Groups Geom. Dyn. 5 (2011), 327–353
DOI 10.4171/GGD/130

Groups, Geometry, and Dynamics
© European Mathematical Society

The congruence subgroup property for Aut F_2: A group-theoretic proof of Asada's theorem

Kai-Uwe Bux, Mikhail V. Ershov[1] and Andrei S. Rapinchuk[2]

To Fritz Grunewald

Abstract. The goal of this paper is to give a group-theoretic proof of the congruence subgroup property for $\mathrm{Aut}(F_2)$, the group of automorphisms of a free group on two generators. This result was first proved by Asada using techniques from anabelian geometry, and our proof is, to a large extent, a translation of Asada's proof into group-theoretic language. This translation enables us to simplify many parts of Asada's original argument and prove a quantitative version of the congruence subgroup property for $\mathrm{Aut}(F_2)$.

Mathematics Subject Classification (2010). Primary 20F28, 20H05; Secondary 20E05, 20E07.

Keywords. Automorphism groups, free groups, congruence subgroup property.

1. Introduction

Let G be a finitely generated group, $\Gamma = \mathrm{Aut}\, G$ be its automorphism group. For a normal subgroup $K \subset G$ of finite index, we set

$$\Gamma[K] = \{\sigma \in \Gamma \mid \sigma(K) = K \text{ and } \sigma \text{ acts trivially on } G/K\}.$$

It is easy to see that $\Gamma[K]$ is a finite index subgroup of Γ. In fact, for $G = \mathbb{Z}^\ell$ we have $\Gamma = \mathrm{GL}_\ell(\mathbb{Z})$, and furthermore if $K = n\mathbb{Z}^\ell$ then $\Gamma[K] = \mathrm{GL}_\ell(\mathbb{Z}, n)$, the congruence subgroup modulo n. So, the following question is a natural analog of the classical congruence subgroup problem:

> Does every finite index subgroup of Γ contain a suitable congruence subgroup $\Gamma[K]$? (∗)

[1]The author would like to acknowledge partial support from the NSF grant DMS-0901703.

[2]The author would like to acknowledge partial support from the NSF grant DMS-0965758 and the Humboldt Foundation.

While there are numerous results on the congruence subgroup problem for arithmetic groups (cf. [10] for a recent survey), very little is known regarding $(*)$ for the automorphism groups of general groups. The purpose of this note is to give a short purely group-theoretic proof of Asada's result [3] that yields the congruence subgroup property (i.e., the affirmative answer to $(*)$) for $\Gamma = \mathrm{Aut}\, F_2$, the automorphism group of the free group $G = F_2$ of rank two. The original argument in [3] was based on the techniques involving Galois extensions of rational function fields of algebraic curves (this area is generally referred to as "anabelian geometry"), and according to some experts, no direct proof was known. The proof we present here is, by and large, a "translation" of Asada's argument into the group-theoretic language. One of the benefits of the translation is that some simplifications and shortcuts in Asada's argument became apparent making the resulting argument very short and, in some sense, even explicit (cf. §5). It also reveals the underlying idea of the method (which we call the "topsy-turvy effect", see Remark 4.5) so that it can potentially be applied to other automorphism groups and their subgroups.

Before formulating the result, we need to recall the standard reformulation of $(*)$ as a question about the comparison of two topologies on Γ. Let τ_{pf} (resp., τ_{c}) be the topology on Γ that admits the family of all subgroups of finite index in Γ (resp., the family of congruence subgroups $\Gamma[K]$ for all finite index subgroups $K \subset G$) as a fundamental system of neighborhoods of the identity.[1] Then τ_{c} is *a priori* weaker than τ_{pf}, and $(*)$ amounts to the question if these topologies are actually identical. Now let $\widehat{\Gamma}$ and $\overline{\Gamma}$ be the completions of Γ relative to τ_{pf} and τ_{c} respectively. Then yet another equivalent reformulation of $(*)$ is whether or not the natural map $\widehat{\Gamma} \to \overline{\Gamma}$ is injective. Clearly, $\widehat{\Gamma}$ is simply the profinite completion of Γ. On the other hand, it is easy to see that $\overline{\Gamma}$ can be identified with the closure of the image of the natural homomorphism $\mathrm{Aut}\, G \to \mathrm{Aut}\, \widehat{G}$ (cf. §3). So, our question becomes if the natural map $\widehat{\mathrm{Aut}\, G} \to \mathrm{Aut}\, \widehat{G}$ is injective. Here two remarks are in order. First, for a *profinite* group F we, of course, use $\mathrm{Aut}\, F$ to denote the group of *continuous* automorphisms of F; it is known however that if F is finitely generated then every abstract automorphism of F is automatically continuous [9]. Second, for a finitely generated profinite group F, the automorphism group $\mathrm{Aut}\, F$ is itself profinite (cf. §3), so the above homomorphism $\widehat{\mathrm{Aut}\, G} \to \mathrm{Aut}\, \widehat{G}$ actually results from the universal property of profinite completions applied to the homomorphism $\mathrm{Aut}\, G \to \mathrm{Aut}\, \widehat{G}$. Likewise, the outer automorphism group $\mathrm{Out}\, \widehat{G} = \mathrm{Aut}\, \widehat{G}/\mathrm{Int}\, \widehat{G}$ is also profinite, so the natural homomorphism $\mathrm{Out}\, G \to \mathrm{Out}\, \widehat{G}$ extends to a continuous homomorphism $\widehat{\mathrm{Out}\, G} \to \mathrm{Out}\, \widehat{G}$. We can now formulate the main result.

Main Theorem (cf. [3], Theorem 5). *For the free group F_2 on two generators, the natural homomorphism $\widehat{\mathrm{Out}\, F_2} \to \mathrm{Out}\, \widehat{F}_2$ is injective.*

[1] We note that τ_{c} can also be defined using the congruence subgroups $\Gamma[K]$ associated only to *characteristic* subgroups $K \subset G$ of finite index. For such K, $\Gamma[K] = \mathrm{Ker}(\Gamma \to \mathrm{Aut}(G/K))$, hence a *normal* subgroup of finite index in Γ.

The following is easily derived from the theorem (cf. Lemma 3.1).

Corollary. *The natural homomorphism* $\widehat{\mathrm{Aut}\, F_2} \to \mathrm{Aut}\, \hat{F}_2$ *is injective, hence* $\mathrm{Aut}\, F_2$ *has the congruence subgroup property.*

(We note that Asada's theorem was interpreted in [2], 1.4.2, as the statement that every finite index subgroup of $\Gamma = \mathrm{Aut}\, F_2$, containing $\mathrm{Int}\, F_2$, must contain a suitable congruence subgroup $\Gamma[K]$, but as we see, it in fact yields this property for *all* finite index subgroups, cf. also Remark 5.3 (3).)

The congruence subgroup property for $\mathrm{Aut}\, F_2$ can be used to establish the congruence subgroup property for certain subgroups (which are analogs of parabolic subgroups) of $\mathrm{Aut}\, F_n$ for $n \geqslant 3$ – we will address this issue elsewhere. On the other hand, the congruence subgroup problem for the group $\mathrm{Aut}\, F_n$, $n \geqslant 3$, itself remains widely open, and it does not appear that the argument for $n = 2$ can be easily extended to $n \geqslant 3$. It is interesting that the proof for $n = 2$ relies on the fact that $\mathrm{Out}\, F_2 \simeq \mathrm{GL}_2(\mathbb{Z})$ is a virtually free group, which is precisely what prevents $\mathrm{GL}_2(\mathbb{Z})$ from having the (usual) congruence subgroup property. The latter is a classical result known already to Klein and Fricke in the 19th century (cf. [10]).

The structure of the note is the following. In §2, we review the facts about profinite groups needed in the proof of the Main Theorem. This section is included for the reader's convenience as although these fact are known, for some of them it is not easy to find an impeccable reference. More importantly, the proofs we present, unlike the traditional proofs (cf., for example, [6]), are based not on the structure theory for profinite groups but rather on the analysis of finite quotients of (discrete) free groups and the associated relation modules. We will use this approach to give an "explicit" form of the Main Theorem in §5 (cf. Theorem 5.1). After some reductions in §3, we present the group-theoretic "translation" of Asada's argument in §4. Finally, in §6, we discuss the topological nature of a homomorphism involved in the proof of the Main Theorem. This theme is prominent in Asada's paper, however the explicit computation of this homomorphism in §6 (as opposed to its description in terms of Galois groups) reveals a shortcut used in §4.

2. Facts about profinite groups

We refer to [11] or [17] regarding basic notions, notations and results on profinite groups. In particular, the profinite completion of an abstract (discrete) group G will be denoted by $\hat{G}$. Thus, if $F = F(X)$ is the free group on a finite set X then $\mathfrak{F} := \hat{F}$ is the free profinite group on X (to be denoted $\mathfrak{F}(X)$). Given a subset S of a profinite group $\mathfrak{G}$, we will write $\hat{S}$ to denote its closure in $\mathfrak{G}$.

Lemma 2.1 (cf. [1], Proposition 3). *Let*

$$1 \to G_1 \xrightarrow{\alpha} G_2 \xrightarrow{\beta} G_3 \to 1$$

be an exact sequence of groups. Assume that G_1 is finitely generated and that its profinite completion $\widehat{G}_1$ has trivial center. Then the sequence of the profinite completions

$$1 \to \widehat{G}_1 \xrightarrow{\hat{\alpha}} \widehat{G}_2 \xrightarrow{\hat{\beta}} \widehat{G}_3 \to 1$$

is also exact.

Proof. We identify G_1 with a normal subgroup of G_2 and consider the conjugation action of the latter on the former. This action extends to an action of G_2 on $\widehat{G}_1$ giving rise to a homomorphism $G_2 \to \operatorname{Aut} \widehat{G}_1$. On the other hand, since G_1 is finitely generated, it is easy to see that the group $\operatorname{Aut} \widehat{G}_1$ is profinite (cf. the beginning of §3), so the homomorphism $G_2 \to \operatorname{Aut} \widehat{G}_1$ extends to a continuous homomorphism $\phi\colon \widehat{G}_2 \to \operatorname{Aut} \widehat{G}_1$ such that $\phi(\hat{\alpha}(x)) = \operatorname{Int} x$ for all $x \in \widehat{G}_1$. Now, given $x \in \widehat{G}_1$, $x \neq 1$, the assumption that $\widehat{G}_1$ has trivial center implies that $\operatorname{Int} x$ is nontrivial, hence $\hat{\alpha}(x) \neq 1$, proving that $\hat{\alpha}$ is injective.

Since $\beta(G_2) = G_3$, we have that $\hat{\beta}(\widehat{G}_2)$ is a compact dense subgroup of $\widehat{G}_3$, yielding the surjectivity of $\hat{\beta}$. Finally, β defines an isomorphism of $G_2/\operatorname{Im}\alpha$ onto G_3, and the inverse of this isomorphism gives rise to a natural map $G_3 \to \widehat{G}_2/\operatorname{Im}\hat{\alpha}$. It is easy to see that the latter satisfies the universal property for the profinite completion of G_3, which yields $\operatorname{Im}\hat{\alpha} = \operatorname{Ker}\hat{\beta}$, as required. □

The proof of the Main Theorem relies on the known results about the centralizers of generators and their commutators in free profinite groups. As we already mentioned in §1, for the purpose of giving an "explicit" version of the Main Theorem (cf. Theorem 5.1), we present the proofs of these results based on the analysis of finite quotients of free groups and their relation modules rather than on the structure theory of profinite groups (cf., for example, [6]).

