The congruence subgroup property of the automorphism group of the free group on two generators

Jacqueline Lefèvre López

Department of Mathematics & Statistics

McGill University, Montréal

December 2019

A thesis submitted to McGill University

in partial fulfillment of the requirements of the degree of Masters of Science.

Acknowledgements

I would like to express my immense gratitude to my supervisor Prof. Mikael Pichot for his invaluable help and guidance. I would also like to thank the Department of Mathematics & Statistics and Hydro-Québec for their generous financial support over these past years. Last but not least, I would like to thank my fellow students and office mates for their helpful discussions in my study.

Abstract

In this thesis, we present the proof of the congruence subgroup property of $\mathrm{Aut}(F_2)$ — the automorphism group of the free group on two generators — in a group-theoretical setting. We follow the main ideas of Lubotzky and Ben-Ezra, based on a previous result by Bux, Ershov and Rapinchuk. This surprising result was first proven by Asada using anabelian geometric techniques.

Abrégé

Dans cette thèse, on présente la preuve de la propriété des groupes de congruence pour $\mathrm{Aut}(F_2)$ – le groupe des automorphismes du groupe libre à deux générateurs – du point de vue de la théorie des groupes. On suit les idées principales de Lubotzky et Ben-Ezra, basées sur un résultat précédent de Bux, Ershov et Rapinchuk. Ce résultat surprenant a d'abord été prouvé par Asada en utilisant des techniques géométriques anabeliennes.

Contents

Chapter 1

Introduction

Let $n \geq 2$. For every $m \geq 2$, set $\Gamma[m]$ to be the kernel of the canonical homomorphism

$$GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/m\mathbb{Z})$$

induced by $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. $\Gamma[m]$ is called the *principal congruence subgroup* of $GL_n(\mathbb{Z})$ of level m. A *congruence subgroup* of $GL_n(\mathbb{Z})$ is then defined as a subgroup that contains $\Gamma[m]$ for some $m \in \mathbb{Z}$. Such subgroups are the most obvious finite index subgroups of $GL_n(\mathbb{Z})$. It is then natural to ask if the converse – every finite index subgroup of $GL_n(\mathbb{Z})$ is a congruence group – holds. This is known as the *congruence subgroup problem*.

By observing that $GL_n(\mathbb{Z})$ is the automorphism group of $\mathbb{Z}^n$ – the free abelian group on n generators – we can generalize the classical congruence subgroup problem to $\mathrm{Aut}(G)$ – the automorphism group of a finitely generated group G. We say that G has the *congruence subgroup property* if the converse holds. If there are no ambiguities, we can also say that $\mathrm{Aut}(G)$ has the congruence subgroup property.

It is a classical result, known already to Klein and Fricke in the 19th century (c.f. [10]), that $\mathbb{Z}^2$ does not have the congruence subgroup property. In 2001, Asada showed the surprising result that this property holds for F_2 [1]. The original argument in [1] was based on techniques

from anabelian geometry.

Main Theorem. (c.f. [1], Theorem 5) $\mathrm{Aut}(F_2)$ has the congruence subgroup property.

The main goal of this thesis is to present a group-theoretical proof of this theorem. This argument was first presented by Bux, Ershov and Rapinchuk in [5], and later shortened by Ben-Ezra and Lubotzky in [4]. In Chapter 2, we study the general setting of the congruence subgroup problem for $\mathrm{Aut}(F_2)$. In Chapter 3, we review the facts about profinite groups that are needed for a direct proof of the Main Theorem. Finally, in Chapter 4, we give a procedure for constructing explicit congruence subgroups of $\mathrm{Aut}(F_2)$.

Chapter 2

Congruence Subgroup Problem

2.1 Congruence Subgroup Problem for $SL_n(\mathbb{Z})$

Consider the principal congruence subgroups of $SL_n(\mathbb{Z})$, the simplest interesting setting for the congruence subgroup problem,

$$\Gamma[m] = \ker\left(SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/m\mathbb{Z}) \right).$$

In 1964, Bass, Lazard and Serre showed the non-trivial result that, for $n \geq 3$, $SL_n(\mathbb{Z})$ has the congruence subgroup property [2]. For $n = 2$, this property is not satisfied as the subgroup of index 12 in $SL_2(\mathbb{Z})$ generated by the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

is free of rank 2. A non-congruence subgroup can then be easily constructed from A and B, as done in Example 2.3.4.

