New York Journal of Mathematics

New York J. Math. **18** (2012) 925–942.

The congruence subgroup problem for pure braid groups: Thurston's proof

D. B. McReynolds

Abstract. We present an unpublished proof of W. Thurston that pure braid groups have the congruence subgroup property.

Contents

1. Introduction

Let $S_{g,n}$ denote a surface of genus g with n punctures. The *pure mapping class group* $\mathrm{PMod}(S_{g,n})$ of $S_{g,n}$ is the subgroup of the group

$$\mathrm{Diffeo}^+(S_{g,n})/\mathrm{Diffeo}_0^+(S_{g,n})$$

of orientation preserving diffeomorphisms that fix each puncture modulo isotopy. The Dehn–Nielsen Theorem (see [8, Theorem 3.6] for instance) affords us with an injection of $\mathrm{PMod}(S_{g,n})$ into the outer automorphism group $\mathrm{Out}(\pi_1(S_{g,n}))$. Being a subgroup of $\mathrm{Out}(S_{g,n})$, the pure mapping class group $\mathrm{PMod}(S_{g,n})$ is endowed with a class of finite index subgroups called congruence subgroups. For each characteristic subgroup K of $\pi_1(S_{g,n})$, we have an induced homomorphism $\mathrm{PMod}(S_{g,n}) \to \mathrm{Out}(\pi_1(S_{g,n}/K))$. When K is finite index, the kernel of the induced homomorphism is a finite index subgroup of $\mathrm{PMod}(S_{g,n})$. These subgroups are called *principal congruence subgroups* (see Section 2 for a more general discussion) and any finite index subgroup

Received September 19, 2012.

2010 *Mathematics Subject Classification.* 20F36, 20E36, 20E26.

Key words and phrases. Congruence subgroup problem, pure braid groups.

Partially supported by DMS-1105710.

ISSN 1076-9803/2012

of $\mathrm{PMod}(S_{g,n})$ containing a principal congruence subgroup is called a *congruence subgroup*. The purpose of this article is to address the following problem sometimes called the *congruence subgroup problem* (see [2], [10]):

Congruence Subgroup Problem. *Is every subgroup of* $\mathrm{PMod}(S_{g,n})$ *of finite index a congruence subgroup?*

The congruence subgroup problem for $\mathrm{PMod}(S_{g,n})$ is a central problem for understanding $\mathrm{Mod}(S_{g,n})$ and $\mathrm{PMod}(S_{g,n})$. A positive answer allows one a means of understanding the finite index subgroup structure of $\mathrm{Mod}(S_{g,n})$ and thus profinite completion of $\mathrm{Mod}(S_{g,n})$. A few potential applications are a more precise understanding of the subgroup growth asymptotics for $\mathrm{Mod}(S_{g,n})$ and a better understanding of the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ via its action on the profinite completion of $\mathrm{Mod}(S_{g,n})$. The first case to be resolved was for $g = 0$, $n > 0$ by Diaz–Donagi–Harbater [6] in 1989 (though explicitly stated in the article only for $n = 4$). Asada [1, Theorem 3A, Theorem 5] gave a proof for $g = 0, 1$ and $n > 0$ in 2001 (for $g = 1$, see also [5] and [7]). Boggi [3, Theorem 6.1] claimed a general solution to the congruence subgroup problem in 2006. However, a gap in [3, Theorem 5.4] was discovered by Abromovich, Kent, and Wieland[1] (see the forthcoming articles [11, 12] for more on this). Boggi [4, Theorem 3.5] has since handled the cases of $g = 0, 1, 2$ (with $n > 0, n > 0, n \geq 0$, resp.). All of these proofs are in the language of algebraic geometry, field extensions, and profinite groups. In contrast, in 2002 W. Thurston [15] outlined an explicit, elementary proof for $g = 0$ that followed the general strategy given in [1, 3, 4]. This article gives a detailed account based on [15]. For future reference, we state the result here.

Theorem 1.1. $\mathrm{PMod}(S_{0,n})$ *has the congruence subgroup property.*

A few words are in order on how Thurston's proof compares to the proofs of Asada and Boggi. The proofs of Asada and Boggi are both short and elegant but use the language of profinite groups. Thurston's proof is longer but avoids the use of profinite groups and is essentially an explicit version of the proofs of Asada and Boggi. All three use the Birman exact sequence and use the fact that certain groups are centerless to control what one might call exceptional symmetries. All three use a homomorphism δ introduced below for this task. The merit of Thurston's proof is it's elementary nature; aside from Birman's work, the proof uses only elementary group theory.

The second goal of this article is to introduce to a larger audience the simplicity of this result, be it Asada, Boggi, or Thurston's proof (see [7] for a better introduction to Diaz–Donagi–Harbater [6]). In addition, we hope to spark more interest in the general congruence subgroup problem for mapping

[1] The gap was discovered by D. Abromovich, R. Kent, and B. Wieland while Abromovich prepared a review of this article for MathSciNet. They informed Boggi of the gap which he acknowledged in [4, p. 3].

class groups, a problem that is substantially more difficult than the simple case addressed here. Finally, we hope that those less familiar with the tools used in Asada, Boggi, and Diaz–Donagi–Harbater will see the potential for their methods, as in comparison to Thurston's proof, they provide a very simple and elegant framework for this problem.

Acknowledgements. I would first like to thank Nathan Dunfield for sharing with me Thurston's ideas. Most of my knowledge on this subject was gained from conversations with Dunfield and Chris Leininger, and I am deeply appreciative of the time both gave to me on this topic. I would also like to acknowledge the hard work of Dan Abromovich, Richard Kent IV, and Ben Wieland on reading [3]. I would like to give Kent special thanks for several conversations on this article and on [3, 4]. I would like to thank Jordan Ellenberg for pointing out [6], and Tom Church, Ellenberg, Benson Farb, Kent, Andy Putman, Justin Sinz, and the referees for several useful and indispensable comments on this article. Finally, I would like to thank Bill Thurston for allowing me to use the ideas presented in this article.

2. Preliminaries

For a group G, the automorphism group of G will be denoted by $\mathrm{Aut}(G)$. The normal subgroup of inner automorphisms will be denoted by $\mathrm{Inn}(G)$, and the group of outer automorphisms $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ will be denoted by $\mathrm{Out}(G)$. For an element $g \in G$, the G-conjugacy class of g will be denoted by $[g]$. The subgroup of G generated by a set of elements $g_1, \dots, g_r$ will be denoted by $\langle g_1, \dots, g_r \rangle$. The center of G will be denoted by $Z(G)$ and the centralizer of an element g will be denoted by $C_G(g)$.

1. Congruence subgroups. Let G be a finitely generated group and Λ a subgroup of $\mathrm{Aut}(G)$ (resp. $\mathrm{Out}(G)$). We say that a normal subgroup H of G is Λ-*invariant* if $\lambda(H) < H$ for all λ in Λ. For such a subgroup, the canonical epimorphism

$$\rho_H \colon G \longrightarrow G/H$$

induces a homomorphism

$$\rho_H^\star \colon \Lambda \longrightarrow \mathrm{Aut}(G/H) \quad (\text{resp. } \rho_H^* \colon \Lambda \longrightarrow \mathrm{Out}(G/H))$$

defined via the formula

$$\rho_H^\star(\lambda)(gH) = \lambda(g)H.$$

When H is finite index, $\ker \rho_H^\star$ (resp. $\ker \rho_H^*$) is finite index in Λ and is called a *principal congruence subgroup*. Any subgroup of Λ that contains a principal congruence subgroup is called a *congruence subgroup*. We say that Λ has the *congruence subgroup property* if every finite index subgroup of Λ is a congruence subgroup (see Bass–Lubotzky [2] for other examples of congruence subgroup problems).