Proposition 2.2. *Let $F = F(X)$ be the free group on $X = \{x_1, \ldots, x_n\}$, and let $G = F/N$ be a finite quotient of F. Fix a prime p not dividing the order of G, set $M = N^p[N, N]$ and let $\gamma\colon F/M \to F/N$ denote the canonical homomorphism. Then*

(i) *$\gamma(C_{F/M}(x_i M))$ coincides with the cyclic group $\langle x_i N\rangle$ for all $i = 1, \ldots, n$;*

(ii) *if $n > 1$ then for any abelian normal subgroup $C \subset F/M$ we have $\gamma(C) = \{e\}$.*

Proof. The proof uses some well-known properties of the relation module $\mathfrak{n} := N/[N, N]$ (cf. [5]). Namely, there is an exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to \mathfrak{n} \xrightarrow{\sigma} \mathbb{Z}[G]^n \xrightarrow{\tau} \mathfrak{g} \to 0 \tag{1}$$

where $\mathfrak{g}$ is the augmentation ideal in $\mathbb{Z}[G]$. We recall the construction of σ and τ. It is known that the augmentation ideal $\mathfrak{f} \subset \mathbb{Z}[F]$ is a free left $\mathbb{Z}[F]$-module with basis

$x_1 - 1, \ldots, x_n - 1$. So, for any $f \in F$, there is a unique presentation of the form

$$f - 1 = a_1(f)(x_1 - 1) + \cdots + a_n(f)(x_n - 1) \quad \text{with } a_i(f) \in \mathbb{Z}[F],$$

and then σ is defined by sending $f \in N$ to $(\overline{a_1(f)}, \ldots, \overline{a_n(f)}) \in \mathbb{Z}[G]^n$, where the bar denotes the image under the natural homomorphism $\mathbb{Z}[F] \to \mathbb{Z}[G]$. Furthermore, τ is defined by sending $(a_1, \ldots, a_n) \in \mathbb{Z}[G]^n$ to $\sum a_i(\bar{x}_i - 1)$. Since all terms in (1) are free $\mathbb{Z}$-modules, by tensoring with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we obtain the following exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \to \mathfrak{n}_p \xrightarrow{\sigma_p} \mathbb{F}_p[G]^n \xrightarrow{\tau_p} \mathfrak{g}_p \to 0 \tag{2}$$

where $\mathfrak{n}_p = \mathfrak{n} \otimes_{\mathbb{Z}} \mathbb{F}_p$ and $\mathfrak{g}_p = \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_p$. Clearly, $\mathfrak{n}_p = N/M$, and $\mathfrak{g}_p$ is the augmentation ideal in $\mathbb{F}_p[G]$. Since $p \nmid |G|$, exact sequence (2) splits, yielding an isomorphism of $\mathbb{F}_p[G]$-modules

$$N/M \simeq \mathbb{F}_p[G]^{n-1} \oplus \mathbb{F}_p, \tag{3}$$

where $\mathbb{F}_p$ is considered as the trivial $\mathbb{F}_p[G]$-module. Besides, since the order of G is relatively prime to that of N/M, there exists a semi-direct product decomposition $F/M \simeq N/M \rtimes G$, which we fix (it is not canonical). This enables us to view G as a subgroup of F/M.

We will now prove assertion (i). To keep our notations simple, we will write the argument for $i = 1$. Let $g \in C_{F/M}(x_1 M)$. Since $\langle g \rangle$ and $\langle g^{p^\ell} \rangle$, for any $\ell \geqslant 1$, have the same image under γ, it is enough to prove our claim assuming that the order of g is prime to p. Then there exists $h \in N/M$ such that $g' := hgh^{-1}$ belongs to G. Let d be the order of $\bar{x}_1$ in G. Then $y := x_1^d M \in N/M$, and, since g commutes with y and N/M is commutative, g' commutes with y. In other words, if N/M is viewed as $\mathbb{F}_p[G]$-module then $y \in N/M$, and hence $\sigma_p(y)$, is fixed by g'. Using the description of σ given above, we obtain

$$\sigma_p(y) = \Big(\sum_{j=0}^{d-1} \bar{x}_1^j, 0, \ldots, 0 \Big) \in \mathbb{F}_p[G]^n.$$

So $g' \sum_{j=0}^{d-1} \bar{x}_1^j = \sum_{j=0}^{d-1} \bar{x}_1^j$ in $\mathbb{F}_p[G]$, which implies that $\gamma(g) = g' \in \langle x_1 N \rangle$, as required.

To prove (ii), we observe that for any $\ell \geqslant 1$, the subgroup C^{p^ℓ} is also normal in F_n/M and $\gamma(C^{p^\ell}) = \gamma(C)$. Since C is abelian, for a sufficiently large ℓ, the subgroup C^{p^ℓ} has order prime to p, and we can assume that C has this property. Then there exists $h \in N/M$ such that $hCh^{-1} \subset G$, and since C is normal, we actually have $C \subset G$. If $C \neq \{e\}$ then as $n > 1$, we conclude from (3) that there exist $c \in C$, $g \in N/M$ such that $cgc^{-1} \neq g$. Then

$$1 \neq cgc^{-1}g^{-1} \in C \cap N/M,$$

a contradiction. □

Corollary 2.3. *Let $\mathfrak{F} = \mathfrak{F}(X)$ be the free profinite group on a finite set X. Then for any $x \in X$, the centralizer $C_{\mathfrak{F}}(x)$ coincides with the pro-cyclic group $\langle \widehat{x} \rangle$. Consequently, if $|X| > 1$ then $\mathfrak{F}$ has trivial center.*

Proof. Let $F = F(X)$ be the free discrete group viewed as a (dense) subgroup of $\mathfrak{F}$. If our assertion is false then there exists an open normal subgroup $U \subset \mathfrak{F}$ such that the image of $C_{\mathfrak{F}}(x)$ in $G := \mathfrak{F}/U$ strictly contains $\langle xU \rangle$. Let $N = F \cap U$. Pick a prime p not dividing $|G|$, and let V denote the closure of $M = N^p[N, N]$ in $\mathfrak{F}$ (so that $F \cap V = M$). Then the image of $C_{\mathfrak{F}}(x)$ in $\mathfrak{F}/V \simeq F/M$ is contained in $C_{F/M}(xM)$. On the other hand, by Proposition 2.2 (i), the image of $C_{F/M}(xM)$ in F/N coincides with $\langle xN \rangle$. Using the natural isomorphism $F/N \simeq \mathfrak{F}/U$, we see that the image of $C_{\mathfrak{F}}(x)$ in $\mathfrak{F}/U$ is contained in $\langle xU \rangle$. A contradiction, proving our first assertion. Since for $x, y \in X$, $x \neq y$, we have $\langle \widehat{x} \rangle \cap \langle \widehat{y} \rangle = \{e\}$, our second assertion follows. □

Corollary 2.4 (cf. [3], Lemma 10). *Let $\mathfrak{F} = \mathfrak{F}(X)$ be the free profinite group on a finite set X with $|X| > 1$. If $C \subset \mathfrak{F}$ is an abelian normal subgroup then $C = \{e\}$.*

Proof. Again, let $F \subset \mathfrak{F}$ be the abstract free group generated by X. Assume that $C \neq \{e\}$, and choose an open normal subgroup $U \subset \mathfrak{F}$ that does not contain C. As in the proof of Corollary 2.3, set $N = F \cap U$ and $M = N^p[N, N]$ where p is a prime not dividing the order of $G := \mathfrak{F}/U$. Let V denote the closure of M in $\mathfrak{F}$. Then CV/V is an abelian normal subgroup of $\mathfrak{F}/V = F/M$. So, it follows from Proposition 2.2 (ii) that its image in F/N is trivial. Using the isomorphism $F/N \simeq \mathfrak{F}/U$, we conclude that $C \subset U$, a contradiction. □

Remark 2.5. The proof of Lemma 10 in [3] is faulty. It is based on the "fact" that if $\mathfrak{H}$ is a free profinite group (of finite rank), and $h \in \mathfrak{H}^{\mathrm{ab}} = \mathfrak{H}/[\mathfrak{H}, \mathfrak{H}]$ is a nontrivial element then for $\beta \in \widehat{\mathbb{Z}}$, we have that $\beta h = 0$ in $\mathfrak{H}^{\mathrm{ab}}$ implies that $\beta = 0$. This is false in general as $\widehat{\mathbb{Z}}$ has zero divisors. The argument in [3], however, can be corrected by passing to the corresponding free pro-p group $\mathfrak{H}_p$ for some prime p (for this, one needs an analog of Corollary 2.3 for $\mathfrak{H}_p$).

We now recall Schreier's method (cf. [7], 2.3, or [12], Ch. VI), which will be used repeatedly in this note: Let G be a group with a generating set X, let H be a subgroup of G, and T be a right transversal (i.e., a system of representatives of right cosets containing the identity) to H in G. Given $g \in G$, we let $\bar{g}$ denote the unique element in T satisfying $Hg = H\bar{g}$. Then the set

$$Y := \{tx(\overline{tx})^{-1} \mid t \in T,\ x \in X\} \setminus \{e\},$$

generates H. Moreover, if G is the free group on X, and T has the Schreier property (i.e., the initial segment of any element of T is again in T), then Y is a free generating set for H.

Lemma 2.6. *Let $F = F(X)$ be the free group on $X = \{x_1, \dots, x_n\}$ with $n > 1$, and let $G = F/N$ be a finite quotient of F. Pick a prime p not dividing $6|G|$, and set $L = N \cap F^6[F,F]$ and $M = L^p[L,L]$. Let $\delta\colon F/M \to F/L$ be the canonical homomorphism. Then for $c = [x_i, x_j] = x_i x_j x_i^{-1} x_j^{-1}$, with $i \neq j$, we have $\delta(C_{F/M}(cM)) = \langle cL \rangle$.*

Proof. Let $F_1 = F^2[F,F]$ and $F_2 = F^3[F,F]$. We will write the argument for $i = 2$, $j = 1$. The set

$$T_1 = \{x_1^{e_1} \dots x_n^{e_n} \mid e_i \in \{0,1\}\}$$

is a transversal to F_1 in F. Applying Schreier's method, we see that F_1 is a free group on a set containing c. Then by Proposition 2.2 (i), we have $\delta(C_{F_1/M}(cM)) = \langle cL \rangle$. Since $F^2 \subset F_1$, we obtain that

$$\text{for any } t \in C_{F/M}(cM) \text{ we have } \delta(t)^2 \in \langle cL \rangle. \tag{4}$$

Similarly,

$$T_2 = \{x_1^{e_1} \dots x_n^{e_n} \mid e_i \in \{0,1,2\}\}$$

is a transversal to F_2 in F. Applying again Schreier's method, we obtain that F_2 is a free group on a set containing c, hence $\delta(C_{F_2/M}(cM)) = \langle cL \rangle$. As $F^3 \subset F_2$, we see that

$$\text{for any } t \in C_{F/M}(cM) \text{ we have } \delta(t)^3 \in \langle cL \rangle. \tag{5}$$

Now our assertion follows from (4) and (5). □

Corollary 2.7 (cf. [3], Lemma 1). *Let $\mathfrak{F} = \mathfrak{F}(X)$ be the free profinite group on a finite set X with $|X| > 1$. Given $x, y \in X$, $x \neq y$, for $c = [x,y]$ we have $C_{\mathfrak{F}}(c) = \widehat{\langle c \rangle}$.*

This is derived from Lemma 2.6 just as Corollary 2.3 was derived from Proposition 2.2 (i).

Lemma 2.8 (cf. [3], Lemma 8). *Let $\mathfrak{F}$ be a free profinite group of finite rank, and $N \subset \mathfrak{F}$ be an open subgroup. If $\sigma \in \operatorname{Aut}\mathfrak{F}$ restricts trivially to N then $\sigma = \mathrm{id}_{\mathfrak{F}}$.*

Proof. We can obviously assume that N is normal in $\mathfrak{F}$, and then $g^m \in N$ for any $g \in \mathfrak{F}$, where $m = [\mathfrak{F} : N]$. If $\mathfrak{F}$ is of rank one then σ is of the form $\sigma(g) = g^\alpha$ for some $\alpha \in \widehat{\mathbb{Z}}$. The fact that $\sigma|N = \mathrm{id}_N$ implies that $m(\alpha - 1) = 0$. Since m is not a zero divisor in $\widehat{\mathbb{Z}}$, we conclude that $\alpha = 1$, i.e., $\sigma = \mathrm{id}_{\mathfrak{F}}$.

