \geq 1$ closed orientable surface. In this paper we show that for fixed g, every finite group occurs as a quotient of a finite index subgroup of Γ_g.

20F38; 57R56

1 Introduction

Throughout this paper, Γ_g will denote the orientation-preserving mapping class group of the genus g closed orientable surface.

A group H is *involved* in a group G if there exists a finite index subgroup $K < G$ and an epimorphism from K onto H. The question as to whether every finite group is involved in Γ_g was raised by U Hamenstädt in her talk at the 2009 Georgia Topology Conference. The main result of this note is the following.

Theorem 1.1 *For all $g \geq 1$, every finite group is involved in Γ_g.*

Some comments are in order. When $g = 1$, $\Gamma_1 \cong \mathrm{SL}(2, \mathbf{Z})$ and in this case the result follows since $\mathrm{SL}(2, \mathbf{Z})$ contains free subgroups of finite index (of arbitrarily large rank). For the case of $g = 2$, it is known that Γ_2 is large (see Korkmaz [21]); that is to say, Γ_2 contains a finite index subgroup that surjects a free nonabelian group, and again the result follows. Thus, it suffices to deal with the case when $g \geq 3$.

Although Γ_g is well-known to be residually finite by Grossman [18], and therefore has a rich supply of finite quotients, apart from those finite quotients obtained from

$$\Gamma_g \to \mathrm{Sp}(2g, \mathbf{Z}) \to \mathrm{Sp}(2g, \mathbf{Z}/N\mathbf{Z}),$$

very little seems known explicitly about what finite groups can arise as quotients of Γ_g (or of subgroups of finite index). Some constructions of finite quotients of finite index subgroups of Γ_g do appear in the literature; for example, in Dunfield and Thurston [10], Funar and Pitsch [13] and Looijenga [25]. In particular, the constructions

Published: 24 July 2012 DOI: 10.2140/gt.2012.16.1393

in [25] using Prym representations associated to finite abelian overs of surfaces can be used to construct finite quotients that are similar in spirit to what is done here. Further information about the structure of finite index subgroups of Γ_g is contained in Berrick, Gebhardt and Paris [4] where the minimal index of a proper subgroup of Γ_g is computed.

Theorem 1.1 will follow (see Section 4) from our next result which gives many new finite simple groups of Lie type as quotients of Γ_g. Throughout the paper, $\mathbf{F}_q$ will denote a finite field of order q, and $\mathrm{SL}(N,q)$ (resp. $\mathrm{PSL}(N,q)$) will denote the finite group $\mathrm{SL}(N,\mathbf{F}_q)$ (resp. $\mathrm{PSL}(N,\mathbf{F}_q)$).

Theorem 1.2 *For each $g \geq 3$, there exist infinitely many N such that for each such N, there exist infinitely many primes q such that Γ_g surjects $\mathrm{PSL}(N,q)$.*

In addition we show that Theorem 1.2 also holds for the Torelli group (with $g \geq 2$).

It is worth emphasizing that one cannot expect to prove Theorem 1.1 simply using the subgroup structure of the groups $\mathrm{Sp}(2g,\mathbf{Z}/N\mathbf{Z})$. The reason for this is that since $\mathrm{Sp}(2g,\mathbf{Z})$ has the Congruence Subgroup Property (see Bass, Milnor and Serre [2]), it is well-known that not all finite groups are involved in $\mathrm{Sp}(2g,\mathbf{Z})$ (see Long and Reid [24, Chapter 4.0], for example).

An interesting feature of the proof of Theorem 1.1 is that it exploits the unitary representations arising in Topological Quantum Field Theory (TQFT) first constructed by Reshetikhin and Turaev [34]. We actually use the so-called SO(3)–TQFT following the skein-theoretical approach of Blanchet, Habegger, Masbaum and Vogel [5] (see Section 3 for a brief resumé of this).

We briefly indicate the strategy of the proof of Theorem 1.2. The unitary representations that we consider are indexed by primes p congruent to 3 modulo 4. For each such p we exhibit a group Δ_g which is the image of a certain central extension $\widetilde{\Gamma}_g$ of Γ_g and satisfies

$$\Delta_g \subset \mathrm{SL}(N_p, \mathbf{Z}[\zeta_p]),$$

where ζ_p is a primitive p–th root of unity, and $\mathbf{Z}[\zeta_p]$ is the ring of integers in $\mathbf{Q}(\zeta_p)$. Moreover, the dimension $N_p \to \infty$ as we vary p. The key part of the proof is the following. We exhibit infinitely many rational primes q, and prime ideals $\widetilde{q} \subset \mathbf{Z}[\zeta_p]$ satisfying $\mathbf{Z}[\zeta_p]/\widetilde{q} \simeq \mathbf{F}_q$, for which the reduction homomorphism $\pi_{\widetilde{q}}$ from $\mathrm{SL}(N_p,\mathbf{Z}[\zeta_p])$ to $\mathrm{SL}(N_p,q)$ (induced by the isomorphism $\mathbf{Z}[\zeta_p]/\widetilde{q} \simeq \mathbf{F}_q$) restricts to a surjection $\Delta_g \twoheadrightarrow \mathrm{SL}(N_p,q)$.

From this, it is then easy to get surjections $\Gamma_g \twoheadrightarrow \mathrm{PSL}(N_p,q)$, which will complete the proof. The details of how all of this is achieved are given in Section 4.

The paper is organized as follows. In Section 2 we collect some background on algebraic and arithmetic subgroups of (special) unitary groups, as well as what is needed for us from Strong Approximation. This is all well-known, but we include this to help make the paper more self-contained. In Section 3 we discuss the (projective) unitary representations of Γ_g arising from SO(3)–TQFT and a density result for these representations due to Larsen and Wang [22]. In Section 4 we put the pieces together to prove Theorem 1.1 and Theorem 1.2 following the strategy outlined above. Finally, in Section 5 we make some additional comments about Theorem 1.1, in particular, how Theorem 1.1 is perhaps reflective of some more "rank 1" phenomena for Γ_g.

Acknowledgements The authors wish to thank the organizers of two conferences in June 2009 at which they first began thinking about this problem: "From Braid groups to Teichmüller spaces", and "On Interactions between Hyperbolic Geometry, Quantum Topology and Number Theory" at CIRM Luminy and Columbia University respectively. We also wish to thank Ian Agol, Mathieu Florence and Matt Stover for helpful conversations. We would particularly like to thank Gopal Prasad who helped enormously in clarifying various points about algebraic groups, their k–forms and fields of definition that are used in Section 4. The second author thanks Max Planck Institute for Mathematics for its hospitality whilst working on this.

The second author was partially supported by the NSF.

Remark 1.3 Whilst in the process of completing the writing of this paper we have learned that similar results have recently been proved by Funar [12].

2 Algebraic and arithmetic aspects of unitary groups

It will be convenient to recall some of the basic background of unitary groups, algebraic groups arising from Hermitian forms (over number fields, local fields and finite fields), their arithmetic subgroups, and some aspects of the Zariski topology that we will make use of.