The following lemma will be useful throughout this article.

Lemma 2.1. *The finite intersection of congruence subgroups is a congruence subgroup.*

The proof of this lemma is straightforward.

2. Geometrically characteristic subgroups. For $\Lambda = \mathrm{PMod}(S_{g,n})$ and $G = \pi_1(S_{g,n})$, we call $\mathrm{PMod}(S_{g,n})$-invariant subgroups of $\pi_1(S_{g,n})$ *geometrically characteristic subgroups*. We will denote the elements of $\pi_1(S_{g,n})$ generated by simple loops about the n punctures by $\gamma_1, \dots, \gamma_n$. The subgroup of $\mathrm{Aut}(S_{g,n})$ that fixes each conjugacy class $[\gamma_j]$ will be denoted by $\mathrm{Aut}_c(\pi_1(S_{g,n}))$ and we set

$$\mathrm{Out}_c(\pi_1(S_{g,n})) = \mathrm{Aut}_c(\pi_1(S_{g,n}))/\,\mathrm{Inn}(\pi_1(S_{g,n})).$$

The image of the pure mapping class group $\mathrm{PMod}(S_{g,n})$ afforded by the Dehn–Nielsen Theorem is a subgroup of $\mathrm{Out}_c(\pi_1(S_{g,n}))$. In the case when $g = 0$, we list only the elements $\gamma_1, \dots, \gamma_{n-1}$ generated by simple loops about the first $n-1$ punctures. For notational simplicity, we single out the element γ_n (or γ_{n-1} in the case $g = 0$) and denote it simply by λ.

3. The Birman exact sequences. The normal closure of $\langle \lambda \rangle$ will be denoted by N_λ and yields the short exact sequence

$$1 \longrightarrow N_\lambda \longrightarrow \pi_1(S_{g,n}) \xrightarrow{\rho_{N_\lambda}} \pi_1(S_{g,n-1}) \longrightarrow 1\ .$$

Since N_λ is $\mathrm{PMod}(S_{g,n})$-invariant, N_λ is geometrically characteristic and induces a short exact sequence

$$1 \longrightarrow K_\lambda \longrightarrow \mathrm{PMod}(S_{g,n}) \xrightarrow{\rho^*_{N_\lambda}} \mathrm{PMod}(S_{g,n-1}) \longrightarrow 1\ .$$

We also have the sequence

$$1 \longrightarrow \pi_1(S_{g,n-1}) \xrightarrow{\mu} \mathrm{Aut}_c(\pi_1(S_{g,n-1})) \xrightarrow{\theta} \mathrm{Out}_c(\pi_1(S_{g,n-1})) \longrightarrow 1, \tag{1}$$

where $\mu(\eta)$ is the associated inner automorphism given by conjugation by η; the homomorphism θ is specifically $\rho_{\mu(\pi_1(S_{g,n-1}))}$ or $\rho_{\mathrm{Inn}(\pi_1(S_{g,n-1}))}$. These two sequences are related via a homomorphism

$$\delta\colon\ \mathrm{Out}_c(\pi_1(S_{g,n})) \longrightarrow \mathrm{Aut}_c(\pi_1(S_{g,n-1})).$$

The map δ is given as follows. First, we select a normalized section of θ

$$s\colon\ \mathrm{Out}_c(\pi_1(S_{g,n})) \longrightarrow \mathrm{Aut}_c(\pi_1(S_{g,n}))$$

by sending an outer automorphism τ to an automorphism $s(\tau)$ such that $s(\tau)(\lambda) = \lambda$. The selection of $s(\tau)$ is unique up to right multiplication by the subgroup $\langle \mu(\lambda) \rangle$ of $\mathrm{Inn}(\pi_1(S_{g,n}))$. As N_λ is $\mathrm{Aut}_c(\pi_1(S_{g,n}))$-invariant, we have an induced homomorphism

$$\rho^\star_{N_\lambda}\colon\ \mathrm{Aut}_c(\pi_1(S_{g,n})) \longrightarrow \mathrm{Aut}_c(\pi_1(S_{g,n-1})),$$

and define δ by

$$\delta(\tau) = \rho^\star_{N_\lambda}(s(\tau)).$$

Since the choice of s is unique up to multiplication by the subgroup $\langle \mu(\lambda) \rangle$ and $\rho^{\star}_{N_\lambda}(\mu(\lambda)) = 1$, the map δ is a homomorphism. Under δ, the subgroup K_λ must map into $\mathrm{Inn}(\pi_1(S_{g,n-1}))$ since the projection to $\mathrm{Out}_c(\pi_1(S_{g,n-1}))$ is trivial. In fact, there exists an isomorphism

$$\mathrm{Push}\colon \pi_1(S_{g,n-1}) \longrightarrow K_\lambda,$$

and the result is the Birman exact sequence (see [8, Theorem 4.5] for instance)

$$(2) \qquad 1 \longrightarrow \pi_1(S_{g,n-1}) \xrightarrow{\mathrm{Push}} \mathrm{PMod}(S_{g,n}) \xrightarrow{\rho^*_{N_\lambda}} \mathrm{PMod}(S_{g,n-1}) \longrightarrow 1.$$

The aforementioned relationship between the sequences (1) and (2) given by δ is the content of our next lemma (see for instance [1, p. 130]).

Lemma 2.2. $\mu = \delta \circ \mathrm{Push}$.

Lemma 2.2 is well known and there are several ways to prove it. One proof is to check by direct computation that $\delta \circ \mathrm{Push} = \mu$. This can be done explicitly by verifying this functional equation for a standard generating set for $\pi_1(S_{g,n-1})$.

Remark. With regard to the congruence subgroup problem, note that there are two a priori different congruence subgroup problems for $\mathrm{PMod}(S_{g,n})$. One via the inclusion $\mathrm{PMod}(S_{g,n}) < \mathrm{Out}_c(\pi_1(S_{g,n}))$ and one using the homomorphism δ and viewing $\mathrm{PMod}(S_{g,n}) < \mathrm{Aut}_c(\pi_1(S_{g,n-1}))$. We will refer to the first as the congruence subgroup problem and not discuss the obviously related second version. In particular, for future reference, when we say a subgroup of $\mathrm{PMod}(S_{g,n})$ has the congruence subgroup property we will mean in the first sense.

We finish this section with the following useful lemma.

Lemma 2.3. *The $\rho^*_{N_\lambda}$-pullback of a congruence subgroup is a congruence subgroup.*

Proof. Given a principal congruence subgroup $\ker \rho^*_\Delta$ of $\mathrm{PMod}(S_{g,n-1})$ with associated geometrically characteristic subgroup Δ of $\pi_1(S_{g,n-1})$, the subgroup $\rho^{-1}_{N_\lambda}(\Delta)$ is a geometrically characteristic subgroup of $\pi_1(S_{g,n})$. The associated principal congruence is the $\rho^*_{N_\lambda}$-pullback of $\ker \rho^*_\Delta$. □

3. Proof of Theorem 1.1

The first and main step in proving Theorem 1.1 is the following (see also [13, Lemma 2.6] for another proof of this proposition).

Proposition 3.1. $\mathrm{Push}(\pi_1(S_{0,n-1}))$ *has the congruence subgroup property.*

Actually something stronger is needed and follows as a scholium of Proposition 3.1. Specifically:

Scholium 3.2. *Every finite index subgroup of* $\mathrm{Push}(\pi_1(S_{0,n-1}))$ *contains the intersection of a congruence subgroup of* $\mathrm{PMod}(S_{0,n})$ *with* $\mathrm{Push}(\pi_1(S_{0,n-1}))$.