Now assume that $\mathfrak{F} = \mathfrak{F}(X)$ where $|X| > 1$, and pick two distinct elements $x_1, x_2 \in X$. Since $g x_i^m g^{-1} \in N$ for $i = 1, 2$ and all $g \in \mathfrak{F}$, we have

$$g x_i^m g^{-1} = \sigma(g x_i^m g^{-1}) = \sigma(g) x_i^m \sigma(g)^{-1},$$

and therefore

$$g^{-1}\sigma(g) \in C_{\mathfrak{F}}(x_i^m) \quad \text{for } i = 1, 2. \tag{6}$$

We will now show that

$$\text{for any } x \in X \text{ and any positive } m \in \mathbb{Z}, \text{ we have } C_{\mathfrak{F}}(x^m) = \widehat{\langle x \rangle}. \tag{7}$$

Indeed, consider the homomorphism $\varepsilon\colon F \to \mathbb{Z}/m\mathbb{Z}$ of the group $F = F(X)$ that takes x to 1 (mod m), and all other generators $y \in X \setminus \{x\}$ to 0 (mod m). Let $H = \operatorname{Ker}\varepsilon$. Applying Schreier's method to the transversal $T = \{x^e \mid e = 0, \dots, m-1\}$ to H in F, we see that H is a free group on a set containing x^m. By Corollary 2.3, for the corresponding free profinite group $\mathfrak{H}$ (the closure of H in $\mathfrak{F}$) we have $C_{\mathfrak{H}}(x^m) = \widehat{\langle x^m \rangle}$. Since $[\mathfrak{F} : \mathfrak{H}] = m$, we have $[C_{\mathfrak{F}}(x^m) : C_{\mathfrak{H}}(x^m)] \leqslant m$. On the other hand $\widehat{\langle x \rangle} \subset C_{\mathfrak{F}}(x^m)$ and $[\widehat{\langle x \rangle} : \widehat{\langle x^m \rangle}] = m$, so (7) follows.

Using (6) and (7), we now see that

$$g^{-1}\sigma(g) \in \widehat{\langle x_1 \rangle} \cap \widehat{\langle x_2 \rangle} = \{e\} \quad \text{for any } g \in \mathfrak{F},$$

i.e., $\sigma = \mathrm{id}_{\mathfrak{F}}$. □

3. Some reductions

Let $\mathfrak{F}$ be a finitely generated profinite group. Then $\mathfrak{F}$ has only finitely many open subgroups of index $\leq n$, for each $n \geqslant 1$, implying that the intersection U_n of all these subgroups is itself an open normal subgroup. It is easy to see that the automorphism group $\operatorname{Aut}\mathfrak{F}$ can be naturally identified with $\varprojlim \operatorname{Aut}(\mathfrak{F}/U_n)$, making it a profinite group. Furthermore, the topology on $\operatorname{Aut}\mathfrak{F}$ arising from the above identification coincides with the natural topology of uniform convergence (cf. [16]). Now if $\mathfrak{F} = \widehat{G}$, where G is a finitely generated discrete group, then the pullback of the topology on $\operatorname{Aut}\widehat{G}$ under the natural map $\operatorname{Aut} G \xrightarrow{\iota} \operatorname{Aut}\widehat{G}$ coincides with the topology τ_c defined in terms of congruence subgroups $\Gamma[K]$ of $\Gamma = \operatorname{Aut} G$ for all finite index subgroups $K \subset G$ (cf. §1). Consequently, the completion $\overline{\Gamma}$ can be identified with the closure of $\operatorname{Im}\iota$ in $\operatorname{Aut}\widehat{G}$. The kernel of the resulting map $\widehat{\operatorname{Aut} G} \xrightarrow{\varphi} \operatorname{Aut}\widehat{G}$ coincides with the intersection $\bigcap_K \widehat{\Gamma[K]}$ taken over all finite index normal subgroups $K \subset G$ where $\widehat{\ }$ denotes the closure in $\widehat{\Gamma} = \widehat{\operatorname{Aut} G}$.[2] Similarly, the group of outer automorphisms

[2]We note that for G a free group of any rank $r \geqslant 1$, the homomorphism $\widehat{\operatorname{Aut} G} \to \operatorname{Aut}\widehat{G}$ is not surjective. This follows from the fact that $\widehat{G}^{\mathrm{ab}} = \widehat{\mathbb{Z}}^r$, and the resulting map $\operatorname{Aut}\widehat{G} \xrightarrow{\hat{\theta}} \mathrm{GL}_r(\widehat{\mathbb{Z}})$ is surjective while $(\hat{\theta} \circ \varphi)(\widehat{\operatorname{Aut} G})$ is contained in (actually, is equal to) the subgroup of $\mathrm{GL}_r(\widehat{\mathbb{Z}})$ of matrices having determinant ± 1. Incidentally, it is well known (and follows, for example, from Dirichlet's Prime Number Theorem) that $\widehat{\mathbb{Z}}^\times$ is not finitely generated, implying that $\operatorname{Aut}\widehat{G}$ is not finitely generated (as a profinite group) – this result is given as Corollary 3 in [13] where it is established using some results of [8].

$\operatorname{Out}\widehat{G} = \operatorname{Aut}\widehat{G}/\operatorname{Int}\widehat{G}$ is profinite, so the natural map $\operatorname{Out} G \xrightarrow{\omega} \operatorname{Out}\widehat{G}$ extends to a continuous homomorphism $\widehat{\operatorname{Out} G} \xrightarrow{\psi} \operatorname{Out}\widehat{G}$. As above, the pullback under ω of the topology on $\operatorname{Out}\widehat{G}$ coincides with the topology on $\Delta = \operatorname{Out} G$ defined by the following "congruence subgroups"

$$\Delta[K] = \operatorname{Ker}(\operatorname{Out} G \to \operatorname{Out}(G/K))$$

associated to characteristic finite index subgroups $K \subset G$. Then the completion $\overline{\Delta}$ of Δ for that topology can be identified with the closure of $\operatorname{Im}\omega$ in $\operatorname{Out}\widehat{G}$, and $\operatorname{Ker}\psi$ coincides with the intersection $\bigcap_K \widehat{\Delta[K]}$ where the intersection is taken over all finite index characteristic subgroups $K \subset G$ and $\widehat{\ }$ denotes the closure in the profinite completion $\widehat{\Delta}$.

We will now relate the injectivity of φ to that of ψ.

Lemma 3.1. *Let G be a finitely generated residually finite group such that $\widehat{G}$ has trivial center. If $\widehat{\operatorname{Out} G} \xrightarrow{\psi} \operatorname{Out}\widehat{G}$ is injective then so is $\widehat{\operatorname{Aut} G} \xrightarrow{\varphi} \operatorname{Aut}\widehat{G}$.*

Proof. Since G is residually finite, the center of G is also trivial, so identifying $\operatorname{Int} G$ and $\operatorname{Int}\widehat{G}$ with G and $\widehat{G}$ respectively, we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G & \longrightarrow & \operatorname{Aut} G & \longrightarrow & \operatorname{Out} G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \widehat{G} & \longrightarrow & \operatorname{Aut}\widehat{G} & \longrightarrow & \operatorname{Out}\widehat{G} & \longrightarrow & 1.
\end{array}$$

Since the center of $\widehat{G}$ is trivial, taking the profinite completion of the groups in the top row yields, by Lemma 2.1, the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \widehat{G} & \longrightarrow & \widehat{\operatorname{Aut} G} & \longrightarrow & \widehat{\operatorname{Out} G} & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} & & \\
1 & \longrightarrow & \widehat{G} & \longrightarrow & \operatorname{Aut}\widehat{G} & \longrightarrow & \operatorname{Out}\widehat{G} & \longrightarrow & 1.
\end{array}$$

Then a simple diagram chase shows that if ψ is injective then φ is also injective. □

Let F be the free group with generators x and y. It is well known (cf. [7], 3.5) that the canonical homomorphism $F \longrightarrow F^{\mathrm{ab}} = F/[F,F]$ combined with the identification $F^{\mathrm{ab}} \simeq \mathbb{Z}^2$ yields the exact sequence

$$1 \to \operatorname{Int} F \to \operatorname{Aut} F \xrightarrow{\theta} \operatorname{Aut} F^{\mathrm{ab}} = \mathrm{GL}_2(\mathbb{Z}) \to 1,$$

i.e., $\operatorname{Out} F$ can be naturally identified with $\mathrm{GL}_2(\mathbb{Z})$. Let Φ be the free group with generators a and b. Consider the automorphisms $\alpha, \beta \in \operatorname{Aut} F$ defined by

$$\alpha\colon \begin{cases} x \to x, \\ y \to yx^2, \end{cases} \qquad \text{and} \qquad \beta\colon \begin{cases} x \to xy^2, \\ y \to y, \end{cases}$$

and let $\Phi \to \mathrm{Aut}\, F$ be the homomorphism defined by $a \mapsto \alpha$ and $b \mapsto \beta$. Since the group $\mathrm{Aut}\, \widehat{F}$ is profinite, this homomorphism extends to a continuous homomorphism $\nu\colon \widehat{\Phi} \to \mathrm{Aut}\, \widehat{F}$.

Proposition 3.2. *If ν is injective then $\varphi\colon \widehat{\mathrm{Aut}\, F} \to \mathrm{Aut}\, \widehat{F}$ is also injective.*

Proof. According to Lemma 3.1, it is enough to show that ψ is injective. We will first establish the injectivity of the composite map

$$\lambda\colon \widehat{\Phi} \xrightarrow{\nu} \mathrm{Aut}\, \widehat{F} \to \mathrm{Out}\, \widehat{F}.$$

It is easy to see that α and β fix $c = [x, y] = xyx^{-1}y^{-1}$, so it follows from Corollary 2.7 that $D := \nu(\widehat{\Phi}) \cap \mathrm{Int}\, \widehat{F}$ is contained in $\widehat{\langle \mathrm{Int}\, c \rangle}$. Since ν is injective, we conclude that $C := \mathrm{Ker}\, \lambda = \nu^{-1}(D)$ is a pro-cyclic, hence abelian, normal subgroup of $\widehat{\Phi}$. Applying Corollary 2.4, we obtain that $C = \{e\}$, i.e., λ is injective.

As we explained in the beginning of this section, $\mathrm{Ker}\, \psi$ is contained in the closure $\widehat{\Delta[K]}$ for any finite index characteristic subgroup $K \subset F$. So, the injectivity of ψ will follow from that of λ if we establish the inclusion

$$\mathrm{Im}\, \mu \supset \Delta[K_0] \quad \text{for } K_0 = F^4[F, F], \tag{8}$$

where μ denotes the composite map $\Phi \to \mathrm{Aut}\, F \to \mathrm{Out}\, F$. However, under the identification $\mathrm{Out}\, F \simeq \mathrm{GL}_2(\mathbb{Z})$, the subgroup $\Delta[K_0]$ corresponds to the congruence subgroup $\mathrm{GL}_2(\mathbb{Z}, 4) = \mathrm{SL}_2(\mathbb{Z}, 4)$ modulo 4, and $\mathrm{Im}\, \mu$ corresponds to the subgroup $H \subset \mathrm{SL}_2(\mathbb{Z})$ generated by the matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

So (8) follows from the well-known fact that H contains $\mathrm{SL}_2(\mathbb{Z}, 4)$ (cf. [14]). □

The following completes the proof of the Main Theorem.