We begin by fixing some notation. Throughout this paper we will fix p to be an odd prime, which will be assumed congruent to 3 modulo 4 from Section 3 on. Let $\zeta = \zeta_p$ denote a primitive p–th root of unity, K_p (or simply K if no confusion will arise) will denote the cyclotomic field $\mathbf{Q}(\zeta)$ and $\mathcal{O}_K$ its ring of integers. We will let the maximal real subfield of K_p be denoted by $k = k_p$, with corresponding ring of integers $\mathcal{O}_k$. We will assume that these fields always come with a specific embedding into $\mathbf{C}$. K_p is a totally imaginary quadratic extension of the totally real field k_p, and both are Galois extensions of $\mathbf{Q}$.

If $G < \mathrm{GL}(m, \mathbf{C})$ is an algebraic group, and $R \subset \mathbf{C}$ is a subring then we will denote the R–points of G by $G(R) = G \cap \mathrm{GL}(m, R)$. We will identify G with its complex points.

2.1

For more details about the material covered in this section, see Platonov and Rapinchuk [33] and Shimura [35; 36].

First, consider the extension of fields K/k. Fixing an embedding of $K \subset \mathbf{C}$, complex conjugation induces a Galois automorphism of K fixing k (since $\overline{\zeta} = \zeta^{-1}$).

Now K/k has a k–basis $\{1, \zeta\}$, and for $\alpha \in K$, we can express the k–linear map $L_z(\alpha) = z\alpha$ in terms of the above basis. If $z = a + b\zeta$ with $a, b \in k$ then L_z is represented by the following element of $M(2, k)$:

$$L_z = \begin{pmatrix} a & -b \\ b & a + bt \end{pmatrix},$$

where $t = \zeta + \zeta^{-1}$. Extending the k–linear map L in the obvious way, it follows that $\mathrm{SL}(N, K)$ may be embedded in $\mathrm{GL}(2N, \mathbf{C})$ as an algebraic group defined over k. Clearly, $\mathrm{SL}(N, K)$ maps into $\mathrm{SL}(2N, k)$. Furthermore, since $\{1, \zeta\}$ generates $\mathcal{O}_K$ over $\mathcal{O}_k$, then $\mathrm{SL}(N, \mathcal{O}_K)$ maps into $\mathrm{SL}(2N, \mathcal{O}_k)$.

Let $V = K^N$ and H a nondegenerate Hermitian form on V. The *special unitary group*

$$\mathrm{SU}(V, H) = \{A \in \mathrm{SL}(N, \mathbf{C}) : \overline{A}^t H A = H\}$$

also has the structure of an algebraic group defined over k (where $\overline{A}$ denotes complex conjugation of matrices.) This is because $L_{\overline{z}}$ is represented by the matrix

$$L_{\overline{z}} = \begin{pmatrix} a + bt & b \\ -b & a \end{pmatrix}$$

so that when we embed K into $M_2(k)$ using the map L, complex conjugation becomes the restriction of a self-map of $M_2(k)$ defined over k.

We will denote this algebraic group by $\mathcal{G}$, and we will frequently blur the distinction between $\mathrm{SU}(V, H)$ and $\mathcal{G}$.

The group $\mathrm{SU}(V, H; \mathcal{O}_K) = \mathrm{SU}(V, H) \cap \mathrm{SL}(N, \mathcal{O}_K)$ embeds in $\mathrm{SL}(2N, k)$ as a subgroup commensurable with $\mathcal{G}(\mathcal{O}_k)$. Indeed, in this case, using the remark above regarding the image of $\mathrm{SL}(N, \mathcal{O}_K)$, we deduce that the image of $\mathrm{SU}(V, H; \mathcal{O}_K)$ is actually equal to $\mathcal{G}(\mathcal{O}_k)$. Denoting this image group by Γ, then Γ is an arithmetic subgroup of a product $\mathbf{SU} = \mathrm{SU}(p_1, q_1) \times \cdots \times \mathrm{SU}(p_s, q_s)$, of special unitary groups

that arise from $\mathrm{SU}(V,H)$ in the following way (see Borel and Harish-Chandra [8] and Shimura [35] for more details). Let $\sigma_1,\dots\sigma_d$ denote the Galois embeddings of $k\hookrightarrow\mathbf{R}$ (with σ_1 chosen to be the identity embedding). We will that assume that at σ_1,

$$\mathrm{SU}(V,H;\mathbf{R})=\mathcal{G}(\mathbf{R})\cong\mathrm{SU}(p_1,q_1),$$

where $p_1+q_1=N$ and $p_1,q_1>0$. Applying a Galois embedding σ_i to $\mathcal{G}$ produces an algebraic group defined over $\sigma_i(k)=k$ whose real points thereby determine another special unitary group of some signature. Assume that for $i=1,\dots,s$ this special unitary group, denoted by $\mathrm{SU}(p_i,q_i)$, is not isomorphic to $\mathrm{SU}(N)$ (ie, is noncompact) and for $i=s+1,\dots,r$ the special unitary group is isomorphic to $\mathrm{SU}(N)$. The theory of arithmetic groups then shows that Γ is an arithmetic subgroup of $\mathbf{SU}=\mathrm{SU}(p_1,q_1)\times\cdots\times\mathrm{SU}(p_s,q_s)$. Thus $\mathbf{SU}/\Gamma$ has finite volume, and moreover, if $s\neq r$, the quotient $\mathbf{SU}/\Gamma$ is compact, or equivalently Γ contains no unipotent elements [8].

If $\mathbf{K}$ denotes the maximal compact subgroup of $\mathbf{SU}$, then the arithmetic groups described above determine finite volume quotients of the symmetric space $\mathbf{SU}/\mathbf{K}$. In fact the full group of holomorphic isometries is obtained by projectivizing these groups; ie Γ projects to an arithmetic lattice in $\mathbf{PSU}=\mathrm{PSU}(p_1,q_1)\times\cdots\times\mathrm{PSU}(p_s,q_s)$ (see Borel [6] and Borel and Harish-Chandra [8]). Notice that for each p_i,q_i, there is a natural epimorphism $\mathrm{SU}(p_i,q_i)\to\mathrm{PSU}(p_i,q_i)$ whose kernel consists of N–th roots of unity, and in particular is finite.

2.2

We maintain the notation of the previous subsection. Let $\mathcal{V}$ denote the set of nonarchimedean places of k. If $\mathcal{P}$ is a prime ideal in $\mathcal{O}_k$, we will write $v_\mathcal{P}$ for the place in $\mathcal{V}$ associated to $\mathcal{P}$, and often simply write v. The theory of the group $\mathcal{G}$ over the local fields k_v is well-understood and we summarize what is needed for us (see Platonov and Rapinchuk [33, Chapter 2.3.3] and Tits [37; 38]).

Suppose that L/F is a finite extension of number fields, with rings of integers $\mathcal{O}_L$ and $\mathcal{O}_F$ respectively. Let v be a place associated to a prime ideal $\mathcal{P}\subset\mathcal{O}_F$. Then the behavior of $\mathcal{P}$ in L/F is determined by how the $\mathcal{O}_L$–ideal $\mathcal{P}\mathcal{O}_L$ factorizes. We say that v (or the prime $\mathcal{P}$) *splits completely* in L/F if $\mathcal{P}\mathcal{O}_L$ decomposes as a product of precisely $[L:F]$ pairwise distinct prime ideals in $\mathcal{O}_L$ (each of norm q the rational prime lying below $\mathcal{P}$).