Using Scholium 3.2, we will deduce the following inductive result, which is the second step in proving Theorem 1.1.

Proposition 3.3. *If* $\mathrm{PMod}(S_{0,n-1})$ *has the congruence subgroup property, then* $\mathrm{PMod}(S_{0,n})$ *has the congruence subgroup property.*

We now give a quick proof of Theorem 1.1 assuming these results.

Proof of Theorem 1.1. The first nontrivial case occurs when $n = 4$ where Proposition 3.1 and (2) establish that $\mathrm{PMod}(S_{0,4})$ has the congruence subgroup property. Specifically, $\mathrm{Push}(\pi_1(S_{0,3})) = \mathrm{PMod}(S_{0,4})$. From this equality, one obtains Theorem 1.1 by employing Proposition 3.3 inductively. □

4. Proof of Proposition 3.3

As the proof of Proposition 3.3 only requires the statement of Proposition 3.1, we prove Proposition 3.3 before commencing with the proof of Proposition 3.1.

Proof of Proposition 3.3. Given a subgroup Λ_0 of $\mathrm{PMod}(S_{0,n})$ of finite index, by passing to a normal finite index subgroup $\Lambda < \Lambda_0$, it suffices to prove that Λ is a congruence subgroup. From Λ, we obtain a surjective homomorphism

$$\rho_\Lambda \colon \mathrm{PMod}(S_{0,n}) \longrightarrow \mathrm{PMod}(S_{0,n})/\Lambda = Q.$$

We decompose Q via the Birman exact sequence. Specifically, the Birman exact sequence (2) produces a diagram

$$\begin{tikzcd} 1 \arrow[r] & \pi_1(S_{0,n-1}) \arrow[r, "\mathrm{Push}"] \arrow[d, "p"] & \mathrm{PMod}(S_{0,n}) \arrow[r, "\rho^*_{N_\lambda}"] \arrow[d, "\rho_\Lambda"] & \mathrm{PMod}(S_{0,n-1}) \arrow[r] \arrow[d, "r"] & 1 \\ 1 \arrow[r] & P \arrow[r] & Q \arrow[r] & R \arrow[r] & 1. \end{tikzcd} \tag{3}$$

Note that since this diagram is induced from the Birman sequence, both p, r are surjective homomorphisms though possibly trivial. According to Scholium 3.2, there exists a homomorphism

$$\rho_\Gamma \colon \pi_1(S_{0,n}) \longrightarrow \pi_1(S_{0,n})/\Gamma$$

with finite index, geometrically characteristic kernel Γ such that

$$\ker(\rho_\Gamma^* \circ \mathrm{Push}) < \mathrm{Push}(\ker p). \tag{4}$$

As we are assuming $\mathrm{PMod}(S_{0,n-1})$ has the congruence subgroup property, by Lemma 2.1 and Lemma 2.3, it suffices to find a finite index subgroup

Δ of $\mathrm{PMod}(S_{0,n-1})$ such that $\ker \rho_\Gamma^* \cap (\rho_{N_\lambda}^*)^{-1}(\Delta) < \ker \rho_\Lambda$. The subgroup $\Delta = \rho_{N_\lambda}^*(\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)$ is our candidate. We assert that

$$\ker \rho_\Gamma^* \cap (\rho_{N_\lambda}^*)^{-1}(\rho_{N_\lambda}^*(\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)) < \ker \rho_\Lambda.$$

To see this containment, first note that

$$(\rho_{N_\lambda}^*)^{-1}(\rho_{N_\lambda}^*(\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)) = \mathrm{Push}(\pi_1(S_{0,n-1})) \cdot (\ker \rho_\Gamma^* \cap \ker \rho_\Lambda).$$

Every element in the latter subgroup can be written in the form sk where s is an element of $\mathrm{Push}(\pi_1(S_{0,n-1}))$ and k is an element of $\ker \rho_\Gamma^* \cap \ker \rho_\Lambda$. If γ is an element of

$$\ker \rho_\Gamma^* \cap (\mathrm{Push}(\pi_1(S_{0,n-1})) \cdot (\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)),$$

then writing $\gamma = sk$, we see that since both sk and k are elements of $\ker \rho_\Gamma^*$, then so is s. In particular, it must be that s is an element of $\ker \rho_\Gamma^* \cap \mathrm{Push}(\pi_1(S_{0,n-1}))$. By (4), we have

$$\ker(\rho_\Gamma^* \circ \mathrm{Push}) = \ker \rho_\Gamma^* \cap \mathrm{Push}(\pi_1(S_{0,n-1})) < \mathrm{Push}(\ker p),$$

and so s is an element of $\mathrm{Push}(\ker p)$. Therefore, we now know that

$$\ker \rho_\Gamma^* \cap (\rho_{N_\lambda}^*)^{-1}(\rho_{N_\lambda}^*(\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)) < \mathrm{Push}(\ker p) \cdot (\ker \rho_\Gamma^* \cap \ker \rho_\Lambda).$$

Visibly, any element of $\mathrm{Push}(\ker p) \cdot (\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)$ is an element of $\ker \rho_\Lambda$, and so we have

$$\ker \rho_\Gamma^* \cap (\rho_{N_\lambda}^*)^{-1}(\rho_{N_\lambda}^*(\ker \rho_\Gamma^* \cap \ker \rho_\Lambda)) < \ker \rho_\Lambda$$

as needed. □

We note that the above proof makes no use of the assumption $g = 0$, provided one knows Proposition 3.1 for $\mathrm{Push}(\pi_1(S_{g,n-1}))$. Indeed, the above proof is entirely formal, in the following sense. Assume that we have a surjective homomorphism

$$\psi \colon G < \mathrm{Out}(\Lambda) \longrightarrow H < \mathrm{Out}(\Gamma)$$

with kernel $K = \ker \psi$. If K, H have the congruence subgroup property (K needs to satisfying the a priori stronger condition as in Scholium 3.2) and the ψ-pullback of congruence groups in H are congruence subgroups of G, then G has the congruence subgroup property.

5. Proof of Proposition 3.1

We now prove Proposition 3.1; after reading the proof, the reader will easily see our proof yields Scholium 3.2. The proof is split into two steps. First, we reduce Proposition 3.1 to a purely group theoretic problem using Lemma 2.2. Using elementary methods, we then solve the associated group theoretic problem. Keep in mind that one of our main goals is keeping the proof of Theorem 1.1 as elementary as possible by which we mean mainly the avoidance of profinite methods. The trade off is that our arguments are longer. A good example of this trade off is our proof of Lemma 5.5 in comparison to [1, Lemma 1], [4, Lemma 2.6], or [13, Proposition 2.7].

Given a finite index subgroup Γ_0 of $\pi_1(S_{0,n-1})$, we first pass to a finite index normal (in $\pi_1(S_{0,n-1})$) subgroup Γ of Γ_0 with associated homomorphism

$$\rho_\Gamma \colon \pi_1(S_{0,n-1}) \to \pi_1(S_{0,n-1})/\Gamma = P_0.$$

It suffices to show that Γ is a congruence subgroup and this will now be our goal.