Proposition 3.3. *The map ν is injective.*

4. Proof of Proposition 3.3

We begin this section with some constructions needed in the proof of Proposition 3.3. Consider the following free product

$$\Psi = \langle z_1 \rangle * \langle z_2 \rangle * \langle z_3 \rangle \quad \text{where } z_i^2 = e \text{ for } i = 1, 2, 3,$$

and let $\varepsilon\colon \Psi \to \langle z_1 \rangle \times \langle z_2 \rangle \times \langle z_3 \rangle$ be the canonical homomorphism (which actually coincides with the homomorphism of abelianization $\Psi \to \Psi^{\mathrm{ab}}$). It follows from

Kurosh's Theorem and the exercise in [15], Ch. I, §5.5, that $\operatorname{Ker}\varepsilon$ is a free group of rank five. More generally, any subgroup of Ψ which does not meet any conjugate of any of the factors is free. This, in particular, applies to the kernel Θ of the following composite homomorphism

$$\Psi \xrightarrow{\varepsilon} \langle z_1\rangle \times \langle z_2\rangle \times \langle z_3\rangle \xrightarrow{\sigma} \mathbb{Z}/2\mathbb{Z},$$

where σ sends each z_i to 1 (mod 2). Choosing $\{1, z_1\}$ as a transversal to Θ in Ψ and applying Schreier's method, we see that Θ is generated by z_2z_1, z_3z_1, z_1z_2 and z_1z_3, and hence by z_1z_2 and z_2z_3. Since Θ is obviously nonabelian, it is the free group on z_1z_2 and z_2z_3. We now identify F with $\Theta \subset \Psi$ using the (fixed) embedding $F \hookrightarrow \Psi$ defined by $x \mapsto z_1z_2$ and $y \mapsto z_2z_3$.

Lemma 4.1. *There exist automorphisms $\dot\alpha, \dot\beta \in \operatorname{Aut}\Psi$ such that*

$$\dot\alpha\colon \begin{cases} z_1 \mapsto (z_1z_2)^{-1}z_1(z_1z_2), \\ z_2 \mapsto (z_1z_2)^{-1}z_2(z_1z_2), \\ z_3 \mapsto (z_1z_2)^{-2}z_3(z_1z_2)^2, \end{cases} \quad \text{and} \quad \dot\beta\colon \begin{cases} z_1 \mapsto z_1, \\ z_2 \mapsto (z_2z_3)^{-1}z_2(z_2z_3), \\ z_3 \mapsto (z_2z_3)^{-1}z_3(z_2z_3). \end{cases} \tag{9}$$

Furthermore, F is invariant under $\dot\alpha$ and $\dot\beta$ and

$$\dot\alpha|F = \alpha \quad \text{and} \quad \dot\beta|F = \beta.$$

Proof. Let $\mathcal{F}$ be the free group on $\tilde z_1, \tilde z_2, \tilde z_3$. Then $\Psi = \mathcal{F}/\mathcal{N}$ where $\mathcal{N}$ is the normal subgroup of $\mathcal{F}$ generated by by $\tilde z_1^2, \tilde z_2^2, \tilde z_3^2$. Let $\tilde\alpha\colon \mathcal{F} \to \mathcal{F}$ be the endomorphism of $\mathcal{F}$ defined by the replicas of equations (9) written in terms of $\tilde z_1$, $\tilde z_2$, $\tilde z_3$, i.e., $\tilde z_1 \mapsto (\tilde z_1\tilde z_2)^{-1}\tilde z_1(\tilde z_1\tilde z_2)$, etc. Using the fact that $\tilde\alpha(\tilde z_1\tilde z_2) = \tilde z_1\tilde z_2$, it is easy to see that $\operatorname{Im}\tilde\alpha$ contains $\tilde z_1, \tilde z_2$ and $\tilde z_3$, making $\tilde\alpha$ surjective. Since $\mathcal{F}$ is hopfian (cf. [12], 6.1.12), we conclude that $\tilde\alpha$ is an automorphism of $\mathcal{F}$ (which can also be checked directly). Clearly, $\tilde\alpha(\tilde z_1^2), \tilde\alpha(\tilde z_2^2)$ and $\tilde\alpha(\tilde z_3^2)$ are contained in $\mathcal{N}$, and in fact generate it as a normal subgroup of $\mathcal{F}$. Thus, $\tilde\alpha(\mathcal{N}) = \mathcal{N}$, and therefore $\tilde\alpha$ descends to an automorphism $\dot\alpha$ of Ψ. By direct computation we obtain that

$$\dot\alpha(x) = \dot\alpha(z_1z_2) = z_1z_2 = x = \alpha(x)$$

and

$$\dot\alpha(y) = \dot\alpha(z_2z_3) = (z_2z_3)(z_1z_2)^2 = yx^2 = \alpha(y).$$

Thus, $\dot\alpha$ leaves F invariant and restricts to α.

The computation for $\dot\beta$ is similar (and even simpler). Again, we observe that for the corresponding $\tilde\beta$ we have $\tilde\beta(\tilde z_2\tilde z_3) = \tilde z_2\tilde z_3$, using which one easily verifies that $\tilde\beta$ is surjective, hence an automorphism of $\mathcal{F}$. Furthermore, $\tilde\beta(\mathcal{N}) = \mathcal{N}$, so $\tilde\beta$ descends to $\dot\beta \in \operatorname{Aut}\Psi$. We have

$$\dot\beta(x) = \dot\beta(z_1z_2) = (z_1z_2)(z_2z_3)^2 = xy^2 = \beta(x)$$

and

$$\dot{\beta}(y) = \dot{\beta}(z_2 z_3) = z_2 z_3 = y = \beta(y),$$

which means that $\dot{\beta}$ also leaves F invariant and restricts to β. □

In the sequel, we will work with the homomorphism $\Phi \to \operatorname{Aut} \Psi$ defined by $a \mapsto \dot{\alpha}, b \mapsto \dot{\beta}$. Now let

$$F' = \{x \in \Psi \mid \varepsilon(x) = (\epsilon_1, \epsilon_2, \epsilon_3) \in (\mathbb{Z}/2\mathbb{Z})^3 \text{ with } \epsilon_1 = \epsilon_2 = \epsilon_3\}.$$

Lemma 4.2. *F' is the free group on*

$$u = z_1 z_2 z_3, \quad v = z_2 z_3 z_1 \quad \textit{and} \quad w = z_3 z_1 z_2.$$

Proof. Clearly, F' intersects trivially every conjugate of each factor $\langle z_i \rangle$, so it follows from Kurosh's theorem that F' is a free group. As $\operatorname{Ker} \varepsilon$ is a free group of rank 5 and $[F' : \operatorname{Ker} \varepsilon] = 2$ we conclude from Schreier's formula that F' is of rank 3. Taking $T = \{1, z_1, z_2, z_3\}$ as a transversal to F' in Ψ and applying Schreier's method, we see that F' is generated by the following set

$$\{z_1 z_2 z_3,\ z_1 z_3 z_2,\ z_2 z_1 z_3,\ z_2 z_3 z_1,\ z_3 z_1 z_2,\ z_3 z_2 z_1\}.$$

But $z_3 z_1 z_2 = (z_2 z_1 z_3)^{-1}$, etc., so F' is generated by u, v and w. Since F' is hopfian, we conclude that it is the free group on $\{u, v, w\}$. □

Remark 4.3. Since $\dot{\alpha}, \dot{\beta} \in \operatorname{Aut} \Psi$ act trivially on Ψ^{ab}, the group Φ leaves F' invariant. We note that the profinite completion $\widehat{F'}$ corresponds to the Galois group $\operatorname{Gal}(\mathcal{M}_t/\mathcal{K})$ in [3], where it is asserted only that the latter is invariant under a certain subgroup of index two $\operatorname{Gal}(\bar{k}/k_1) \subset \operatorname{Gal}(\bar{k}/k)$ (cf. the end of §5 in [3]). As a result, the argument in [3] involves (in our notations) an index two subgroup $\widehat{\Phi}_1 \subset \widehat{\Phi}$ that leaves $\widehat{F'}$ invariant, and amounts to proving first that the restriction $\nu|\widehat{\Phi}_1$ is injective, and then deriving that ν itself is injective. As F' is in fact Φ-invariant, the step involving the introduction of $\widehat{\Phi}_1$ can be eliminated from the argument.

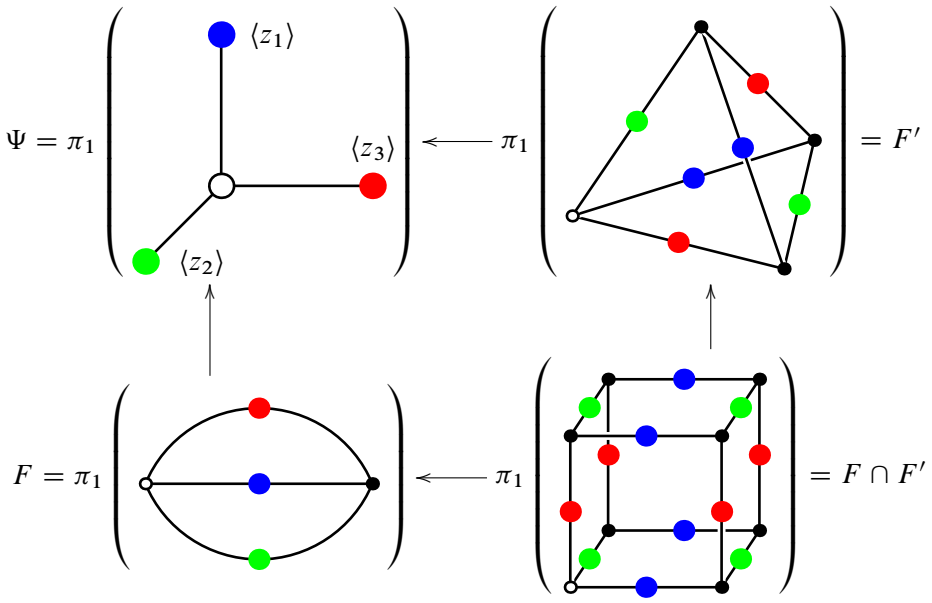
The action of $\dot{\alpha}, \dot{\beta}$ on F' is described explicitly in the following lemma.

Lemma 4.4. *We have*

$$\dot{\alpha}(u) = w^{-1} u w, \quad \dot{\alpha}(v) = v, \quad \dot{\alpha}(w) = (uw)^{-1} w (uw),$$

and

$$\dot{\beta}(u) = u, \quad \dot{\beta}(v) = v, \quad \dot{\beta}(w) = (vu)^{-1} w (vu).$$



The groups Ψ, F, F', and $F \cap F'$ can be realized as the fundamental groups of suitable graphs of groups as shown above. In the case of Ψ the vertex groups at the three terminal vertices are taken to be $\mathbb{Z}/2\mathbb{Z}$, and all other vertex and edge groups are trivial. The inclusions correspond to covering maps of graphs.

Proof. This is verified by direct computation. We have

$$\dot{\alpha}(u) = \dot{\alpha}(z_1 z_2 z_3) = (z_2 z_1 z_3)(z_1 z_2 z_3)(z_3 z_1 z_2) = w^{-1} u w,$$
$$\dot{\alpha}(v) = \dot{\alpha}(z_2 z_3 z_1) = z_2 z_3 z_1 = v,$$

and

$$\dot{\alpha}(w) = \dot{\alpha}(z_3 z_1 z_2) = (z_1 z_2)^{-2}(z_3 z_1 z_2)(z_1 z_2)^2 = (uw)^{-1} w (uw).$$

The computation for $\dot{\beta}$ is even easier:

$$\dot{\beta}(u) = \dot{\beta}(z_1 z_2 z_3) = z_1 z_2 z_3 = u,$$
$$\dot{\beta}(v) = \dot{\beta}(z_2 z_3 z_1) = z_2 z_3 z_1 = v,$$

and

$$\dot{\beta}(w) = \dot{\beta}(z_3 z_1 z_2) = (z_2 z_3)^{-2}(z_3 z_1 z_2)(z_2 z_3)^2 = (vu)^{-1} w (vu). \qquad \square$$

In the sequel, the restrictions of $\dot{\alpha}$, $\dot{\beta}$ to F' will be denoted by α' and β', respectively.