Consider the degree 2 extension K/k, and so a k–prime either remains prime in K, is ramified in K or splits into a product of two distinct primes. The structure of $\mathcal{G}(k_v)$ depends on the splitting type described above. Briefly, in the first two cases, the

persistence of the quadratic extension locally is enough to show that $\mathcal{G}(k_v)$ is a special unitary group. However, if v splits as a product of two primes in the quadratic extension K/k, then $k_v \otimes_k K \cong k_v \times k_v$ is not a quadratic field extension of k_v. Using this, it can be shown that

$$\mathcal{G}(k_v) \cong \{(A, B) \in \mathrm{SL}(N, k_v) \times \mathrm{SL}(N, k_v) : A = {H^{-1}}^t B^{-1} H\} \cong \mathrm{SL}(N, k_v).$$

For more details see the discussion in [33, Chapter 2.3.3] or [37, page 55; 38]. We summarize what is needed from this discussion in the following:

Theorem 2.1 *Suppose that q is a rational prime that splits completely to K, and v a place of k dividing q. Then $\mathcal{G}(k_v) \cong \mathrm{SL}(N, k_v) \cong \mathrm{SL}(N, \mathbf{Q}_q)$.*

The last isomorphism in Theorem 2.1 follows from the fact that for the places v in Theorem 2.1, $k_v \cong \mathbf{Q}_q$. That there are infinitely many such primes q follows from Cebotarev's density theorem.

For all but finitely many primes $\mathcal{P} \subset \mathcal{O}_k$, we can also consider $\mathcal{G}$ as an algebraic group over the residue class field $\mathbf{F}_v = \mathbf{F}_\mathcal{P} \cong \mathbf{F}_q$ (see [33, pages 142–143]). Moreover, by [33, Chapter 3, Proposition 3.20], for these primes the reduction map $\mathcal{G}(\mathcal{O}_k) \to \mathcal{G}(\mathbf{F}_\mathcal{P})$ is a surjective homomorphism. Thus, together with Theorem 2.1 we deduce:

Corollary 2.2 *Suppose that q is a rational prime that splits completely to K, and $\mathcal{P}$ a k–prime dividing q. Then for all but finitely many such primes $\mathcal{P}$, $\mathcal{G}(\mathbf{F}_\mathcal{P}) \cong \mathrm{SL}(N, q)$.*

2.3

We continue with the notation above. Being an algebraic subgroup of $\mathrm{SL}(N, \mathbf{C})$, $\mathcal{G}$ comes equipped with the Zariski topology, and so in particular is Zariski closed by definition. It also has the *analytic* ("usual") topology arising from the subspace topology inherited from $\mathrm{SL}(N, \mathbf{C})$. Thus given a subgroup $D < \mathcal{G}$ we can talk about its Zariski closure and analytic closure. Furthermore $\mathcal{G}(\mathbf{R})$ is a Lie group and a real algebraic group, and as such we can talk about the real Zariski closure and analytic closure of subgroups $D < \mathcal{G}(\mathbf{R})$. We collect some facts about the interplay between these topologies on these groups and their subgroups that will be used.

The following lemma is due to Chevalley (see Morris [30, Proposition 4.6.1]).

Lemma 2.3 *Let $D < \mathrm{SU}(N)$ be a subgroup. Then D is Zariski closed in $\mathrm{SU}(N)$ if and only if it is analytically closed.*

Lemma 2.4 *Suppose that $D<\mathcal{G}(k)$ is (real) Zariski dense in $\mathcal{G}(\mathbf{R})$, then D is Zariski dense in $\mathcal{G}$.*

Proof Let Z denote the Zariski closure of D in $\mathcal{G}$. Since $D<\mathcal{G}(k)$, Z is an algebraic subgroup of $\mathcal{G}$ defined over k (see [7, Chapters I.1.3, and AG 14.4], for example). Hence $Z(\mathbf{R})<\mathcal{G}(\mathbf{R})$ are real algebraic groups defined over k, and so are real Zariski closed sets. But the Zariski closure of D in $\mathcal{G}(\mathbf{R})$ is $\mathcal{G}(\mathbf{R})$, and so it follows that $Z(\mathbf{R})=\mathcal{G}(\mathbf{R})$.

Now viewed as real algebraic groups, the groups $\mathcal{G}(\mathbf{R})$ and $Z(\mathbf{R})$ are defined over k. The algebraic groups $\mathcal{G}$ and Z are also defined over k and are simply the complexifications of these real algebraic groups. Thus the ideals of polynomials defining $\mathcal{G}(\mathbf{R})$ and $\mathcal{G}$ (resp. $Z(\mathbf{R})$ and Z) agree. From this it follows that $Z=G$ as required. □

2.4

We will apply Strong Approximation, and in particular, a corollary of Theorem 10.5 of Weisfeiler [40] (see also Nori [32]). Note that $\mathcal{G}$ is an absolutely almost simple simply connected algebraic group defined over k (ie the only proper normal algebraic subgroups of $\mathcal{G}$ are finite) which is required in [40].

For convenience we state the main consequence of [40, Theorem 10.5 and Corollary 10.6] (see also the discussion in [26, Window 9]) in our context.

Definition 2.5 The *adjoint trace field* of a subgroup $D<\mathcal{G}(k)$ is defined to be the field $\mathbf{Q}(\{\mathrm{tr}(\mathrm{Ad}\,\gamma):\gamma\in D\})$. Here Ad denotes the adjoint representation of $\mathcal{G}$ on its Lie algebra.

Theorem 2.6 *Let $\mathcal{G}$ be as above, and let $D<\mathcal{G}(k)$ be a finitely generated Zariski dense subgroup of $\mathcal{G}$ such that the adjoint trace field of D is k. Then for all but finitely many k–primes $\mathcal{P}$, the reduction homomorphism $\pi_{\mathcal{P}}\colon D\to\mathcal{G}(\mathbf{F}_{\mathcal{P}})$ is surjective.*

Proof We briefly discuss how this is deduced from [40, Theorem 10.5 and Corollary 10.6]. Since D is finitely generated, apart from a finite set of places in $\mathcal{V}$, the image of D (which we will identify with D) under the embedding $\mathcal{G}(k)\hookrightarrow\mathcal{G}(k_v)$, lies in the subgroup $\mathcal{G}(\mathcal{O}_{k_v})$. Now the conclusion of [40, Corollary 10.6] states that there is a (perhaps different) finite set $T\subset\mathcal{V}$ so that the closure of D in the restricted direct product group $\prod_{\mathcal{V}\setminus T}\mathcal{G}(\mathcal{O}_{k_v})$ is open. That this closure is open, in particular implies that for all $v\in\mathcal{V}\setminus T$, the closure of D in the v–adic topology is all of $\mathcal{G}(\mathcal{O}_{k_v})$. It follows that the associated reduction homomorphism $\pi_{\mathcal{P}}$ is surjective. □

Theorem 2.6 together with Corollary 2.2 now shows the following:

Corollary 2.7 *Let $D < \mathcal{G}(k)$ be a finitely generated Zariski dense subgroup of $\mathcal{G}$ such that the adjoint trace field of D coincides with k. Then there are infinitely many k–primes $\mathcal{P}$ of norm q a prime in $\mathbf{Z}$, for which the reduction homomorphism $\pi_{\mathcal{P}}\colon D \to \mathrm{SL}(N, q)$ is surjective.*

Remark 2.8 It is clear from the proof that Theorem 2.6 and Corollary 2.7 also hold if we assume the adjoint trace field is a subfield $\ell \subset k$, provided that $\mathcal{G}$ can be defined over ℓ, and D lies in the ℓ–points of $\mathcal{G}$ (the point being that a rational prime that splits completely in k must split completely in ℓ). This observation will allow for a shortcut in our proof of Theorem 1.1 in Section 4.