Step 1. We first describe congruence subgroups in $\pi_1(S_{0,n-1})$. Given a geometrically characteristic subgroup Δ of $\pi_1(S_{0,n})$ with associated homomorphism

$$\rho_\Delta \colon \pi_1(S_{0,n}) \to \pi_1(S_{0,n})/\Delta = Q,$$

we obtain a geometrically characteristic subgroup Γ of $\pi_1(S_{0,n-1})$ via the commutative diagram

$$\begin{tikzcd} \pi_1(S_{0,n}) \arrow[r, "\rho_{N_\lambda}"] \arrow[d, "\rho_\Delta"'] & \pi_1(S_{0,n-1}) \arrow[d, "\rho_\Gamma"] \\ Q \arrow[r, "\rho_{\rho_\Delta(N_\lambda)}"'] & Q/\rho_\Delta(N_\lambda) = P_0. \end{tikzcd} \tag{5}$$

In addition, we have the homomorphism

$$\overline{\mu} \colon P_0 \longrightarrow \mathrm{Inn}(P_0) = P_0/Z(P_0),$$

where $Z(P_0)$ is the center of P_0. We would like, as before, to define a homomorphism

$$\overline{\delta} \colon \mathrm{Out}_c(Q) \longrightarrow \mathrm{Aut}_c(P_0)$$

that relates $\rho_\Delta^* \circ \mathrm{Push}$ and $\overline{\mu} \circ p_0$. Proceeding as before, we define the map

$$\overline{\delta} \colon \mathrm{Out}_c(Q) \longrightarrow \mathrm{Aut}_c(P_0).$$

Unfortunately, $\overline{\delta}$ need not be a homomorphism. To be precise, we set $\mathrm{Aut}_c(Q)$ to be the subgroup of $\mathrm{Aut}(Q)$ of automorphisms that preserve the conjugacy classes $[\rho_\Delta(\gamma_1)], \dots, [\rho_\Delta(\gamma_{n-2})], [\rho_\Delta(\lambda)]$ and

$$\mathrm{Out}_c(Q) = \mathrm{Aut}_c(Q)/\mathrm{Inn}(Q).$$

Similarly, $\mathrm{Aut}_c(P_0)$ is the subgroup of $\mathrm{Aut}(P_0)$ that preserve the classes $[\rho_\Gamma(\gamma_1)], \dots, [\rho_\Gamma(\gamma_{n-2})]$. We take a normalized section

$$\overline{s} \colon \mathrm{Out}_c(Q) \longrightarrow \mathrm{Aut}_c(Q)$$

by mandating that $s(\tau)(\rho_\Delta(\lambda)) = \rho_\Delta(\lambda)$ and then apply the homomorphism

$$\rho^\star_{\rho_\Delta(N_\lambda)} \colon \mathrm{Aut}_c(Q) \longrightarrow \mathrm{Aut}_c(P_0)$$

induced by the homomorphism $\rho_{\rho_\Delta(N_\lambda)}$. The ambiguity in the selection of the section $\overline{s}$ is up to multiplication by the subgroup $\overline{\mu}(C_Q(\rho_\Delta(\lambda)))$ of

$\mathrm{Inn}(Q)$, the image of the centralizer of $\rho_\Delta(\lambda)$ in Q under $\overline{\mu}$. Provided $C_Q(\rho_\Delta(\lambda))$ maps to the trivial subgroup under $\rho_{\rho_\Delta(N_\lambda)}$, the resulting map

$$\overline{\delta}\colon\ \mathrm{Out}_c(Q) \longrightarrow \mathrm{Aut}_c(P_0)$$

given by $\overline{\delta} = \rho^\star_{\rho_\Delta(N_\lambda)} \circ \overline{s}$ is a homomorphism.

Lemma 5.1. *If $C_Q(\rho_\Delta(\lambda)) < \rho_\Delta(N_\lambda)$, then $\overline{\delta}$ is a homomorphism and $\overline{\delta} \circ \rho^*_\Delta \circ \mathrm{Push} = \overline{\mu} \circ \rho_\Gamma$.*

Proof. The essence of this lemma is that in the diagram

(6)

$$\begin{tikzcd}
 & & & \mathrm{Out}_c(Q) \arrow[d, "\overline{s}"] \arrow[ddr, "\overline{\delta}"] & \\
 & \mathrm{Out}_c(\pi_1(S_{0,n})) \arrow[r, "s"'] \arrow[urr, "\rho^*_\Delta"] \arrow[dr, "\delta"'] & \mathrm{Aut}_c(\pi_1(S_{0,n})) \arrow[r, "\rho^\star_\Delta"] \arrow[d, "\rho^\star_{N_\lambda}"] & \mathrm{Aut}_c(Q) \arrow[dr, "\rho^\star_{\rho_\Delta(N_\lambda)}"] & \\
\pi_1(S_{0,n-1}) \arrow[ur, "\mathrm{Push}"] \arrow[rr, "\mu"] \arrow[dr, "\rho_\Gamma"'] & & \mathrm{Aut}_c(\pi_1(S_{0,n-1})) \arrow[rr, "\rho^\star_\Gamma"] & & \mathrm{Aut}_c(P_0) \\
 & P_0 \arrow[urrr, "\overline{\mu}"'] & & &
\end{tikzcd}$$

we can push the bottom map $\overline{\mu} \circ \rho_\Gamma$ through to the top map $\overline{\delta} \circ \rho^*_\Delta \circ \mathrm{Push}$. The chief difficulty in proving this assertion is the noncommutativity of the top most square ((10) below) in (6). To begin, the diagrams

(7)
$$\begin{tikzcd}
\pi_1(S_{0,n-1}) \arrow[r, "\mu"] \arrow[d, "\rho_\Gamma"'] & \mathrm{Aut}_c(\pi_1(S_{0,n-1})) \arrow[d, "\rho^*_\Gamma"] \\
P_0 \arrow[r, "\overline{\mu}"'] & \mathrm{Aut}_c(P_0)
\end{tikzcd}$$

and

(8)
$$\begin{tikzcd}
\mathrm{Aut}_c(\pi_1(S_{0,n})) \arrow[r, "\rho^\star_{N_\lambda}"] \arrow[d, "\rho^\star_\Delta"'] & \mathrm{Aut}_c(\pi_1(S_{0,n-1})) \arrow[d, "\rho^\star_\Gamma"] \\
\mathrm{Aut}_c(Q) \arrow[r, "\rho^\star_{\rho_\Delta(N_\lambda)}"'] & \mathrm{Aut}_c(P_0)
\end{tikzcd}$$

commute. The commutativity of (7) and (8) in tandem with Lemma 2.2 yield the following string of functional equalities:

$$\begin{aligned}
\overline{\mu} \circ \rho_\Gamma &= \rho^\star_\Gamma \circ \mu && \text{(by (7))} \\
&= \rho^\star_\Gamma \circ \delta \circ \mathrm{Push} && \text{(by Lemma 2.2)} \\
&= \rho^\star_\Gamma \circ \rho^\star_{N_\lambda} \circ s \circ \mathrm{Push} && \text{(by definition of } \delta\text{)} \\
&= \rho^\star_{\rho_\Delta(N_\lambda)} \circ \rho^\star_\Delta \circ s \circ \mathrm{Push} && \text{(by (8)).}
\end{aligned}$$