Proof of Proposition 3.3. For a discrete (resp. profinite) group G and its abstract (resp. closed) subgroup H, we let $\mathrm{Aut}(G, H)$ denote the subgroup of $\mathrm{Aut}\, G$ consisting of those automorphisms that leave H invariant. Since $\dot{\alpha}, \dot{\beta}$ do leave $F, F' \subset \Psi$ invariant, the homomorphism $\Phi \to \mathrm{Aut}\, \Psi$ (given by $a \mapsto \dot{\alpha}, b \mapsto \dot{\beta}$) leads to the following commutative diagram in which all maps are given by restriction:

$$\begin{array}{ccc} \Phi & \xrightarrow{\nu_0} & \mathrm{Aut}(F, F \cap F') \\ {\scriptstyle \varkappa_0}\downarrow & & \downarrow \\ \mathrm{Aut}(F', F \cap F') & \longrightarrow & \mathrm{Aut}\, F \cap F'. \end{array} \tag{10}$$

Moreover, ν_0 and $\varkappa_0$ send the generators a, b of Φ to α, β and α', β', respectively (cf. Lemma 4.1). Then (10) gives rise to the following commutative diagram

$$\begin{array}{ccc} \widehat{\Phi} & \xrightarrow{\nu} & \mathrm{Aut}(\widehat{F}, \widehat{F \cap F'}) \\ {\scriptstyle \varkappa}\downarrow & & \downarrow \\ \mathrm{Aut}(\widehat{F'}, \widehat{F \cap F'}) & \longrightarrow & \mathrm{Aut}\, \widehat{F \cap F'}. \end{array} \tag{11}$$

Assume that $\varkappa$ is injective. Then, given $x \in \mathrm{Ker}\, \nu$, we see from (11) that $\varkappa(x) \in \mathrm{Aut}\, \widehat{F'}$ restricts trivially to $\widehat{F \cap F'}$. Invoking Lemma 2.8, we see that $\varkappa(x) = 1$, and hence $x = 1$.

To prove the injectivity of $\varkappa$, we consider the canonical homomorphism $F' \to F'/V =: \bar{F}$ where V is the normal subgroup of F' generated by v. Clearly, $\bar{F}$ is the free group on the images $\bar{u}, \bar{w}$ of u and w, respectively. The description of α', β' given in Lemma 4.4 implies that $\mathrm{Im}\, \varkappa_0$ is contained in the subgroup $\mathrm{Aut}(F', v) \subset \mathrm{Aut}\, F'$ of all automorphisms that fix v. Let $\widehat{\bar{F}} = \widehat{F'}/\widehat{V}$ (where $\widehat{V}$ is the closure of V in $\widehat{F'}$) be the profinite completion of $\bar{F}$ and let $\mathrm{Aut}(\widehat{F'}, v) \subset \mathrm{Aut}\, \widehat{F'}$ be the subgroup of all automorphisms that fix v. We then have the following commutative diagram:

$$\begin{array}{ccccc} \Phi & \xrightarrow{\varkappa_0} & \mathrm{Aut}(F', v) & \longrightarrow & \mathrm{Aut}\, \bar{F} \\ \downarrow & & \downarrow & & \downarrow \\ \widehat{\Phi} & \xrightarrow{\varkappa} & \mathrm{Aut}(\widehat{F'}, v) & \longrightarrow & \mathrm{Aut}\, \widehat{\bar{F}}. \end{array}$$

It follows from Lemma 4.4 that the images of a, b in $\mathrm{Aut}\, \bar{F}$, and hence in $\mathrm{Aut}\, \widehat{\bar{F}}$, coincide with the inner automorphisms $\mathrm{Int}\, \bar{u}\bar{w}$ and $\mathrm{Int}\, \bar{u}$, respectively. Since $\bar{u}\bar{w}$ and $\bar{u}$ freely generate $\bar{F}$ and $\widehat{\bar{F}}$ has trivial center (Corollary 2.3), we conclude that the composite homomorphism $\widehat{\Phi} \to \mathrm{Aut}\, \widehat{\bar{F}}$ is injective, and hence $\varkappa$ is injective, as required. □

Remark 4.5. The proof of Proposition 3.3 can be informally, but adequately, described as the "topsy-turvy effect" in the following sense. Let us think about Out F and Int F as the "top" and the "bottom" parts of Aut F. The image of the homomorphism $\nu_0\colon \Phi \to \mathrm{Aut}\, F$ that leads to ν, has trivial intersection with Int F, so ν_0 can be characterized as a homomorphism to the top part of Aut F. In essence, the proof of Proposition 3.3 is based on constructing another free group on two generators $\bar{F}$, which is a quotient of a group F' commensurable with F, and relating ν_0 to a homomorphism $\Phi \to \mathrm{Aut}\, \bar{F}$ whose image lies in the bottom part Int $\bar{F}$. Then the injectivity of the corresponding homomorphism $\hat{\Phi} \to \mathrm{Aut}\, \hat{\bar{F}}$ reduces to the fact that $\hat{\bar{F}}$ has trivial center.

5. Explicit construction

In this section, we will recast the proof of the Main Theorem in a way that involves only finite quotients of free groups rather than free profinite groups. This leads to an explicit procedure enabling one to construct, for a given finite index normal subgroup N of $\Gamma = \mathrm{Aut}\, F$ containing Int F (where F is, as above, the free group on two generators, x and y), a finite index normal subgroup K of F such that $\Gamma[K] \subset N$.

Let $\mathrm{SL}_2'(\mathbb{Z})$ denote the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (freely) generated by $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 2 & 1\end{smallmatrix}\right)$ (we recall that $[\mathrm{SL}_2(\mathbb{Z}) : \mathrm{SL}_2'(\mathbb{Z})] = 12$), and let $\mathrm{Aut}'\, F$ be the preimage of $\mathrm{SL}_2'(\mathbb{Z})$ under the canonical homomorphism $\mathrm{Aut}\, F \xrightarrow{\theta} \mathrm{GL}_2(\mathbb{Z})$. Then replacing N with the normal subgroup $N \cap \mathrm{Aut}'\, F$ which contains Int F and whose index in Γ divides $12[\Gamma : N]$, we can assume that Int $F \subset N \subset \mathrm{Aut}'\, F$.

Theorem 5.1. *Let N be a finite index normal subgroup of Γ such that* Int $F \subset N \subset \mathrm{Aut}'\, F$, *and let $n = [\mathrm{Aut}'\, F : N]$. Pick two distinct odd primes $p, q \nmid n$, and set $m = n \cdot p^{n+1}$. Then there exist an explicitly constructed normal subgroup $K \subset F$ of index dividing $144m^4 \cdot q^{36m^4+1}$ such that $\Gamma[K] \subset N$.*

Proof. We will freely use the notations introduced in the previous sections; in particular, $\nu_0\colon \Phi \to \mathrm{Aut}\, F$ will denote the homomorphism given by $a \mapsto \alpha$, $b \mapsto \beta$. We notice that $\theta \circ \nu_0$ is an isomorphism between Φ and $\mathrm{SL}_2'(\mathbb{Z})$; in particular, ν_0 is injective and

$$\mathrm{Aut}'\, F = \mathrm{Int}\, F \rtimes \nu_0(\Phi). \tag{12}$$

We let $\pi\colon \mathrm{Aut}'\, F \to \nu_0(\Phi) \to \Phi$ denote the homomorphism induced by the corresponding projection. It follows from (12) that ν_0 induces an isomorphism $\bar{\nu}_0$ between Φ and $\mathrm{Out}'\, F := \mathrm{Aut}'\, F/\mathrm{Int}\, F$. Let $\bar{N}$ denote the image of N in $\mathrm{Out}'\, F$, and let $\mathcal{N} = \bar{\nu}_0^{-1}(\bar{N})$. Since p does not divide $n = |\Phi/\mathcal{N}|$, it follows from Proposition 2.2 (ii) that $\mathcal{M} := \mathcal{N}^p[\mathcal{N}, \mathcal{N}]$ has the following property:

$$\text{any cyclic normal subgroup of } \Phi/\mathcal{M} \text{ has trivial image in } \Phi/\mathcal{N}. \tag{13}$$

Furthermore, according to (3), we have an isomorphism $\mathcal{N}/\mathcal{M} \simeq \mathbb{F}_p[\Phi/\mathcal{N}] \oplus \mathbb{F}_p$, which shows that $|\Phi/\mathcal{M}|$ equals $m = n \cdot p^{n+1}$. Observing that for an $(\mathrm{Aut}' F)$-invariant subgroup $K \subset F$, the congruence subgroup $\Gamma[K]$ is normalized by $\mathrm{Aut}' F$, we conclude from (13) that it is enough to explicitly construct an $(\mathrm{Aut}' F)$-invariant subgroup $K \subset F$ of index dividing $144m^4 \cdot q^{36m^4+1}$ such that

$$\Gamma[K] \subset \mathrm{Aut}' F \text{ and the image of } \pi(\Gamma[K]) \text{ in } \Phi/\mathcal{M} \text{ is cyclic.} \tag{14}$$

(Indeed, then the image of $\Gamma[K]$ in $\mathrm{Out}' F$ is contained in $\bar{N}$, hence $\Gamma[K] \subset N$ as $N \supset \mathrm{Int}\, F$.)

Now let $\mathcal{L} = \mathcal{M}^q[\mathcal{M}, \mathcal{M}]$ and $\mathcal{G} = \Phi/\mathcal{L}$. Since $q \nmid m$, there is a semi-direct product decomposition $\mathcal{G} \simeq \mathcal{M}/\mathcal{L} \rtimes \Phi/\mathcal{M}$, and by the analog of (3), we have $\mathcal{M}/\mathcal{L} \simeq \mathbb{F}_q[\Phi/\mathcal{M}] \oplus \mathbb{F}_q$ as $(\Phi/\mathcal{M})$-modules. This implies that $C_{\mathcal{G}}(\mathcal{M}/\mathcal{L}) = \mathcal{M}/\mathcal{L}$, and as q is odd, we obtain the following:

$$\begin{aligned} &\text{for any subgroup } \mathcal{G}' \subset \mathcal{G} \text{ of index } \leqslant 2, \text{ the centralizer} \\ &C_{\mathcal{G}}(\mathcal{G}') \text{ has trivial image in } \Phi/\mathcal{M}. \end{aligned} \tag{15}$$

As before, $F(X)$ will denote a free group on a set X. Let $\phi\colon \Phi \to F(\bar{u}, \bar{v})$ be the isomorphism such that $a \mapsto \bar{u}\bar{w}$, $b \mapsto \bar{u}$, and let $\rho\colon F' = F(u, v, w) \to F(\bar{u}, \bar{w})$ be the homomorphism defined by $u \mapsto \bar{u}$, $v \mapsto 1$, $w \mapsto \bar{w}$. We will consider F and F' as subgroups of Ψ, and let $\varkappa_0\colon \Phi \to \mathrm{Aut}\, F'$ denote the homomorphism defined by sending a, b to the restrictions of $\dot{\alpha}$, $\dot{\beta}$ to F'. Then it follows from Lemma 4.4 that $\mathrm{Ker}\, \rho$ (which is the normal subgroup of F' generated by v) is invariant under $\varkappa_0(\Phi)$, and for $r \in \Phi$, the induced action of $\varkappa_0(r)$ on $F(\bar{u}, \bar{w})$ coincides with $\mathrm{Int}\, \phi(r)$ (cf. the proof of Proposition 3.3).