3 The SO(3)–TQFT representations

We briefly recall some of the background from the SO(3)–TQFT constructed in Blanchet et al [5] and its integral version constructed in Gilmer and Masbaum [16]. We also record some consequences of this and Larsen and Wang [22] that we will make use of. From now on, we only consider the case where the prime p satisfies $p \equiv 3 \pmod 4$.

Remark 3.1 It is possible to make everything what follows work for all odd primes, but doing so requires some modifications and some extra arguments in the case $p \equiv 1 \pmod 4$. Since primes $p \equiv 3 \pmod 4$ are enough to prove Theorems 1.1 and 1.2, we prefer to restrict to that case for simplicity.

Let Σ be a compact oriented surface of genus g without boundary, and let Γ_g be its mapping class group. The integral SO(3)–TQFT constructed in [16] provides a representation of a central extension $\widetilde{\Gamma}_g$ of Γ_g by $\mathbf{Z}$ on a free lattice (ie a free module of finite rank) $\mathcal{S}_p(\Sigma)$ over the ring of cyclotomic integers $\mathbf{Z}[\zeta_p]$:

$$\rho_p\colon \widetilde{\Gamma}_g \longrightarrow \mathrm{GL}(\mathcal{S}_p(\Sigma)) \simeq \mathrm{GL}(N_g(p), \mathbf{Z}[\zeta_p]),$$

where $N_g(p)$ is the rank of $\mathcal{S}_p(\Sigma)$. We refer to this representation as the SO(3)–TQFT–representation. Some results and conjectures about this representation are discussed by the first author in [27]. We also denote by $V_p(\Sigma)$ the K–vector space $\mathcal{S}_p(\Sigma) \otimes K$ where $K = \mathbf{Q}(\zeta_p)$ as in Section 2. The V_p–theory is a version of the Reshetikhin–Turaev TQFT associated with the Lie group SO(3), and we think of $\mathcal{S}_p$ as an integral refinement of that theory (see Gilmer and Masbaum [16] for more details). The rank $N_g(p)$ of $\mathcal{S}_p(\Sigma)$ is given by a Verlinde-type formula and goes to infinity as $p \to \infty$. The construction uses the skein theory of the Kauffman bracket with

Kauffman's skein variable A specialized to $A = -\zeta_p^{(p+1)/2}$. Note that $A^2 = \zeta_p$ and A is a primitive $2p$–th root of unity.

We assume $g \geq 3$, so that Γ_g is perfect and $H^2(\Gamma_g; \mathbf{Z}) \simeq \mathbf{Z}$. It is customary in TQFT to take the extension $\widetilde{\Gamma}_g$ to be isomorphic to Meyer's signature extension, whose cohomology class is 4 times a generator of $H^2(\Gamma_g; \mathbf{Z}) \simeq \mathbf{Z}$. However, in this paper we take $\widetilde{\Gamma}_g$ so that the cohomology class $[\widetilde{\Gamma}_g]$ is a generator of $H^2(\Gamma_g; \mathbf{Z})$. Thus our $\widetilde{\Gamma}_g$ is (isomorphic to) an index four subgroup of the signature extension. The advantage of this choice is that $\widetilde{\Gamma}_g$ is a perfect group. In fact, $\widetilde{\Gamma}_g$ is a universal central extension of Γ_g for $g \geq 4$.

Remark 3.2 The are various constructions of these central extensions of the mapping class group from the TQFT point of view. We will not discuss them here as the details are not relevant for this paper. To be specific, we follow the approach of Gilmer and Masbaum [15], except for notation: our $\widetilde{\Gamma}_g$ is denoted by $\widetilde{\Gamma}_g^{++}$ in [15]. Up to isomorphism, this is the same as the extension denoted by $\widetilde{\Gamma}_1$ in Masbaum and Roberts [28].

The generator of the kernel of $\widetilde{\Gamma}_g \to \Gamma_g$ acts as multiplication by ζ_p^{-6} on $\mathcal{S}_p(\Sigma)$. (This is the fourth power of the number κ as given in [15, Section 11].) Since $\zeta_p^{-6} \neq 1$, the TQFT–representation ρ_p induces only a projective representation of the mapping class group Γ_g.

Notation 3.3 Henceforth, the image group $\rho_p(\widetilde{\Gamma}_g)$ will be denoted by Δ_g.

Remark 3.4 The following observation will be used in the proof of our main theorem: If we have a surjection from Δ_g to a finite group H, the induced surjection

$$\widetilde{\Gamma}_g \twoheadrightarrow \Delta_g \twoheadrightarrow H$$

will factor through a surjection $\Gamma_g \twoheadrightarrow H$ as soon as H has no nontrivial central element of order p (because $\widetilde{\Gamma}_g \to \Gamma_g$ is a central extension and the generator of its kernel is sent to an element of order p in Δ_g). In particular if H has trivial center this will hold.

We now refine the strategy outlined in Section 1. First, as observed by Dunfield and Wong [11], the map

$$\det \circ \rho_p \colon \widetilde{\Gamma}_g \longrightarrow \mathbf{Z}[\zeta_p]^\times$$

is trivial, since $\widetilde{\Gamma}_g$ is perfect. Therefore the group $\Delta_g = \rho_p(\widetilde{\Gamma}_g)$ is contained in a special linear group:

$$\Delta_g \subset \mathrm{SL}(\mathcal{S}_p(\Sigma)) \simeq \mathrm{SL}(N, \mathbf{Z}[\zeta_p]),$$

where $N = N_g(p)$. The primes $\widetilde{q}$ in $\mathbf{Z}[\zeta_p]$ mentioned in Section 1 lie above those rational primes q which split completely in $\mathbf{Z}[\zeta_p]$. For every such prime $\widetilde{q}$ of $\mathbf{Z}[\zeta_p]$ lying over q, we can consider the group

$$\pi_{\widetilde{q}}(\Delta_g) \subset \mathrm{SL}(N, q),$$

where $\pi_{\widetilde{q}}$ is the reduction homomorphism from $\mathrm{SL}(N, \mathbf{Z}[\zeta_p])$ to $\mathrm{SL}(N, q)$ induced by the isomorphism $\mathbf{Z}[\zeta_p]/\widetilde{q} \simeq \mathbf{F}_q$. The key step in the proof of Theorem 1.2 is to establish

$$\pi_{\widetilde{q}}(\Delta_g) = \mathrm{SL}(N, q) \tag{1}$$

for all but finitely many such $\widetilde{q}$. This will be an application of Corollary 2.7 and is described in Section 4. Thus, as announced in Section 1, we will have surjections $\Delta_g \twoheadrightarrow \mathrm{SL}(N, q)$ for infinitely many primes q. The surjections $\Gamma_g \twoheadrightarrow \mathrm{PSL}(N, q)$ follow easily and this will complete the proof of Theorem 1.2.