We claim that

$$\rho^{\star}_{\rho_\Delta(N_\lambda)} \circ \overline{s} \circ \rho^{*}_{\Delta} = \rho^{\star}_{\rho_\Delta(N_\lambda)} \circ \rho^{\star}_{\Delta} \circ s \tag{9}$$

holds. However, since the diagram

$$\begin{tikzcd} \mathrm{Aut}_c(\pi_1(S_{0,n})) \arrow[r, "\rho^{\star}_{\Delta}"] & \mathrm{Aut}_c(Q) \\ \mathrm{Out}_c(\pi_1(S_{0,n})) \arrow[u, "s"] \arrow[r, "\rho^{*}_{\Delta}"'] & \mathrm{Out}_c(Q) \arrow[u, "\overline{s}"'] \end{tikzcd} \tag{10}$$

need not commute, to show (9), we must understand the failure of (10) to commute. Note that the validity of (9) amounts to showing the failure of the commutativity of (10), namely $(\rho^{\star}_{\Delta}(s(\tau)))^{-1}\overline{s}(\rho^{*}_{\Delta}(\tau))$, resides in the kernel of $\rho^{\star}_{\rho_\Delta(N_\lambda)}$. To that end, set

$$\theta\colon \mathrm{Aut}_c(\pi_1(S_{0,n})) \longrightarrow \mathrm{Out}_c(\pi_1(S_{0,n}))$$

and

$$\overline{\theta}\colon \mathrm{Aut}_c(Q) \longrightarrow \mathrm{Out}_c(Q)$$

to be the homomorphisms induced by reduction modulo the subgroups $\mathrm{Inn}(\pi_1(S_{0,n}))$ and $\mathrm{Inn}(Q)$, respectively. As s and $\overline{s}$ are normalized sections of θ and $\overline{\theta}$, we have

$$\theta \circ s = \mathrm{Id}, \quad \overline{\theta} \circ \overline{s} = \mathrm{Id}. \tag{11}$$

The commutativity of the diagram

$$\begin{tikzcd} \mathrm{Aut}_c(\pi_1(S_{0,n})) \arrow[r, "\rho^{\star}_{\Delta}"] \arrow[d, "\theta"'] & \mathrm{Aut}_c(Q) \arrow[d, "\overline{\theta}"] \\ \mathrm{Out}_c(\pi_1(S_{0,n})) \arrow[r, "\rho^{*}_{\Delta}"'] & \mathrm{Out}_c(Q) \end{tikzcd}$$

with (11) yields

$$\overline{\theta} \circ \rho^{\star}_{\Delta} \circ s = \rho^{*}_{\Delta}, \quad \overline{\theta} \circ \overline{s} \circ \rho^{*}_{\Delta} = \rho^{*}_{\Delta}. \tag{12}$$

Since $s(\tau)(\lambda) = \lambda$ and $\overline{s}(\overline{\tau})(\rho_\Delta(\lambda)) = \rho_\Delta(\lambda)$, we also have

$$\rho^{\star}_{\Delta}(s(\tau))(\rho_\Delta(\lambda)) = \overline{s}(\rho^{*}_{\Delta}(\tau))(\rho_\Delta(\lambda)) = \rho_\Delta(\lambda).$$

This equality in combination with (12) imply that $\rho^{\star}_{\Delta}(s(\tau))$ and $\overline{s}(\rho^{*}_{\Delta}(\tau))$ differ by multiplication by an element of $\overline{\mu}(C_Q(\rho_\Delta(\lambda)))$. Equivalently, the element

$$(\rho^{\star}_{\Delta}(s(\tau)))^{-1}\overline{s}(\rho^{*}_{\Delta}(\tau)),$$

which measures the failure of the commutativity of (10), resides in the subgroup $\overline{\mu}(C_Q(\rho_\Delta(\lambda)))$. However, by assumption, $C_Q(\rho_\Delta(\lambda)) < \ker \rho_{\rho_\Delta(N_\lambda)}$

and so we have the equality claimed in (9). Continuing our string of functional equalities started prior to (9), the following string of functional equalities completes the proof:

$$\begin{aligned}\overline{\mu}\circ\rho_\Gamma &= \rho^\star_{\rho_\Delta(N_\lambda)}\circ\rho^\star_\Delta\circ s\circ\mathrm{Push} && \text{(by the computation above)}\\ &= \rho^\star_{\rho_\Delta(N_\lambda)}\circ\overline{s}\circ\rho^*_\Delta\circ\mathrm{Push} && \text{(by (9))}\\ &= \overline{\delta}\circ\rho^*_\Delta\circ\mathrm{Push} && \text{(by definition of } \overline{\delta}\text{).} \qquad\square\end{aligned}$$

Definition 5.2. Given a finite index normal subgroup Γ of $\pi_1(S_{0,n-1})$ with associated homomorphism $\rho_\Gamma\colon \pi_1(S_{0,n-1})\to P_0$, we say ρ_Γ is *induced by* $\pi_1(S_{0,n})$ if

(a) ρ_Γ arises as in (5) from a geometrically characteristic subgroup Δ of $\pi_1(S_{0,n})$.
(b) The map $\overline{\delta}$ is a homomorphism; equivalently

$$C_Q(\rho_\Delta(\lambda)) < \ker\rho_{\rho_\Delta(N_\lambda)}.$$

Under these assumptions, by Lemma 5.1,

$$\overline{\delta}\circ\rho^*_\Delta\circ\mathrm{Push} = \overline{\mu}\circ\rho_\Gamma.$$

Consequently,

$$\ker(\rho^*_\Delta\circ\mathrm{Push}) < \ker(\overline{\mu}\circ\rho_\Gamma).$$

The following immediate corollary justifies our interest in subgroups induced by $\pi_1(S_{0,n})$.

Corollary 5.3. *If Γ is a finite index normal subgroup of $\pi_1(S_{0,n-1})$ has associated homomorphism ρ_Γ induced by $\pi_1(S_{0,n})$, then* $\ker(\overline{\mu}\circ\rho_\Gamma)$ *is a congruence subgroup.*

By Corollary 5.3, we have reduced the proof of Proposition 3.1 to the proof of the following lemma.

Lemma 5.4. *Let Γ be a finite index normal subgroup of $\pi_1(S_{0,n-1})$. Then there exists a finite index normal subgroup Γ' of $\pi_1(S_{0,n-1})$ whose associated homomorphism $\rho_{\Gamma'}$ is induced by $\pi_1(S_{0,n})$ and* $\ker(\overline{\mu}\circ\rho_{\Gamma'}) < \Gamma$.

Step 2. The proof of Lemma 5.4 will also be split into two parts. This division is natural in the sense that we need to produce a homomorphism induced by $\pi_1(S_{0,n})$ and also control the center of the target of the induced homomorphism. We do the latter first via our next lemma as this lemma is only needed at the very end of the proof of Lemma 5.4. In addition, some of the ideas used in the proof will be employed in the proof of Lemma 5.4 (see [13, Proposition 2.7] for a more general result).

Lemma 5.5. *Let $p\colon \pi_1(S_{0,n-1})\longrightarrow P$ be a surjective homomorphism with $|P|<\infty$ and $n>3$. Then there exists a finite extension P_0 of P and a* *surjective homomorphism* $p_0 \colon \pi_1(S_{0,n-1}) \longrightarrow P_0$ *such that the diagram*

$$\begin{tikzcd} \pi_1(S_{0,n-1}) \arrow[r, "p"] \arrow[dr, "p_0"'] & P \\ & P_0 \arrow[u] \end{tikzcd}$$

commutes and $Z(P) = 1$.

Before proving this lemma, we again note that the lemma is a formal result. Namely, every rank $r > 1$ finite group has a rank r finite extension with trivial center. The proof below proves precisely this statement.