Let $M' = \rho^{-1}(\phi(\mathcal{M}))$ and $L' = \rho^{-1}(\phi(\mathcal{L}))$, and set $M = M' \cap F$ and $L = L' \cap F$. Since $\mathcal{M}$ and $\mathcal{L}$ are normal subgroups of Φ, we see that $\phi(\mathcal{M})$ and $\phi(\mathcal{L})$ are normal, hence $\varkappa_0(\Phi)$-invariant, subgroups of $F(\bar{u}, \bar{w})$. It follows that M' and L' are normal and $\varkappa_0(\Phi)$-invariant subgroups of F', and therefore M and L are normal and $\varkappa_0(\Phi)$-, or equivalently, $\nu_0(\Phi)$-invariant subgroups of $F \cap F'$; besides, $[F \cap F' : M]$ obviously divides m.

Set

$$S = \bigcap_{g \in F} (gMg^{-1}), \quad T = S \cap F^6[F, F] \quad \text{and} \quad U = T^q[T, T].$$

Lemma 5.2. (i) *U is $(\mathrm{Aut}' F)$-invariant and is contained in L;*

(ii) *$[F : U]$ divides $36m^4 \cdot q^{36m^4+1}$;*

(iii) *if $h \in \Phi$ is such that $\nu_0(h)$ acts on F/U as $\mathrm{Int}\, s$ for some $s \in S$ then $h \in \mathcal{M}$.*

Proof. (i): By construction, S is a normal $\nu_0(\Phi)$-invariant subgroup of F. So, it follows from (12) that it is $(\mathrm{Aut}' F)$-invariant. Then T and U are also $(\mathrm{Aut}' F)$-invariant. Since $S \subset M$, we have $\rho(S) \subset \phi(\mathcal{M})$, implying that $\rho(U) \subset \phi(\mathcal{L})$, and therefore $U \subset L$.

(ii): The normalizer $N_F(M)$ contains $F \cap F'$, and since $F/(F \cap F') \simeq (\mathbb{Z}/2\mathbb{Z})^2$, we see that $(F \cap F')/S$ embeds in a product of at most four copies of $(F \cap F')/M$, hence $[F : S]$ divides $4m^4$. Taking into account that

$$F^6[F, F] = F^3[F, F] \cap F^2[F, F]$$

and that $S \subset F \cap F' = F^2[F, F]$, we conclude that $[F : T]$ divides $36m^4$. Since $T/U \simeq \mathbb{F}_q[F/T] \oplus \mathbb{F}_q$, the index $[F : U]$ divides $36m^4 \cdot q^{36m^4+1}$.

(iii): Since $s \in S \subset M'$, there exists $m \in \mathcal{M}$ such that $\phi(m) = \rho(s)$. Set $g = hm^{-1}$. By (i), $U \subset L$, so the action of $\nu_0(h)$ on $(F \cap F')/L'$ coincides with Int s. On the other hand, there are isomorphisms

$$\Phi/\mathcal{L} \simeq F(\bar{u}, \bar{w})/\phi(\mathcal{L}) \simeq F'/L',$$

such that for $r \in \Phi$, the action of Int r on $\Phi/\mathcal{L}$ agrees with the action of Int $\phi(r)$ on $F(\bar{u}, \bar{w})/\phi(\mathcal{L})$, and with that of $\nu_0(r)$ on F'/L'. So, the action of $\nu_0(m)$ on F'/L' coincides with the action of Int s, and therefore $\nu_0(g)$ acts on $(F \cap F')L'/L'$ trivially. Since the latter is a subgroup of index $\leqslant 2$ in F'/L', we conclude that Int g acts trivially on a suitable subgroup $\mathcal{G}'$ of $\mathcal{G} = \Phi/\mathcal{L}$ having index $\leqslant 2$, and then by (15), $g \in \mathcal{M}$. □

Now set

$$K = U \cap K_0 \quad \text{where } K_0 = F^4[F, F].$$

Clearly, K is $(\mathrm{Aut}'\, F)$-invariant, and since $U \subset F \cap F' = F^2[F, F]$, it is easy to see that $[F : K]$ divides $144m^4 \cdot q^{36m^4+1}$. We will now show that K is as required. As we mentioned earlier,

$$\Gamma[K_0] = \theta^{-1}(\mathrm{SL}_2(\mathbb{Z}, 4)) \subset \mathrm{Aut}'\, F,$$

which implies that $\Gamma[K] \subset \mathrm{Aut}'\, F$. So, to complete the verification of (14), all we need to show is that the image of $\pi(\Gamma[K])$ in $\Phi/\mathcal{M}$ is cyclic.

Now let $g \in \Gamma[K]$. According to (12), we can write $g = (\mathrm{Int}\, f) \cdot \nu_0(h)$ for some $f \in F$, $h \in \Phi$, and then $\nu_0(h)$ acts on F/K as Int f^{-1}. As we already mentioned, $\nu_0(h)$ fixes $c = [x, y]$, so $fK \in C_{F/K}(cK)$, and therefore, by Lemma 2.6, $f \in \langle c \rangle S$. Consider the subgroup $W \subset \mathrm{Aut}(F/K)$ formed by the automorphisms induced by Int s with $s \in S$, and let Ω be the preimage of W under the composite map $\Phi \xrightarrow{\nu_0} \mathrm{Aut}'\, F \to \mathrm{Aut}(F/K)$. Set

$$\Theta = \Gamma[K] \cap (\mathrm{Int}\, F \rtimes \nu_0(\Omega)).$$

Then our argument shows that the quotient $\pi(\Gamma[K])/\pi(\Theta)$ is cyclic. On the other hand, by Lemma 5.2 (iii), the image of $\pi(\Theta)$ in $\Phi/\mathcal{M}$ is trivial, and therefore the image of $\pi(\Gamma[K])$ is a cyclic normal subgroup, as required. □

Remark 5.3. 1. If N is a normal subgroup of Γ satisfying $\mathrm{Int}\, F \subset N \subset \mathrm{Aut}'\, F$ and such that the quotient $(\mathrm{Aut}'\, F)/N$ has no cyclic normal subgroups then (13), and hence the entire argument, is valid for $\mathcal{M} = \mathcal{N}$ (in other words, we can set $m = n$). Then the resulting normal subgroup $K \subset F$ has index dividing $144n^4 \cdot q^{36n^4+1}$, which is much smaller number than the one given in the statement of the theorem.

2. One can somewhat improve the estimation given in the theorem by choosing for $\mathcal{M}$ the pullback of $(\mathcal{N}/\mathcal{N}^p[\mathcal{N}, \mathcal{N}])^{\Phi/\mathcal{N}}$ (then $\mathcal{N}/\mathcal{M}$ is isomorphic to the augmentation ideal in $\mathbb{F}_p[\Phi/\mathcal{N}]$) – this would change $[\Phi : \mathcal{M}]$ from $n \cdot p^{n+1}$ to $n \cdot p^{n-1}$; similar improvements are also possible in the construction of $\mathcal{L}$. However, with these changes, our construction would become more cumbersome and less explicit.

3. Any explicit procedure yielding a solution of the congruence subgroup problem for those finite index normal subgroups of Γ that contain $\mathrm{Int}\, F$ leads in fact to its solution for *all* finite index normal subgroups. Indeed, let $N \subset \Gamma$ be an arbitrary finite index normal subgroup, and let $Q \subset F$ be the characteristic subgroup that corresponds to $(\mathrm{Int}\, F) \cap N$ under the natural isomorphism $F \simeq \mathrm{Int}\, F$. Pick a prime p not dividing $|F/Q|$, and set $R = Q^p[Q, Q]$. As we noted above, $C_{F/R}(Q/R) = Q/R$, so if $\mathrm{Int}\, h \in \Gamma[R]$ then $h \in Q$. By our assumption, we can explicitly find a normal subgroup $K \subset F$ such that $\Gamma[K] \subset (N \cap \Gamma[R]) \cdot \mathrm{Int}\, F$. We claim that $\Gamma[K \cap R] \subset N$. Indeed, a given $g \in \Gamma[K \cap R]$ can be written in the form $g = s \cdot \mathrm{Int}\, h$ with $s \in N \cap \Gamma[R]$ and $h \in F$. Then $\mathrm{Int}\, h \in \Gamma[R]$, so $h \in Q$ and therefore $\mathrm{Int}\, h \in (\mathrm{Int}\, F) \cap N$. It follows that $g \in N$, as required. We observe, however, that the described procedure leads to a rather cumbersome estimation for the index $[F : K \cap R]$.

6. Topological connection

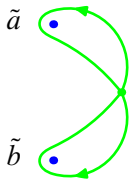
In the argument given in [3], the role of $\varkappa_0$ in (10) is played by a homomorphism coming from the following topological setting. Let Σ_g^n be a closed orientable surface of genus g with n punctures such that $2-2g-n < 0$, whose fundamental group will be denoted $\pi_1(g, n)$. Consider the configuration space $\mathrm{Conf}_2(\Sigma_g^n)$ of ordered pairs of distinct points in Σ_g^n. It was shown in [4] that the natural projection $\mathrm{Conf}_2(\Sigma_g^n) \to \Sigma_g^n$ is a (locally trivial) fibration with fiber Σ_g^{n+1}. Since $\pi_2(\Sigma_g^n) = 0$, the exact sequence of homotopy groups associated to a fibration assumes the form

$$0 \to \pi_1(g, n+1) \to \pi_1(\mathrm{Conf}_2(\Sigma_g^n)) \to \pi_1(g, n) \to 0.$$

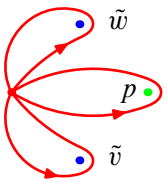
This sequence gives rise to a homomorphism $\rho_{g,n} : \pi_1(g, n) \to \mathrm{Out}\, \pi_1(g, n+1)$. We will now show that under appropriate identifications $\Phi \simeq \pi_1(0, 3)$ and $F' \simeq \pi_1(0, 4)$, the homomorphism $\rho_{0,3}$ coincides with composite map $\Phi \xrightarrow{\varkappa_0} \mathrm{Aut}\, F' \to \mathrm{Out}\, F'$.

We think of $\pi_1(0, 3)$ and $\pi_1(0, 4)$ as the fundamental groups of a plane with two and three punctures, respectively; i.e., in terms of punctured spheres, we move one

of the punctures to infinity. We fix generators as follows:



for $\pi_1(0,3) = \langle \tilde{a}, \tilde{b} \rangle$



for $\pi_1(0,4) = \langle \tilde{w}, \tilde{u}, \tilde{v} \rangle$

Note that the base point p chosen for $\pi_1(0,3)$ is among the punctures for $\pi_1(0,4)$.

Of course, the names of the generators are chosen suggestively. So, we consider the isomorphisms

$$\pi_1(0,3) \to \Phi, \quad \tilde{a} \mapsto a, \quad \tilde{b} \mapsto b,$$

and

$$\pi_1(0,4) \to F', \quad \tilde{w} \mapsto w, \quad \tilde{u} \mapsto u, \quad \tilde{v} \mapsto v.$$

Proposition 6.1. *The action of* $\pi_1(0,3)$ *on* $\pi_1(0,4)$ *induced by the fibration*

$$\Sigma_0^4 \to \mathrm{Conf}_2(\Sigma_0^3) \to \Sigma_0^3$$

is given by

$$\begin{aligned} &\tilde{a}(\tilde{w}) = \tilde{w}^{-1}\tilde{u}^{-1}\tilde{w}\tilde{u}\tilde{w}, && \tilde{a}(\tilde{u}) = \tilde{w}^{-1}\tilde{u}\tilde{w}, && \tilde{a}(\tilde{u}) = \tilde{v}, \\ &\tilde{b}(\tilde{w}) = \tilde{w}, && \tilde{b}(\tilde{u}) = \tilde{v}\tilde{u}\tilde{v}^{-1}, && \tilde{b}(\tilde{u}) = \tilde{v}\tilde{u}\tilde{v}\tilde{u}^{-1}\tilde{v}^{-1}. \end{aligned}$$

Consequently, with the above identifications, $\tilde{a}$ *acts exactly as* $\varkappa_0(a) = \dot{\alpha}$*, whereas* $\tilde{b}$ *acts as* $\mathrm{Int}(u^{-1}v^{-1}) \circ \dot{\beta}$*. Therefore, the composite map* $\Phi \xrightarrow{\varkappa_0} \mathrm{Aut}\, F' \to \mathrm{Out}\, F'$ *coincides with* $\rho_{0,3}$.