Remark 3.5 As far as proving the equality (1) for all but finitely many $\widetilde{q}$, we do not actually need Integral TQFT. Here by Integral TQFT we mean the fact that the TQFT–representation ρ_p preserves the lattice $\mathcal{S}_p(\Sigma)$ inside the TQFT–vector space $V_p(\Sigma) = \mathcal{S}_p(\Sigma) \otimes K$, which we used to arrange that $\Delta_g = \rho_p(\widetilde{\Gamma}_g)$ lies in $\mathrm{SL}(N, \mathbf{Z}[\zeta_p])$ rather than just in $\mathrm{SL}(N, \mathbf{Q}(\zeta_p))$. The point is that even if Δ_g is only known to lie in $\mathrm{SL}(N, \mathbf{Q}(\zeta_p))$, we can still define $\pi_{\widetilde{q}}(\Delta_g)$ for all but finitely many $\widetilde{q}$ (because Δ_g is a finitely generated group, and so involves only finitely many primes in the denominators of its matrix entries). This is enough for our application of Corollary 2.7. On the other hand, it is interesting to know that the group $\pi_{\widetilde{q}}(\Delta_g)$ is always defined, and one may ask which are the exceptional primes q (if any) for which this group is strictly smaller than $\mathrm{SL}(N, q)$?

In order to apply Corollary 2.7 to Δ_g, we need to describe the Zariski closure of Δ_g as an algebraic group defined over a number field, which we will now do in the remainder of this section. The first step is to observe that Δ_g lies in a (special) unitary group. This is because, as always in TQFT, the representation ρ_p preserves a nondegenerate Hermitian form. Here, conjugation is given by $\overline{\zeta_p} = \zeta_p^{-1}$. Let us denote by H_p the Hermitian form on the vector space $V_p(\Sigma)$ defined in [5]. There is a basis of $V_p(\Sigma)$ which is orthogonal for this form; moreover the diagonal terms of the matrix of H_p in this basis lie in the maximal real subfield k. Explicit formulas for these diagonal terms are given in [5, Theorem 4.11].

Remark 3.6 (i) Note that H_p is denoted by $\langle\ ,\ \rangle_\Sigma$ in [5]. We are using here that $p \equiv 3 \pmod 4$, because in this case the coefficient $\eta = \langle S^3 \rangle_p$ which appears

in [5, Theorem 4.11] lies in k. Indeed, we have $\overline{\eta} = \eta$ and it is shown in [17, Lemma 4.1(ii)] that η^{-1} (which is called $\mathcal{D}$ in [17; 16]) lies in $\mathbf{Z}[\zeta_p]$.

(ii) It is shown in [17; 16] that one can rescale the hermitian form so that its values on the lattice $\mathcal{S}_p(\Sigma)$ lie in $\mathbf{Z}[\zeta_p]$ (it suffices to multiply the form by the number $\mathcal{D}$).

Thus the Hermitian form H_p is defined over k. As in Section 2.1, let $\mathcal{G}$ be the group $\mathrm{SU}(V_p(\Sigma), H_p)$; this is an algebraic group $\mathcal{G}$ defined over k, and

$$\Delta_g = \rho_p(\widetilde{\Gamma}_g) \subset \mathcal{G}(k).$$

The signature of the Hermitian form H_p depends on the choice of ζ_p in $\mathbf{C}$. For the choice

$$A = i^p e^{2\pi i/4p}, \quad \zeta_p = A^2 = (-1)^p e^{2\pi i/2p} = (e^{2\pi i/p})^{(p+1)/2}$$

the form H_p is positive definite so that $\mathcal{G}(\mathbf{R})$ is isomorphic to the usual special unitary group $\mathrm{SU}(N)$ where $N = N_g(p) = \mathrm{rk}\,\mathcal{S}_p(\Sigma) = \dim V_p(\Sigma)$. For other choices of ζ_p in $\mathbf{C}$ the form is typically indefinite as soon as the genus is at least two [5, Remark 4.12].

We now recall the following result of Larsen and Wang [22].

Theorem 3.7 [22] *For the choice of root of unity given above, Δ_g projects to a subset of $\mathrm{PSU}(N)$ that is dense in the analytic topology.*

Remark 3.8 Larsen and Wang actually take $A = ie^{2\pi i/4p}$ if $p \equiv 3 \pmod 4$. This differs from our choice of A by a sign. The explanation is that Larsen and Wang take A to be a primitive p–th root whereas in the skein-theoretic approach to TQFT of [5] which we are using, A must be a primitive $2p$–th root (essentially because in the axiomatics of [5], Kauffman's skein variable must be A rather than $-A$). However, in the SO(3)–case, the TQFT–representation ρ_p of $\widetilde{\Gamma}_g$ only depends on $A^2 = \zeta_p$, so the sign of A is, in fact, irrelevant here.

Since $\mathrm{SU}(N) \to \mathrm{PSU}(N)$ is a finite covering, a corollary of Theorem 3.7 is:

Corollary 3.9 *With the notation as above, Δ_g is a dense subgroup of $\mathrm{SU}(N)$ in the analytic topology.*

We also see from this discussion, and that contained in Section 2.1, that Δ_g contains no unipotent elements.

Corollary 3.10 *In the notation above, Δ_g is Zariski dense in the algebraic group $\mathcal{G}$.*

Proof This follows applying Lemma 2.3, and Lemma 2.4. □

Remark 3.11 (1) At present it remains open whether the index of Δ_g in the arithmetic group $\Gamma \simeq \mathcal{G}(\mathcal{O}_k)$ (see the discussion in Section 2.1) is finite or infinite. If this index were finite then Δ_g would have been arithmetic and so Zariski density would follow from Borel density.

(2) We also note that Zariski density at other embeddings of k into $\mathbf{R}$ follows easily from this, but we will not need to make use of this fact.

4 Proof of the main results

4.1 Proof of Theorem 1.1 and Theorem 1.2

Fixing $g \geq 3$ and a prime $p \equiv 3 \pmod 4$, the discussion in Section 3 shows that we have a representation ρ_p of $\widetilde{\Gamma}_g$ whose image Δ_g lies in the k–points of the algebraic group $\mathcal{G}$ defined over k, where k is the maximal real subfield of the cyclotomic field $K = \mathbf{Q}(\zeta_p)$, with the root of unity $\zeta_p \in \mathbf{C}$ chosen so that $\mathcal{G}(\mathbf{R}) \cong \mathrm{SU}(N)$. Moreover, Δ_g is Zariski dense in $\mathcal{G}$. We wish to apply Corollary 2.7 to this situation. Notice that all the hypotheses of this corollary are already satisfied, except the hypothesis about the adjoint trace field. Denote the adjoint trace field of Δ_g by

$$\ell = \mathbf{Q}(\mathrm{tr}(\mathrm{Ad}\,\gamma) : \gamma \in \Delta_g).$$

As observed in Remark 2.8, it is enough to check that $\mathcal{G}$ can be defined over ℓ, and that Δ_g lies in the ℓ–points of $\mathcal{G}$. This is the content of Proposition 4.2 below, which we prove next.