Proof. First note that if P is cyclic, then $\ker p$ contains the kernel of the homology map $\pi_1(S_{0,n-1}) \to H_1(S_{0,n-1}, \mathbf{Z}/m\mathbf{Z})$ for some m. In this case, we replace P with $H_1(S_{0,n-1}, \mathbf{Z}/m\mathbf{Z})$. Since $n > 3$, the group $H_1(S_{0,n-1}, \mathbf{Z}/m\mathbf{Z})$ is not cyclic and so we may assume P is not cyclic. For a fixed prime ℓ, let V_ℓ denote the $\mathbf{F}_\ell$-group algebra of P where $\mathbf{F}_\ell$ is the finite field of prime order ℓ. Recall

$$V_\ell = \left\{ \sum_{p' \in P} \alpha_{p'} p', \quad \alpha_{p'} \in \mathbf{F}_\ell \right\}$$

is an $\mathbf{F}_\ell$-vector space with basis P and algebra structure given by polynomial multiplication. The group P acts by left multiplication on V_ℓ and this action yields the split extension $V_\ell \rtimes P$. Let $p(\gamma_j) = p_j$ and set R_ℓ to be the subgroup $V_\ell \rtimes P$ generated by

$$\{(1, p_1), (0, p_2), \dots, (0, p_{n-2})\} = \{r_1, r_2, \dots, r_{n-2}\}.$$

We have a surjective homomorphism $r \colon \pi_1(S_{0,n-1}) \to R_\ell$ given by $r(\gamma_j) = r_j$. If p_1 has order k_1, note that

$$r_1^{k_1} = (1, p_1)^{k_1} = (1 + p_1 + \cdots + p_1^{k_1 - 1}, 1).$$

Now assume that $r' \in Z(R_\ell)$ is central and of the form (v, p'). It follows that $p' \in Z(P)$ and

$$v + p'(1 + p_1 + \cdots + p_1^{k_1-1}) = v + (1 + p_1 + \cdots + p_1^{k_1-1}).$$

Canceling v from both side, we see that

$$p' + p'p_1 + \cdots + p'p_1^{k_1-1} = 1 + p_1 + \cdots + p_1^{k_1-1}.$$

In particular, there must be some power k such that $p'p_1^k = 1$ and so $p' \in \langle p_1 \rangle$. Next, set W_ℓ to be the $\mathbf{F}_\ell$-group algebra of R_ℓ and let S_ℓ be the subgroup of $W_\ell \rtimes R_\ell$ generated by the set

$$\begin{aligned} \{(1,(1,p_1)), (0,(0,p_2)), \dots, (0,(0,p_{n-2}))\} &= \{(1, r_1), (0, r_2), \dots, (0, r_{n-2})\} \\ &= \{s_1, s_2, \dots, s_{n-2}\}. \end{aligned}$$

We again have a surjective homomorphism $s\colon \pi_1(S_{0,n-1}) \to S_\ell$ given by $s(\gamma_j) = s_j$. As before, if $s' \in Z(S_\ell)$ is central and of the form (w, r'), then $r' \in Z(R_\ell)$ and $r' \in \langle r_1 \rangle$. In particular, for some $k \leq |r_1|$, we have

$$r' = (1 + p_1 + \cdots + p_1^{k-1}, p_1^k).$$

Since $r' \in Z(R_\ell)$, we have

$$r_j r' = (0, p_j) r' = r'(0, p_j) = r' r_j$$

for $j > 1$. This equality yields the equation

$$p_j(1 + p_1 + \cdots + p_1^{k-1}) = 1 + p_1 + \cdots + p_1^{k-1}.$$

As before, this equality implies $p_j \in \langle p_1 \rangle$ for all $j > 1$ since $k < |r_1|$. However, if this holds, P must be cyclic. As P is noncyclic, r' must be trivial and s' has the form $(w, 0)$. For $(w, 0)$ to be central in S_ℓ, we must have

$$(w, 0)(0, r_j) = (0, r_j)(w, 0)$$

for all $j \neq 1$ and

$$(w, 0)(1, r_1) = (1, r_1)(w, 0).$$

These equalities imply that $r_j w = w$ for $j = 1, \dots, n-2$. Since $\{r_j\}$ generate R_ℓ, the element w must be fixed by every element $r \in R_\ell$. However, the only vectors in W_ℓ that are fixed by every element of R_ℓ are of the form (see for instance [9, p. 37])

$$w_\alpha = \alpha \sum_{r \in R_\ell} r, \quad \alpha \in \mathbf{F}_\ell.$$

Let C be the normal cyclic subgroup $S_\ell \cap \langle (w_1, 0) \rangle$ of S_ℓ, $P_0 = S_\ell / C$, and $p_{j,\ell}$ be the image of s_j under this projection. By construction, P_0 is centerless and for the homomorphism

$$p_0\colon \pi_1(S_{0,n-1}) \longrightarrow P_0$$

given by $p_0(\gamma_j) = p_{j,\ell}$, we have $\ker p_0 < \ker p$. To see the latter, we simply note that we have the commutative diagram

$$\begin{tikzcd}
\pi_1(S_{0,n-1}) \arrow[d, "s"'] \arrow[dr, "p_0"] \arrow[drr, "r"] \arrow[drrr, "p"] & & & \\
S_\ell \arrow[r] & P_0 \arrow[r] & R_\ell \arrow[r] & P,
\end{tikzcd}$$

where the bottom maps are given by

$$s_j \longmapsto p_{j,\ell} \longmapsto r_j \longmapsto p_j = p(\gamma_j). \qquad \square$$

We are now ready to prove Lemma 5.4.

Proof of Lemma 5.4. Given a normal subgroup Γ of $\pi_1(S_{0,n-1})$ of finite index, we must show that there exists a finite index normal subgroup Γ' of $\pi_1(S_{0,n-1})$ with associated homomorphism $\rho_{\Gamma'}$ that is induced by $\pi_1(S_{0,n})$ and $\ker(\overline{\mu}\circ\rho_{\Gamma'}) < \Gamma$. By Lemma 5.5, we may assume that $P = \pi_1(S_{0,n-1})/\Gamma$ is centerless. The homomorphism ρ_Γ provides us with a homomorphism

$$\rho_\Gamma \circ \rho_{N_\lambda} \colon \pi_1(S_{0,n}) \longrightarrow P.$$

Let U_ℓ be the $\mathbf{F}_\ell$-group algebra of P and define

$$\varphi\colon \pi_1(S_{0,n}) \longrightarrow U_\ell \rtimes P$$

by

$$\varphi(\lambda) = (1, \rho_\Gamma \circ \rho_{N_\lambda}(\lambda)), \quad \varphi(\gamma_j) = (0, \rho_\Gamma \circ \rho_{N_\lambda}(\gamma_j)).$$

Note that the normal closure (in $\varphi(\pi_1(S_{0,n}))$) of $\varphi(\lambda)$ contains the centralizer of $\varphi(\lambda)$. Indeed, the normal closure of $\varphi(\lambda)$ is simply $U_\ell \cap \varphi(\pi_1(S_{0,n}))$. If $(v,p') \in \varphi(\pi_1(S_{0,n}))$ commutes with $(1,1) = \varphi(\lambda)$, then

$$(v,p')(1,1) = (v+p',p') = (v+1,p') = (1,1)(v,p').$$

Thus, $p' = 1$ and $(v,p') \in U_\ell$. By construction, the diagram

$$\begin{array}{ccc} \pi_1(S_{0,n}) & \xrightarrow{\rho_{N_\lambda}} & \pi_1(S_{0,n-1}) \\ \varphi\downarrow & & \downarrow\rho_\Gamma \\ U_\ell \rtimes P & \xrightarrow[\rho_{U_\ell}]{} & P \end{array} \tag{13}$$

commutes. This representation is unlikely to have a geometrically characteristic kernel. We rectify that as follows. Let $\mathcal{O}_\varphi$ denote the orbit of φ under the action of $\mathrm{Aut}_c(\pi_1(S_{0,n}))$ on $\mathrm{Hom}(\pi_1(S_{0,n}), U_\ell \rtimes P)$ given by pre-composition. We define a new homomorphism