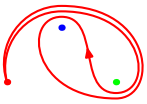
Proof. The action of $\pi_1(0,3)$ on $\pi_1(0,4)$ induced by the fibration

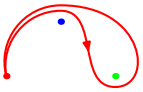
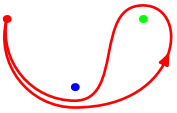
$$\Sigma_0^4 \longrightarrow \mathrm{Conf}_2(\Sigma_0^4) \longrightarrow \Sigma_0^3$$

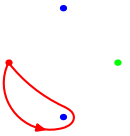
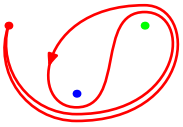
is given by the "push map": Representing an element of $\pi_1(0,3)$ as a loop γ based at p, its effect on an element of $\pi_1(0,4)$, also given as a loop δ, can be seen by pushing the base point p along the inverse of the curve γ and have it drag the loop δ along. (Here the inverse is taken in order to obtain a left action.)

Using this interpretation, we can read off this action on the generators and verify

the first claim:

$\tilde{a}(\tilde{w}) = \tilde{w}^{-1}\tilde{u}^{-1}\tilde{w}\tilde{u}\tilde{w}$  $\tilde{b}(\tilde{w}) = \tilde{w}$ 

$\tilde{a}(\tilde{u}) = \tilde{w}^{-1}\tilde{u}\tilde{w}$  $\tilde{b}(\tilde{u}) = \tilde{v}\tilde{u}\tilde{v}^{-1}$ 

$\tilde{a}(\tilde{v}) = \tilde{v}$  $\tilde{b}(\tilde{v}) = \tilde{v}\tilde{u}\tilde{v}\tilde{u}^{-1}\tilde{v}^{-1}$ 

Comparing this description to Lemma 4.4, we obtain our second claim. The last claim follows as $\rho_{0,3}$ is induced by the above action of $\pi_1(0,3)$ on $\pi_1(0,4)$. □

To interpret ν_0, one needs to consider the following complex affine algebraic surface

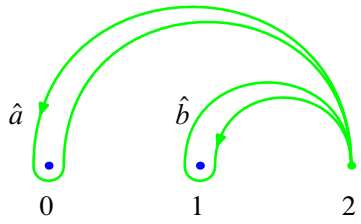
$$S = \{(s,t,\lambda) \in \mathbb{C}^3 \mid s^2 = t(t-1)(t-\lambda),\ \lambda \neq 0,1\}.$$

The projection to the λ-coordinate gives a fibration $S \to \mathbb{P}^1 \setminus \{0,1,\infty\}$ (where $\mathbb{P}^1$ is the complex projective line). The fiber above the value $\lambda \in \mathbb{C} \setminus \{0,1\}$ is $E_\lambda \setminus \{O\}$ where E_λ is the elliptic curve given by $s^2 = t(t-1)(t-\lambda)$ and O is the point at infinity on E_λ (thus, from the topological point of view, each fiber $E_\lambda \setminus \{O\}$ is a once punctured torus Σ_1^1). As above, we have the following exact sequence

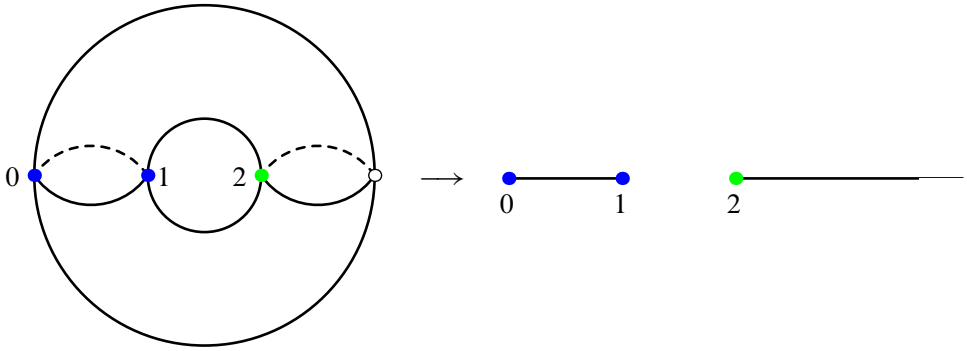
$$0 \to \pi_1(\Sigma_1^1) \to \pi_1(S) \to \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}) \to 0,$$

which gives rise to a homomorphism $\theta\colon \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}) \to \operatorname{Out} \pi_1(\Sigma_1^1)$ (cf. [3], 3.1). We will show in Proposition 6.2, that under appropriate identifications $\Phi \simeq \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})$ and $F \simeq \pi_1(\Sigma_1^1)$, this homomorphism coincides with the composition $\Phi \xrightarrow{\nu_0} \operatorname{Aut} F \to \operatorname{Out} F$. (Incidentally, this also provides a proof of the fact, mentioned and used on p. 145 of [3], that $\operatorname{Im}\theta$ contains the congruence subgroup $\mathrm{GL}_2(\mathbb{Z},4)$, which is helpful as the reference given in *loc. cit.* does not seem to contain this fact explicitly.)

Note that $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ is just the complex plane punctured at 0 and 1. To talk about its fundamental group, we designate 2 to be the basepoint. We fix generators of its fundamental group as follows:



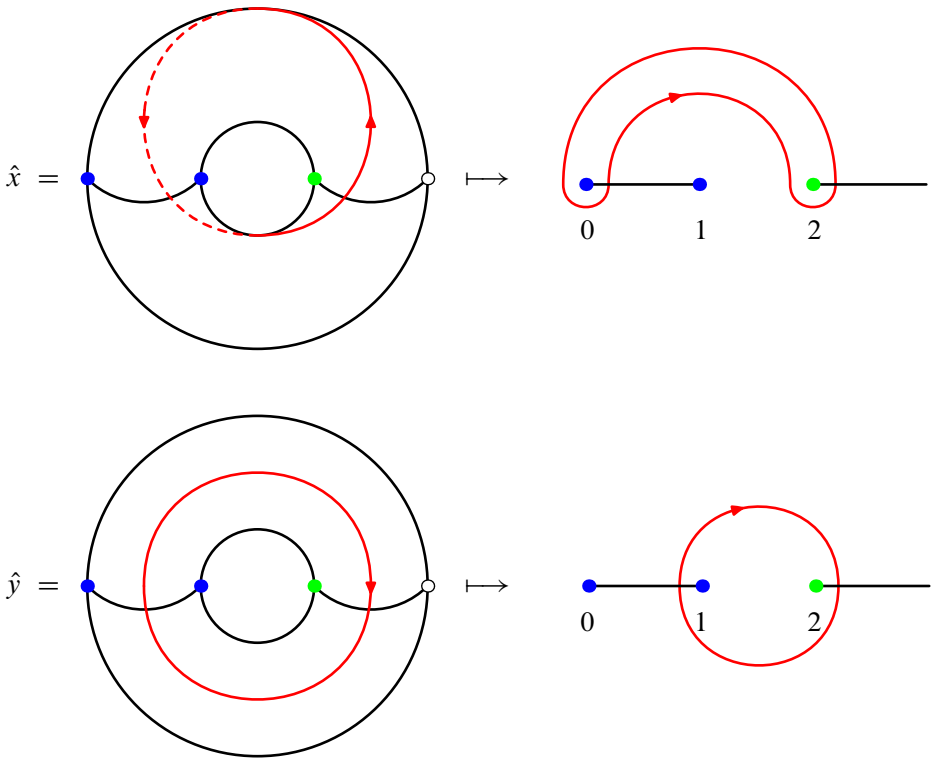
We also have to deal with the fibers $E_\lambda \setminus \{O\}$. To do that, we use the projection onto the t-coordinate. It defines a two sheeted cover $E_\lambda \setminus \{O\} \to \mathbb{C}$ branched above the points 0, 1, and λ. It will be convenient to be more explicit in the case $\lambda = 2$. The surface $E_2 \setminus \{O\}$ is a torus with one puncture (far right in the pictures). We use $\lambda = 2$ as the basepoint 2. The point 0 is on the outside left and the point 1 is on the inside.



The projection onto the t-plane identifies two points if they are equivalent under the 180-degree rotation about the axis running through the colored points. We will think of the of the surface $E_2 \setminus \{O\}$ as a two sheeted cover of the complex plane branched above "slits" (along the real line) from 0 to 1 and from 2 to ∞. The two small circles on the torus are the preimages of the slits. Thus, the top of the torus is one sheet, and the bottom of the torus is the other sheet. Moreover, we adopt the convention that the top-front and bottom-back correspond to the upper half plane and the top-back and bottom-front project onto the lower half plane.

Note that $\mathrm{Out}\, \pi_1(E_2 \setminus \{O\})$ is naturally isomorphic to the group of $\mathbb{Z}$-linear automorphisms of $\mathrm{H}_1(E_2 \setminus \{O\}; \mathbb{Z})$. Thus, it suffices to study the action of $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\})$ on the homology of $E_2 \setminus \{O\}$. We start by choosing a basis. In the following pictures, dashed lines run through the back of the punctured torus. We also

provide the image in the t-plane.



The pictures in the t-plane are ambiguous. The lift $\hat{x}$ is given by the rule that the crossing of the slit from 0 to 1 lifts to a change of sheets from the top to the bottom whereas the lift $\hat{y}$ follows the converse convention.

Proposition 6.2. *The action of* $\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})$ *on* $\mathrm{H}_1(E_2 \setminus \{O\}; \mathbb{Z})$ *induced by the fibration*

$$E_2 \setminus \{O\} \to S \to \mathbb{P}^1 \setminus \{0,1,\infty\}$$

is given by

$$\begin{aligned} \hat{a}(\hat{x}) &= \hat{x}, & \hat{a}(\hat{y}) &= \hat{y} + 2\hat{x}, \\ \hat{b}(\hat{x}) &= \hat{x} + 2\hat{y}, & \hat{b}(\hat{y}) &= \hat{y}. \end{aligned}$$

We use the obvious identifications of $\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}) = \langle \hat{a}, \hat{b} \rangle = \langle a, b \rangle = \Phi$ *and* $\mathrm{H}_1(E_2 \setminus \{O\}; \mathbb{Z}) = \mathbb{Z}\hat{x} \oplus \mathbb{Z}\hat{y} = \langle x, y \rangle^{\mathrm{ab}} = F^{\mathrm{ab}}$ *as indicated by the letters. Thus, with these identifications, the homomorphism* θ *coincides with* $\Phi \xrightarrow{\nu_0} \mathrm{Aut}\, F \to \mathrm{Out}\, F$.