Lemma 4.1 *We have $\ell \subset k$.*

Proof As in Sections 2.1 and 2.2, we are considering $\mathcal{G}$ as a k–algebraic subgroup of $\mathrm{SL}(2N)$. We denote the adjoint group $\mathrm{Ad}\,\mathcal{G}$ by $\mathcal{G}_{\mathrm{ad}}$. Since $\Delta_g \subset \mathcal{G}(k)$, we have $\mathrm{Ad}\,\gamma \in \mathcal{G}_{\mathrm{ad}}(k)$ for all $\gamma \in \Delta_g$. This shows $\ell \subset k$. □

Proposition 4.2 *The group $\mathcal{G}$ can be defined over ℓ, and one has $\Delta_g \subset \mathcal{G}(\ell)$.*

Proof By Vinberg's theorem [39, Theorem 1] (see also Mostow [31, (2.5.1)]), Zariski density of Δ_g in $\mathcal{G}$ together with $\mathbf{Q}(\mathrm{tr}(\mathrm{Ad}\,\gamma) : \gamma \in \Delta_g) = \ell$ imply that there is an ℓ–structure on $\mathcal{G}_{\mathrm{ad}}$ (ie, the group $\mathcal{G}_{\mathrm{ad}}$ can be defined over ℓ) so that $\mathrm{Ad}\,\Delta_g \subset \mathcal{G}_{\mathrm{ad}}(\ell)$. Since $\mathcal{G}$ is simply connected, by a well-known result of Borel and Tits [9] (see also Platonov and Rapinchuk [33, Section 2.2]), this ℓ–structure on $\mathcal{G}_{\mathrm{ad}}$ can be lifted to an ℓ–structure on $\mathcal{G}$ so that the canonical projection $\pi\colon \mathcal{G} \to \mathcal{G}_{\mathrm{ad}}$ is defined over ℓ.

As already mentioned, Vinberg's theorem also gives that $\operatorname{Ad}\Delta_g \subset \mathcal{G}_{\mathrm{ad}}(\ell)$. We must show that, in fact, $\Delta_g \subset \mathcal{G}(\ell)$. This is, however, not a formal consequence of Vinberg's theorem, but uses the fact that Δ_g is perfect. We proceed as follows. To show that $\Delta_g \subset \mathcal{G}(\ell)$, we will show that $\sigma(\gamma) = \gamma$ for every $\gamma \in \Delta_g \subset \mathcal{G}(k)$ and $\sigma \in \mathrm{Gal}(k/\ell)$ (recall that Lemma 4.1 shows that $\ell \subset k$). Consider the exact sequence

$$C(k) \to \mathcal{G}(k) \xrightarrow{\pi} \mathcal{G}_{\mathrm{ad}}(k),$$

where C is the center of $\mathcal{G}$. Since $\operatorname{Ad}\gamma \in \mathcal{G}_{\mathrm{ad}}(\ell)$ for $\gamma \in \Delta_g$, we have

$$\pi(\sigma(\gamma)) = \sigma(\pi(\gamma)) = \pi(\gamma)$$

for every $\sigma \in \mathrm{Gal}(k/\ell)$. Hence the function f_γ defined by

$$f_\gamma(\sigma) = \gamma\,\sigma(\gamma^{-1})$$

is a $C(k)$–valued 1–cocycle on $\mathrm{Gal}(k/\ell)$. (One easily checks the cocycle condition $f_\gamma(\sigma_1\sigma_2) = f_\gamma(\sigma_1)\sigma_1(f_\gamma(\sigma_2))$.) Let $Z^1(\mathrm{Gal}(k/\ell); C(k))$ denote the space of such cocycles. It is an abelian group (since $C(k)$ is abelian.) Moreover, the assignment $\gamma \mapsto f_\gamma$ is a group homomorphism from Δ_g to $Z^1(\mathrm{Gal}(k/\ell); C(k))$. But since Δ_g is perfect, this homomorphism is trivial; in other words, we have $f_\gamma = 1$ for all $\gamma \in \Delta_g$. This shows that $\Delta_g \subset \mathcal{G}(\ell)$, as asserted. □

Remark 4.3 A natural question at this point is whether $\ell = k$. As far as the proofs of Theorems 1.1 and 1.2 are concerned, whether the answer is in the affirmative or not, does not matter because, as observed in Remark 2.8, we can simply apply Corollary 2.7 with ℓ in place of k. However, for completeness, and because it seems worthwhile recording, we will prove that indeed $\ell = k$ (using Proposition 4.2) in Section 4.3.

We can now give the proof of Theorem 1.2 which is restated below for convenience.

Theorem 1.2 *For each $g \geq 3$, there exists infinitely many N such that for each such N, there exists infinitely many primes q such that Γ_g surjects $\mathrm{PSL}(N, q)$.*

Proof Fixing $g \geq 3$, the discussion in Section 3 together with Proposition 4.2 shows that for every prime $p \equiv 3 \pmod 4$ we have a representation ρ_p of $\widetilde{\Gamma}_g$ whose image Δ_g lies in the ℓ–points of the algebraic group $\mathcal{G}$ defined over ℓ, where ℓ is a finite Galois extension of $\mathbf{Q}$ and $\mathcal{G}(\mathbf{R}) \cong \mathrm{SU}(N)$, with $N = N_g(p)$ going to infinity as $p \to \infty$. Moreover, Δ_g is Zariski dense in $\mathcal{G}$ and its adjoint trace field is ℓ.

Fixing such a dimension N as above, we deduce from Corollary 2.7 that there are infinitely many rational primes q such that Δ_g surjects the groups $\mathrm{SL}(N, q)$. Now

quotienting out by the center of $\mathrm{SL}(N,q)$ gives surjections of Δ_g onto $\mathrm{PSL}(N,q)$. As remarked in Remark 3.3, the induced homomorphisms $\widetilde{\Gamma}_g \to \mathrm{PSL}(N,q)$ will factor through Γ_g since $\mathrm{PSL}(N,q)$ has trivial center. □

The proof of Theorem 1.1 will be completed by the following basic fact about embedding finite groups in the groups $\mathrm{PSL}(N,q)$.

Lemma 4.4 *Let H be a finite group, then there exists an integer N such that for all odd primes q, H is isomorphic to a subgroup of $\mathrm{PSL}(N,q)$.*

Proof By Cayley's theorem, every finite group embeds in a symmetric group. Thus it suffices to prove the lemma for symmetric groups S_n. Note first that $\mathrm{PSL}(N,q)$ has even order and so will trivially contain a copy of S_2 (being isomorphic to the cyclic group of order 2). Thus we can assume that $n \geq 3$. We first prove that S_n injects into $\mathrm{SL}(N,q)$ (for large enough N).

To that end, recall that the standard permutation representation of S_n injects $S_n \hookrightarrow \mathrm{GL}(n,\mathbf{Z})$. Furthermore, $\mathrm{GL}(n,\mathbf{Z})$ can be embedded in $\mathrm{SL}(n+1,\mathbf{Z})$ by sending $g \in \mathrm{GL}(n,\mathbf{Z})$ to the element

$$\begin{pmatrix} g & 0 \\ 0 & \epsilon(g) \end{pmatrix},$$

where $\epsilon(g) = \pm 1$ depending on whether $\det(g) = \pm 1$.