$$q\colon \pi_1(S_{0,n}) \longrightarrow Q < \bigoplus_{\varphi' \in \mathcal{O}_\varphi} U_\ell \rtimes P,$$

by

$$q = \bigoplus_{\varphi' \in \mathcal{O}_\varphi} \varphi'.$$

By construction, the kernel of this homomorphism is geometrically characteristic. In addition, each representation φ' has the property that the normal closure of $\varphi'(\lambda)$ contains the centralizer of $\varphi'(\lambda)$. Note that this follows from the fact that this containment holds for φ and the homomorphism φ' is equal to $\varphi \circ \tau$ for some $\tau \in \mathrm{Aut}_c(\pi_1(S_{0,n}))$. As τ preserves the conjugacy class $[\lambda]$, $\varphi'(\lambda)$ is conjugate to $\varphi(\lambda)$ in $U_\ell \rtimes P$. Let Γ' be the finite index normal subgroup of $\pi_1(S_{0,n-1})$ with associated homomorphism $\rho_{\Gamma'}$ induced by the homomorphism q. Namely we have the diagram

$$\begin{tikzcd} \pi_1(S_{0,n}) \arrow[r, "\rho_{N_\lambda}"] \arrow[d, "q"'] & \pi_1(S_{0,n-1}) \arrow[d, "\rho_{\Gamma'}"] \\ Q \arrow[r, "\rho_{q(N_\lambda)}"'] & Q/q(N_\Lambda) = P_0. \end{tikzcd}$$

We assert that we have the inclusion $\ker(\overline{\mu} \circ \rho_{\Gamma'}) < \Gamma$. To see this containment, we first observe that

$$Q/q(N_\lambda) = P_0 < \bigoplus_{\varphi' \in \mathcal{O}_\varphi} \varphi'(\pi_1(S_{0,n}))/\varphi'(N_\lambda) = \bigoplus_{\varphi' \in \mathcal{O}_\varphi} P.$$

Composing with the projection map π_φ onto the factor $\varphi(\pi_1(S_{0,n}))$ associated with φ, we get the commutative diagram

$$\begin{tikzcd} \pi_1(S_{0,n}) \arrow[r, "q"] \arrow[d, "\rho_{N_\lambda}"'] & Q \arrow[r, "\pi_\varphi"] \arrow[d, "\rho_{q(N_\lambda)}"] & U_\ell \rtimes P \arrow[d, "\rho_{U_\ell}"] \\ \pi_1(S_{0,n-1}) \arrow[r, "\rho_{\Gamma'}"'] & P_0 \arrow[r, "\pi_\varphi"'] & P. \end{tikzcd} \tag{14}$$

Now, if $\gamma \in \ker(\overline{\mu} \circ \rho_{\Gamma'})$, then $\rho_{\Gamma'}(\gamma)$ is central in P_0. As central elements map to central elements under homomorphisms, $\pi_\varphi(\rho_{\Gamma'}(\gamma))$ must be central in P. However, by assumption P is centerless and so $\pi_\varphi(\rho_{\Gamma'}(\gamma)) = 1$. Since $\pi_\varphi \circ \rho_{\Gamma'} = p$ by (13) and (14), we see that $\rho_\Gamma(\gamma) = 1$. Therefore,

$$\ker(\overline{\mu} \circ \rho_{\Gamma'}) < \Gamma. \qquad \square$$

The construction above only uses that $\pi_1(S_{0,n-1})$ is a free group in the proof of Lemma 5.5. With more care, the same method used in the proof of Lemma 5.5 can be used to prove the following (for $g = 1$, we must assume $n > 1$)—this again follows from [13, Proposition 2.7].

Lemma 5.6. *Let $p\colon \pi_1(S_{g,n-1}) \longrightarrow P$ be a surjective homomorphism with $|P| < \infty$ and $n > 3$ if $g = 0$, $n > 0$ if $g = 1$. Then there exists a finite extension P_0 of P and a surjective homomorphism $p_0\colon \pi_1(S_{g,n-1}) \longrightarrow P_0$ such that the diagram*

$$\begin{tikzcd} \pi_1(S_{g,n-1}) \arrow[r, "p"] \arrow[dr, "p_0"'] & P \\ & P_0 \arrow[u] \end{tikzcd}$$

commutes and $Z(P) = 1$.

The issue in proving this lemma versus the proof of Lemma 5.5 is that we must take additional care in selecting the vector components in the $\mathbf{F}_\ell$-group algebra of P in order to produce a homomorphism into $V_\ell \rtimes P$; there are nontrivial relations that must be satisfied now. Unwrapping [13] in this context, this selection corresponds to a nontrivial solution of an $\mathbf{F}_\ell$-linear system. The condition required in the proof of Proposition 2.7 in [13] ensures the dimension of the solution space is positive. Specifically, they require a positive deficiency of the presentation (more generators than relations), a condition that holds for the standard representation of a closed surface group. For example, if we take the presentation

$$\{\alpha_1, \beta_1, \alpha_2, \beta_2 \ : \ [\alpha_1, \beta_1][\alpha_2, \beta_2]\}$$

for the genus two surface group and are given a homomorphism of the surface group to a finite group P_0 with

$$\alpha_j \mapsto A_j, \quad \beta_j \mapsto B_j, \quad A_j, B_j \in P_0.$$

Setting V_ℓ to be the $\mathbf{F}_\ell$-group algebra of P_0 and sending

$$\alpha_j \mapsto (v_j, A_j), \quad \beta_j \mapsto (w_j, B_j) < V_\ell \rtimes P_0,$$

we must have the (linear) equation hold in order for the map into $V_\ell \rtimes P_0$ to be a homomorphism:

$$\begin{aligned}(1 - A_1B_1A_1^{-1})v_1 + (A_1 - [A_1, B_1])w_1 + ([A_1, B_1](1 - A_2B_2A_2^{-1}))v_2 \\ + ([A_1, B_1]A_2B_2 - 1)w_2 = 0.\end{aligned}$$

We can, for instance, select $v_2 = w_1 = w_2 = 0$ and $v_1 = v = B_1^{-1}[A_2, B_2]$. In fact, for higher genus surface groups, setting all v_j, w_j to zero except for v_1, we can make the selection $v_1 = B_1^{-1}[A_2, B_2] \dots [A_g, B_g]$. Another choice would be to set $v_1 = v_2 = w_1 = 0$ and $w_2 = A_2^{-1}B_2^{-1}$ and for higher genus setting $w_2 = A_2^{-1}B_2^{-1}[A_3, B_3] \dots [A_g, B_g]$. With any of these selections, the same argument employed in the free case yields a proof of Lemma 5.6. In total, this yields an elementary proof of the following—this also follows from [13, Lemma 2.6].

Proposition 5.7. $\mathrm{Push}(\pi_1(S_{g,n-1}))$ *has the congruence subgroup property (when* $g = 1$, $n > 1$*).*

Finally, since the proof of Proposition 3.3 does not require $g = 0$, we have an elementary proof of the following, which was also proved in [1, Theorem 2] and [4, Proposition 2.3].