Proof. Suppose we have a commutative diagram of continuous maps

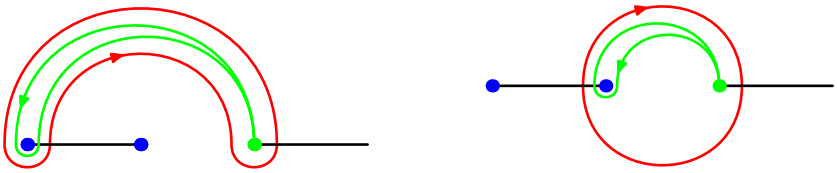
$$\begin{array}{ccc} S^1 \times [0,1] & \xrightarrow{H} & S \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_\lambda} \\ [0,1] & \xrightarrow[\gamma]{} & \mathbb{P}^1 \setminus \{0,1,\infty\}. \end{array}$$

That is, H is a homotopy of loops in S each of which runs within a fiber. Assume further, that $\gamma(0) = \gamma(1) = 2$, i.e., γ is a closed loop in $\mathbb{P}^1 \setminus \{0,1,\infty\}$ based at the basepoint. Then H is a homotopy in S connecting two loops in $E_2 \setminus \{O\}$. Note that the composite curve $H(0,\cdot) \circ H(\cdot,1) \circ H(0,\cdot)^{\mathrm{rev}}$ is homotopic to the loop $H(\cdot,0)$ in S. Since $H(0,\cdot)$ is a lift of γ, the concatenation represents the action of γ on the curve $H(\cdot,1)$ by conjugation. Thus $H(\cdot,0) = \gamma(H(\cdot,1))$, i.e., to compute the effect of a loop γ in $\mathbb{P}^1 \setminus \{0,1,\infty\}$ on a loop c in $E_2 \setminus \{O\}$, we have to move c inside S continuously so that (a) at each time the curve stays within a single fiber and (b) so that the shadow cast by the motion in $\mathbb{P}^1 \setminus \{0,1,\infty\}$ traces the path γ^{rev}. As we are only interested in the action on homology, we can consider free loops.

Now we have to apply this recipe to the generators. To better visualize the process, we use the pictures in the t-plane. Suppose c_λ is a loop in $E_\lambda \setminus \{O\}$ whose image in the t-plane avoids the branch points 0, 1, and λ. Then $s^2 = t(t-1)(t-\lambda)$ is bounded away from 0 along the compact loop c_λ, and we can push this loop continuously into nearby fibers without changing the image in the t-plane at all. That allows us to drag λ along sufficiently small intervals on γ; and whenever λ would run into the t-image of the curve, we deform the curve within the fiber to avoid the collision. This way, we keep $s \neq 0$ at all times and thereby do not loose control over the lift. Note that deforming a curve in the t-plane as λ traces γ^{rev} so as to avoid a collision is the same as the "push map" from the proof of Proposition 6.1.

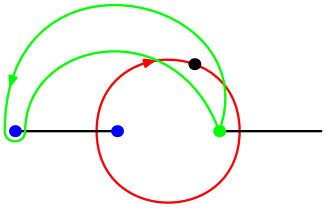
At the end of the process, we have to chose between the two possible lifts. We will rig the process so that one particular point on the initial curve stays put all time (this is easy, we just have to make sure that λ does not run into its t-projection). Assume that this point has t-coordinate t_0. From $s^2 = t_0(t_0-1)(t_0-\lambda)$, we see that the lift of this point changes sheets if and only if the path that λ traces winds around t_0 an odd number of times. This determines the lift.

Note that the push map is trivial in the pictures for $\hat{a}(\hat{x})$ and $\hat{b}(\hat{y})$:



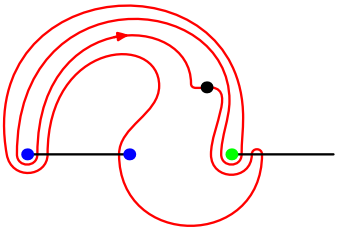
Thus, $\hat{a}(\hat{x}) = \hat{x}$ and $\hat{b}(\hat{y}) = \hat{y}$.

We now compute $\hat{a}(\hat{y})$, i.e., we have to figure out the effect of the push map in the following picture:

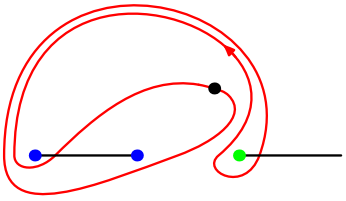


The black dot represents the point that we keep fixed along the transformation. Since the path $\hat{a}$ surrounds this point, we will encounter a change of sheets, which we will have to take into account at the end when we determine the lift.

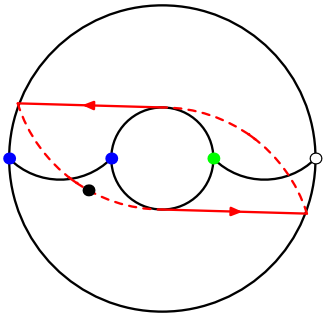
In the t-plane, the result after applying the push map is first as follows:



We can simplify this by performing some obvious shortening homotopies, still keeping the marked point fixed:

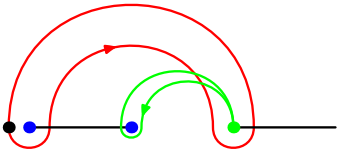


Drawing the lift in $E_2 \setminus \{O\}$, we have to remember that the marked point underwent a change of sheets, i.e., it now corresponds to a point in the bottom back of the torus:

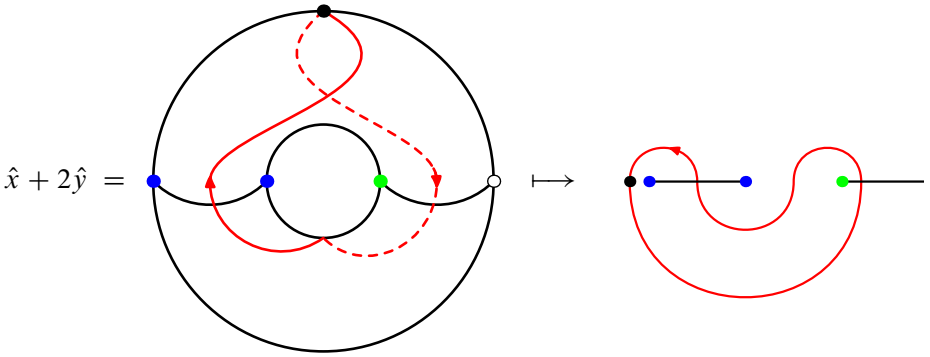


From this picture, we can read off that $\hat{a}(\hat{y}) = \hat{y} + 2\hat{x}$.

To compute $\hat{b}(\hat{x})$, we have to determine the action of the push map in the following picture:



The black dot marks the point that we keep fixed. Note that the generator $\hat{b}$ does not wind around it. After a simplifying homotopy, we get the following lift



which shows that $\hat{b}(\hat{x}) = \hat{x} + 2\hat{y}$. □

To prove the Main Theorem, Asada actually constructs, using anabelian geometry, certain lifts

$$\rho_0^* \colon \widehat{\pi_1(0,3)} \to \operatorname{Aut} \widehat{\pi_1(0,4)} \quad \text{and} \quad \rho_{\mathcal{K}} \colon \widehat{\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})} \to \operatorname{Aut} \widehat{\pi_1(E \setminus \{O\})},$$

for the homomorphisms that can be identified with the homomorphisms

$$\widehat{\pi_1(0,3)} \to \operatorname{Out} \widehat{\pi_1(0,4)} \quad \text{and} \quad \widehat{\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})} \to \operatorname{Out} \widehat{\pi_1(E \setminus \{O\})} \tag{16}$$

induced by the homomorphisms of the (discrete) fundamental groups described above (in his set-up, $\rho_{\mathcal{K}}$ is defined on a certain index two subgroup of $\widehat{\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})}$, but the passage to this subgroup is not necessary, cf. the remark prior to Lemma 4.4). The Main Theorem easily follows from the fact that $\rho_{\mathcal{K}}$ is injective, and for this Asada argues that interpreting Σ_0^3 as $\mathbb{P}^1 \setminus \{0,1,\infty\}$, we will have

$$\operatorname{Ker} \rho_0^* | \Theta = \operatorname{Ker} \rho_{\mathcal{K}} | \Theta, \tag{17}$$

where Θ is the normal subgroup of $\widehat{\pi_1(0,3)} = \widehat{\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\})}$ generated (as a closed normal subgroup) by one of the generators of the latter. Then the injectivity

of $\rho_{\mathcal{K}}$ is derived from the injectivity of ρ_0^* which is provided by Theorem 3B in [3]. Our Propositions 6.1 and 6.2 show that $\varkappa$ and ν can be taken as the lifts of the homomorphisms in (16). Then the commutativity of (11) in conjunction with Lemma 2.8 immediately yields that $\operatorname{Ker}\varkappa = \operatorname{Ker}\nu$, which is stronger than (17) and yields the desired injectivity of ν much quicker.

Acknowledgments. We are grateful to Pavel Zalesskii and to the anonymous referee for useful comments. The third-named author would like to acknowledge that he was introduced to Asada's paper by Fritz Grunewald.

References

[1] M. P. Anderson, Exactness properties of profinite completion functors. *Topology* **13** (1974), 229–239. Zbl 0324.20041 MR 0354882

[2] D. Appel and E. Ribnere, On the index of congruence subgroups of $\mathrm{Aut}(F_n)$. *J. Algebra* **321** (2009), 2875–2889. Zbl 1178.20036 MR 2512632

[3] M. Asada, The faithfulness of the monodromy representations associated with certain families of algebraic curves. *J. Pure Appl. Algebra* **159** (2001), 123–147. Zbl 1045.14013 MR 1828935

[4] E. Fadell and L. Neuwirth, Configuration spaces. *Math. Scand.* **10** (1962), 111–118. Zbl 0136.44104 MR 0141126

[5] K. W. Gruenberg, *Cohomological topics in group theory*. Lecture Notes in Math. 143, Springer-Verlag, Berlin 1970. Zbl 0205.32701 MR 0279200

[6] W. Herfort and L. Ribes, Torsion elements and centralizers in free products of profinite groups. *J. Reine Angew. Math.* **358** (1985), 155–161. Zbl 0549.20017 MR 797680

[7] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*. Interscience Publishers, New York 1966. Zbl 0138.25604 MR 0207802

[8] O. V. Mel′nikov, Characteristic subgroups and automorphisms of free profinite groups. *Mat. Zametki* **31** (1982), 339–349; English transl. *Math. Notes* **31** (1982), 174–179. Zbl 0512.20011 MR 652838

[9] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds. *Ann. of Math.* (2) **165** (2007), 171–238. Zbl 1126.20018 MR 2276769

[10] G. Prasad and A. S. Rapinchuk, Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre (2010). In *Collected papers of John Milnor*, Vol. V, Algebra, Amer. Math. Soc., Providence, RI, 2010, 307–325.

[11] L. Ribes and P. Zalesskii, *Profinite groups*. Ergeb. Math. Grenzgeb. (3) 40, Springer-Verlag, Berlin 2000. Zbl 0949.20017 MR 1775104

[12] D. J. S. Robinson, *A course in the theory of groups*. 2nd ed., Grad. Texts in Math. 80, Springer-Verlag, New York 1996. Zbl 0836.20001 MR 1357169

[13] V. A. Roman′kov, Infinite generation of automorphism groups of free pro-p groups. *Sibirsk. Mat. Zh.* **34** (1993), No. 4, 153–159; English transl. *Siberian Math. J.* **34** (1993), 727–732. Zbl 0824.20031 MR 1248800

[14] I. N. Sanov, A property of a representation of a free group (Russian). *Doklady Akad. Nauk SSSR* (*N. S.*) **57** (1947), 657–659. Zbl 0029.00404 MR 0022557

[15] J.-P. Serre, *Trees*. Springer-Verlag, Berlin 1980. Zbl 0548.20018 MR 0607504

[16] J. H. Smith, On products of profinite groups. *Illinois J. Math.* **13** (1969), 680–688. Zbl 0182.35001 MR 0257232

[17] J. S. Wilson, *Profinite groups*. London Math. Soc. Monogr. (N.S.) 19, Oxford University Press, Oxford 1998. Zbl 0909.20001 MR 1691054

Received August 31, 2009; revised March 3, 2010

K.-U. Bux, Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, 33501 Bielefeld, Germany

E-mail: bux_2009@kubux.net

M. V. Ershov, Department of Mathematics, University of Virginia, Charlottesville, VA 22904-4137, U.S.A.

E-mail: ershov@virginia.edu

A. S. Rapinchuk, Department of Mathematics, University of Virginia, Charlottesville, VA 22904-4137, U.S.A.

E-mail: asr3x@virginia.edu