It is a well-known result of Minkowski that the kernels of the homomorphisms $\mathrm{SL}(N,\mathbf{Z}) \to \mathrm{SL}(N,q)$ are torsion-free for q an odd prime (see [33, Lemma 4.19]). Hence the copies of S_n constructed above inject in $\mathrm{SL}(N,q)$ as required.

To pass to $\mathrm{PSL}(N,q)$, simply note that $\mathrm{PSL}(N,q)$ is the central quotient of $\mathrm{SL}(N,q)$, and the center of S_n is trivial for $n \geq 3$. Hence S_n will inject into $\mathrm{PSL}(N,q)$. □

4.2 The case of the Torelli group

We now discuss the case of the Torelli subgroup (ie, the kernel of the homomorphism $\Gamma_g \to \mathrm{Sp}(2g,\mathbf{Z})$). We will denote the Torelli group by $\mathcal{I}_g$. Johnson [20] showed that $\mathcal{I}_g$ is finitely generated for $g \geq 3$ and Mess [29] showed that $\mathcal{I}_2$ is an infinitely generated free group.

Theorem 4.5 *For each $g \geq 2$, there exists infinitely many N such that for each such N, there exists infinitely many primes q such that $\mathcal{I}_g$ surjects $\mathrm{PSL}(N,q)$.*

Proof As noted above $\mathcal{I}_2$ is an infinitely generated free group and so the result easily holds in this case. Thus we fix a $g \geq 3$, and consider a surjection $f\colon \Gamma_g \twoheadrightarrow \mathrm{PSL}(N,q)$ as constructed in Theorem 1.2. Since $\mathcal{I}_g$ is normal in Γ_g, the image $f(\mathcal{I}_g)$ in $\mathrm{PSL}(N,q)$ will also be normal. The groups $\mathrm{PSL}(N,q)$ are simple, and so $f(\mathcal{I}_g)$ is either trivial or $\mathrm{PSL}(N,q)$.

We claim that for N large enough the image must be $\mathrm{PSL}(N,q)$. For suppose not, then for some arbitrarily large N the image $f(\mathcal{I}_g)$ will be trivial, and so the epimorphisms $f\colon \Gamma_g \twoheadrightarrow \mathrm{PSL}(N,q)$ will factor through $\mathrm{Sp}(2g,\mathbf{Z})$. However, as mentioned in Section 1, $\mathrm{Sp}(2g,\mathbf{Z})$ has the Congruence Subgroup Property and so cannot surject the groups $\mathrm{PSL}(N,q)$ (for N large). □

4.3 The adjoint trace field

We briefly discuss how to deduce that the adjoint trace field $\ell = \mathbf{Q}(\mathrm{tr}(\mathrm{Ad}\,\gamma) : \gamma \in \Delta_g)$ is equal to k. (Recall that k is the maximal real subfield of the cyclotomic field $K = \mathbf{Q}(\zeta_p)$.) We proceed as follows.

From Lemma 4.1 and Proposition 4.2, we have that ℓ is a subfield of k so that $\mathcal{G}$ can be defined over ℓ, and $\Delta_g \subset \mathcal{G}(\ell)$. The group $\mathcal{G}$, when considered as defined over ℓ, is an ℓ–form of $\mathrm{SU}(N)$. By the classification of forms of $\mathrm{SU}(N)$ over number fields [33, Sections (2.3.3) and (2.3.4)], there is a central simple algebra A, with center L a quadratic field extension of ℓ, so that

$$\mathcal{G}(\ell) = \{x \in A \mid x\,\tau(x) = 1,\ \mathrm{Nrd}(x) = 1\},$$

where τ is an (anti)involution of A of the second kind, and Nrd is the reduced norm. Therefore for all $\gamma \in \Delta_g \subset \mathcal{G}(\ell)$, we have

$$\mathrm{Trd}(\gamma) \in L,$$

where Trd is the reduced trace. When we extend scalars from ℓ to k, our group $\mathcal{G}$ viewed as an ℓ–group becomes k–isomorphic to our original k–group $\mathcal{G}$. Thus

$$A \otimes K \simeq M_N(K)$$

(where $N = N_g(p)$ is the dimension of the K–vector space $V_p(\Sigma)$), and the reduced trace $\mathrm{Trd}(\gamma)$ is (strictly by definition) nothing but the ordinary trace of γ viewed as an element of $M_N(K)$. For $\gamma \in \Delta_g = \rho_p(\widetilde{\Gamma}_g)$, this is the same as the trace of γ acting on $V_p(\Sigma)$.

Now recall that the generator of the kernel of the central extension $\widetilde{\Gamma}_g \to \Gamma_g$ acts as multiplication by a primitive p–th root of unity on the vector space $V_p(\Sigma)$. Thus

$\Delta_g = \rho_p(\widetilde{\Gamma}_g)$ contains an element γ whose trace on $V_p(\Sigma)$ is N times ζ_p. Since this is the same as $\mathrm{Trd}(\gamma)$, and we know that $\mathrm{Trd}(\gamma) \in L$, it follows that $\zeta_p \in L$, hence $L = K$. Since $\ell \subset k$ and $[L : \ell] = 2$, this shows $\ell = k$.

5 Comments

(1) As shown by Long and Reid [24] for example, if Γ is a finitely generated group that contains a nonabelian free group, and Γ is LERF (ie, all finitely generated subgroups of Γ are closed in the profinite topology on Γ), then all finite groups are involved in Γ. In the context of lattices in semisimple Lie groups, it is only in rank 1 that examples of LERF lattices are known, although large classes of lattices in these rank 1 Lie groups are known to have a slightly weaker separability property (see for example Agol, Long and Reid [1], Bergeron, Haglund and Wise [3] and Long and Reid [24]). In higher rank the expectation is that lattices will not be LERF, since the expectation is that the Congruence Subgroup Property should hold for these higher rank lattices. As mentioned in Section 1, if the group Γ is an arithmetic lattice that has the Congruence Subgroup Property, then the finite groups that are involved in Γ are restricted.

It is an easy fact that Γ_g is not LERF (see Leininger and McReynolds [23, Appendix A]).

(2) Let F_n denote a free group of rank n and $\mathrm{Out}(F_n)$ denote its outer automorphism group. The family of groups $\mathrm{Out}(F_n)$, $n \geq 2$ are often studied in comparison to mapping class groups. Typically, a theorem about mapping class groups is reworked in the context of $\mathrm{Out}(F_n)$. In regards to Theorem 1.1, it was already known from Gilman [14] that all finite groups are involved in $\mathrm{Out}(F_n)$. Indeed, for $n \geq 3$, Gilman [14] showed that $\mathrm{Out}(F_n)$ is residually symmetric (ie, given $1 \neq \alpha \in \mathrm{Out}(F_n)$ there is a finite symmetric group S_m and an epimorphism $\theta\colon \mathrm{Out}(F_n) \to S_m$ with $\theta(\alpha) \neq 1$).

Another proof that all finite groups are involved in $\mathrm{Out}(F_n)$ can be deduced from Grunewald and Lubotzky [19] using methods similar to those used here.