Proposition 5.8. *If* $\mathrm{PMod}(S_{g,n-1})$ *has the congruence subgroup property, then* $\mathrm{PMod}(S_{g,n})$ *has the congruence subgroup property.*

6. Comparison of the proofs

We conclude this article with a more detailed comparison of the proofs of Theorem 1.1. Instead of using the homomorphisms $\overline{\delta}$ employed above, Asada extends the homomorphism δ to

$$\widehat{\delta}\colon \mathrm{Out}_c(\widehat{\pi_1(S_{g,n})}) \longrightarrow \mathrm{Aut}_c(\widehat{\pi_1(S_{g,n-1})}).$$

The group $\mathrm{Aut}_c(\widehat{\pi_1(S_{g,n})})$, for any n, is the group of continuous automorphisms of the profinite completion $\widehat{\pi_1(S_{g,n})}$ that preserve the conjugacy classes $[\gamma_j]$ and $[\lambda]$. We set $\mathrm{Out}_c(\widehat{\pi_1(S_{g,n})}) = \mathrm{Aut}_c(\widehat{\pi_1(S_{g,n})})/\,\mathrm{Inn}(\widehat{\pi_1(S_{g,n})})$. This extension is defined as before, though some care is needed in showing $\widehat{\delta}$ is a homomorphism. The result of the construction of $\widehat{\delta}$ yields a relationship similar to Lemma 2.2 and is equivalent to our Step 1. The final ingredient needed is the fact that $Z(\widehat{\pi_1(S_{g,n})})$ is trivial, which is equivalent to Lemma 5.5. Indeed, we have a sequence

$$\widehat{\pi_1(S_{g,n-1})} \xrightarrow{\widehat{\mathrm{Push}}} \mathrm{Out}_c(\widehat{\pi_1(S_{g,n})}) \xrightarrow{\widehat{\rho^*_{N_\lambda}}} \mathrm{Out}_c(\widehat{\pi_1(S_{g,n-1})}) \longrightarrow 1.$$

Proposition 3.1 is equivalent to the injectivity of $\widehat{\mathrm{Push}}$. The homomorphism $\widehat{\delta}$ relates this profinite version of (2) to the profinite version of (1)

$$\widehat{\pi_1(S_{g,n-1})} \xrightarrow{\widehat{\mu}} \mathrm{Aut}_c(\widehat{\pi_1(S_{g,n-1})}) \longrightarrow \mathrm{Out}_c(\widehat{\pi_1(S_{g,n-1})}) \longrightarrow 1.$$

Specifically, the relationship is

$$\widehat{\mu} = \widehat{\delta} \circ \widehat{\mathrm{Push}}. \tag{15}$$

Thus, the injectivity of $\widehat{\mathrm{Push}}$ follows from the triviality of $Z(\widehat{\pi_1(S_{g,n-1})})$. Note that it is not obvious that (15) holds and this was established in [14]. The content of Step 1 and parts of Step 2 reprove (15). Boggi's proof [4, p. 4–5] is essentially the same Asada's proof though with different language and different notation that might initially veil the similarities. His analysis of centralizers in $\widehat{\pi_1(S_{g,n})}$ is different as he makes use of cohomological dimension and Shapiro's Lemma. Like the other two proofs, he also makes use of the homomorphism $\widehat{\delta}$. To summarize, in all of the proofs mentioned above, the main thrust is the reduction of Proposition 3.1 to a group theoretic statement like Lemma 5.4 followed by an argument that controls centers like Lemma 5.5.

The proof given by Diaz–Donagi–Harbater [6] also requires control of symmetries and a generalization of a group theoretic analog of their proof is given in [7]. However, their proof is sufficiently different from the rest as it is more geometric in nature.

Boggi's general framework for the congruence subgroup problem introduced in [3] and [4] is a step in resolving the congruence subgroup problem in general. Despite the gap in [3], his work has introduced new tools and also he proves results that may be of independent interest to algebraic geometers, geometric group theorists, and geometers. Those with interests in these fields should study his work at far greater depth than what has been presented in this article. The recent article of Kent [11] is a beautiful introduction to the current state and parallels the approach to the congruence subgroup problem in the linear setting.

References

[1] Asada, Mamoru. The faithfulness of the monodromy representations associated with certain families of algebraic curves. *J. Pure Appl. Algebra* **159** (2001), no. 2–3, 123–147. MR1828935 (2002c:14040), Zbl 1045.14013, doi: 10.1016/S0022-4049(00)00056-6.

[2] Bass, Hyman; Lubotzky, Alexander. Automorphisms of groups and of schemes of finite type. *Israel J. Math.* **44** (1983), no. 1, 1–22. MR0693651 (84i:14031), Zbl 0517.14015, doi: 10.1007/BF02763168.

[3] Boggi, Marco. Profinite Teichmüller theory. *Math. Nachr.* **279** (2006), no. 9–10, 953–987. MR2242960 (2008f:14037), Zbl 1105.14031, doi: 10.1002/mana.200510405.

[4] Boggi, Marco. The congruence subgroup property for the hyperelliptic modular group: the open surface case. *Hiroshima Math. J.* **39** (2009), no. 3, 351–362. MR2569009 (2011a:14049), Zbl 1209.14023.

[5] Bux, Kai-Uwe; Ershov, Mikhail V.; Rapinchuk, Andrei S. The congruence subgroup property for $\mathrm{Aut}(F_2)$: a group-theoretic proof of Asada's theorem. *Groups Geom. Dyn.* **5** (2011), no. 2, 327–353. MR2782176 (2012c:20099), Zbl 1251.20035, arXiv:0909.0304v2, doi: 10.4171/GGD/130.

[6] Diaz, Steven; Donagi, Ron; Harbater, David. Every curve is a Hurwitz space. *Duke Math. J.* **59** (1989), no. 3, 737–746. MR1046746 (91i:14021), Zbl 0712.14013, doi: 10.1215/S0012-7094-89-05933-4.

[7] Ellenberg, J. S.; McReynolds, D. B. Every curve is a Teichmüller curve. *Duke J. Math.* **161** (2012), 415–429.

[8] Farb, Benson; Margalit, Dan. A primer on mapping class groups. Princeton Mathematical Series, 49. *Princeton University Press, Princeton, NJ*, 2012. xiv+472 pp. ISBN: 978-0-691-14794-9. MR2850125 (2012h:57032), Zbl 1245.57002.

[9] Fulton, William; Harris, Joe. Representation theory. A first course. Graduate Texts in Mathematics, 129. Readings in Mathematics. *Springer-Verlag, New York*, 1991. xvi+551 pp. ISBN: 0-387-97527-6; 0-387-97495-4. MR1153249 (93a:20069), Zbl 0744.22001.

[10] Ivanov, Nikolai V. Fifteen problems about the mapping class groups. *Problems on mapping class groups and related topics*, 71–80. Proc. Sympos. Pure Math., 74. *Amer. Math. Soc., Providence, RI*, 2006. MR2264532 (2008b:57003), Zbl 05124675, arXiv:math/0608325.

[11] Kent, R. P. Congruence kernels around affine curves. Preprint. arXiv:1109.1267v2.

[12] Kent, R. P.; Wieland, B. Approaching the congruence subgroup problem for mapping class groups. In preparation.

[13] Lubotzky, Alexander; Shalom, Yehuda. Finite representations in the unitary dual and Ramanujan groups. *Discrete geometric analysis*, 173–189. Contemp. Math., 347. *Amer. Math. Soc., Providence, RI*, 2004. MR2077037 (2005e:22011) Zbl 1080.22006.

[14] Nakamura, Hiroaki; Tsunogai, Hiroshi. Some finiteness theorems on Galois centralizers in pro-l mapping class groups. *J. Reine Angew. Math.* **441** (1993), 115–144. MR1228614 (94g:14005), Zbl 0771.14006.

[15] Thurston, W. P. Commmunication to N. Dunfield, 2002.

Department of Mathematics, Purdue University, West Lafayette, IN 47906
dmcreyno@math.purdue.edu

This paper is available via `http://nyjm.albany.edu/j/2012/18-47.html`.