References

[1] **I Agol**, **D D Long**, **A W Reid**, *The Bianchi groups are separable on geometrically finite subgroups*, Ann. of Math. 153 (2001) 599–621 MR1836283

[2] **H Bass**, **J Milnor**, **J-P Serre**, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. (1967) 59–137 MR0244257

[3] **N Bergeron**, **F Haglund**, **D T Wise**, *Hyperplane sections in arithmetic hyperbolic manifolds*, J. Lond. Math. Soc. 83 (2011) 431–448 MR2776645

[4] **J A Berrick**, **V Gebhardt**, **L Paris**, *Finite index subgroups of mapping class groups* arXiv:1105.2468

[5] **C Blanchet**, **N Habegger**, **G Masbaum**, **P Vogel**, *Topological quantum field theories derived from the Kauffman bracket*, Topology 34 (1995) 883–927 MR1362791

[6] **A Borel**, *Compact Clifford–Klein forms of symmetric spaces*, Topology 2 (1963) 111–122 MR0146301

[7] **A Borel**, *Linear algebraic groups*, W. A. Benjamin, New York-Amsterdam (1969) MR0251042 Notes taken by H Bass

[8] **A Borel**, **Harish-Chandra**, *Arithmetic subgroups of algebraic groups*, Ann. of Math. 75 (1962) 485–535 MR0147566

[9] **A Borel**, **J Tits**, *Compléments à l'article: "Groupes réductifs"*, Inst. Hautes Études Sci. Publ. Math. (1972) 253–276 MR0315007

[10] **N M Dunfield**, **W P Thurston**, *Finite covers of random* 3*–manifolds*, Invent. Math. 166 (2006) 457–521 MR2257389

[11] **N M Dunfield**, **H Wong**, *Quantum invariants of random* 3*–manifolds*, Algebr. Geom. Topol. 11 (2011) 2191–2205 MR2826936

[12] **L Funar**, *Zariski density and finite quotients of mapping class groups*, to appear in Int. Math. Res. Not. 2012 (2012) arXiv:1106.4165

[13] **L Funar**, **W Pitsch**, *Finite quotients of symplectic groups vs mapping class groups* arXiv:1103.1855

[14] **R Gilman**, *Finite quotients of the automorphism group of a free group*, Canad. J. Math. 29 (1977) 541–551 MR0435226

[15] **P M Gilmer**, **G Masbaum**, *Maslov index, Lagrangians, mapping class groups and TQFT*, to appear in Forum Math. arXiv:0912.4706

[16] **P M Gilmer**, **G Masbaum**, *Integral lattices in TQFT*, Ann. Sci. École Norm. Sup. 40 (2007) 815–844 MR2382862

[17] **P M Gilmer**, **G Masbaum**, **P van Wamelen**, *Integral bases for TQFT modules and unimodular representations of mapping class groups*, Comment. Math. Helv. 79 (2004) 260–284 MR2059432

[18] **E K Grossman**, *On the residual finiteness of certain mapping class groups*, J. London Math. Soc. 9 (1974/75) 160–164 MR0405423

[19] **F Grunewald**, **A Lubotzky**, *Linear representations of the automorphism group of a free group*, Geom. Funct. Anal. 18 (2009) 1564–1608 MR2481737

[20] **D Johnson**, *The structure of the Torelli group I: A finite set of generators for $\mathcal{I}$*, Ann. of Math. 118 (1983) 423–442 MR727699

[21] **M Korkmaz**, *On cofinite subgroups of mapping class groups*, Turkish J. Math. 27 (2003) 115–123 MR1975334

[22] **M Larsen**, **Z Wang**, *Density of the* SO(3) *TQFT representation of mapping class groups*, Comm. Math. Phys. 260 (2005) 641–658 MR2183960

[23] **C J Leininger**, **D B McReynolds**, *Separable subgroups of mapping class groups*, Topology Appl. 154 (2007) 1–10 MR2271769

[24] **D D Long**, **A W Reid**, *Surface subgroups and subgroup separability in* 3*–manifold topology*, IMPA Math. Publ., Inst. Nacional de Mat. Pura e Aplicada, Rio de Janeiro (2005) MR2164951 25th Brazilian Math. Colloquium

[25] **E Looijenga**, *Prym representations of mapping class groups*, Geom. Dedicata 64 (1997) 69–83 MR1432535

[26] **A Lubotzky**, **D Segal**, *Subgroup growth*, Progress in Math. 212, Birkhäuser, Basel (2003) MR1978431

[27] **G Masbaum**, *On representations of mapping class groups in Integral TQFT*, Oberwolfach Reports 5 (2008) 1157–1232 Available at `http://people.math.jussieu.fr/~masbaum`

[28] **G Masbaum**, **J D Roberts**, *On central extensions of mapping class groups*, Math. Ann. 302 (1995) 131–150 MR1329450

[29] **G Mess**, *The Torelli groups for genus* 2 *and* 3 *surfaces*, Topology 31 (1992) 775–790 MR1191379

[30] **D W Morris**, *Ratner's theorems on unipotent flows*, Chicago Lectures in Math., Univ. of Chicago Press (2005) MR2158954

[31] **G D Mostow**, *On a remarkable class of polyhedra in complex hyperbolic space*, Pacific J. Math. 86 (1980) 171–276 MR586876

[32] **M V Nori**, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. 88 (1987) 257–275 MR880952

[33] **V Platonov**, **A Rapinchuk**, *Algebraic groups and number theory*, Pure and Applied Math. 139, Academic Press, Boston (1994) MR1278263 Translated from the 1991 Russian original by R Rowen

[34] **N Reshetikhin**, **V G Turaev**, *Invariants of* 3*–manifolds via link polynomials and quantum groups*, Invent. Math. 103 (1991) 547–597 MR1091619

[35] **G Shimura**, *Arithmetic of unitary groups*, Ann. of Math. 79 (1964) 369–409 MR0158882

[36] **G Shimura**, *Arithmetic of Hermitian forms*, Doc. Math. 13 (2008) 739–774 MR2466186

[37] **J Tits**, *Classification of algebraic semisimple groups*, from: "Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, CO, 1965)", (A Borel, G D Mostow, editors), Amer. Math. Soc. (1966) 33–62 MR0224710

[38] **J Tits**, *Reductive groups over local fields*, from: "Automorphic forms, representations and L–functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, OR, 1977), Part 1", (A Borel, editor), Proc. Sympos. Pure Math. XXXIII, Amer. Math. Soc. (1979) 29–69 MR546588

[39] **E B Vinberg**, *Rings of definition of dense subgroups of semisimple linear groups*, Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971) 45–55 MR0279206

[40] **B Weisfeiler**, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. of Math. 120 (1984) 271–315 MR763908

Institut de Mathématiques de Jussieu (UMR 7586 du CNRS)
Case 247, 4 pl. Jussieu, 75252 Cedex 5 Paris, France

Department of Mathematics, University of Texas
1 Station C1200, Austin TX 78712-0257, USA

masbaum@math.jussieu.fr, areid@math.utexas.edu

http://www.math.jussieu.fr/~masbaum/,
http://www.ma.utexas.edu/users/areid/

Proposed: Benson Farb Received: 22 September 2011
Seconded: Ronald J Stern, Martin R Bridson Revised: 11 May 2012