2.2 Congruence Subgroup Problem for $\mathrm{Aut}(G)$

Let G be a finitely generated group and let K be a characteristic subgroup of finite index in G. Then $\mathrm{Aut}(G)$ acts on the quotient group G/K, and the kernel of this action corresponds to a principal congruence subgroup:

$$\Gamma[K] = \mathrm{Ker}(\mathrm{Aut}(G) \to \mathrm{Aut}(G/K)).$$

More generally, for a normal subgroup K of finite index in G, we can define the standard congruence subgroup associated to K in the following way:

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

Equivalently, we can consider an epimorphism $\pi : G \to H$ where H is a finite group. The standard congruence subgroup associated to H and π is then:

$$\Gamma[H, \pi] = \{\, \sigma \in \mathrm{Aut}(G) \mid \pi\sigma = \pi \,\}.$$

Clearly, a congruence subgroup is a finite-index subgroup of $\mathrm{Aut}(G)$. Similarly to the classical congruence subgroup problem, it is natural to ask if every finite-index subgroup of $\mathrm{Aut}(G)$ contains a suitable congruence subgroup. This remains an open problem for $G = F_n$, the free group on n generators. However, it was proved by Asada [1] that $\mathrm{Aut}(F_2)$ does have the congruence subgroup property. In Chapter 3, Section 3.4, we will give a group-theoretic proof for the Main Theorem.

2.3 Examples of Congruence Subgroups

We start by giving two examples of congruence subgroups of $SL_2(\mathbb{Z})$.

Example 2.3.1. Consider the subgroups $\Gamma_0(m)$ of $SL_2(\mathbb{Z})$ defined as the preimage of the upper triangular matrices under $\pi_m : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$. These are called the Hecke

congruence subgroups of level m in $SL_2(\mathbb{Z})$ and can be explicitly defined as follows:

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{m} \right\}.$$

Using the Chinese Remainder Theorem, we can compute their index :

$$[\, SL_2(\mathbb{Z}) : \Gamma_0(m) \,] = m \cdot \prod_{p \,|\, m} \left(1 + \frac{1}{p}\right),$$

where p runs through the primes dividing m. Observe that for all m,

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(m)$$

therefore none of the Hecke congruence subgroups are torsion-free.

Example 2.3.2. Let $\Gamma_1(m) \leq SL_2(\mathbb{Z})$ be the preimage of the unipotent matrices under $\pi_m : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$ defined as

$$\Gamma_1(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ a, d \equiv 1 \pmod{m} \text{ and } c \equiv 0 \pmod{m} \right\}.$$

As opposed to $\Gamma_0(m)$, they are torsion-free when $m \geq 3$ and their index is given by

$$[\, SL_2(\mathbb{Z}) : \Gamma_1(m) \,] = m^2 \cdot \prod_{p \,|\, m} \left(1 - \frac{1}{p^2}\right),$$

where p runs through the primes dividing m.

Remark 2.3.3. These examples can easily be extended to the $SL_n(\mathbb{Z})$ case by letting $\Gamma_0^n(m)$ and $\Gamma_1^n(m)$ be the preimage of the upper triangular matrices and the preimage of the unipotent matrices under $\pi_m : SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/m\mathbb{Z})$, respectively.

Next, we give an example of a non-congruence subgroup of $SL_2(\mathbb{Z})$.

Example 2.3.4 (c.f. [10], Example 3-4.2)**.** Recall that the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

generate a free subgroup F in $SL_2(\mathbb{Z})$ of finite index. Define an homomorphism

$$E_A : F \to \mathbb{Z}$$

by sending any word w in F to the sum of all the exponents of A appearing in w. Let $l = 2k$, where $k > 1$ is an odd number. We claim that

$$\Gamma_l = \{\, w \in F \mid E_A(w) \equiv 0 \pmod{l} \,\}$$

is a non-congruence subgroup of $SL_2(\mathbb{Z})$.

Observe that

$$A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \in \Gamma(n)$$

so if n is not a multiple of k, $\Gamma(n) \nsubseteq \Gamma_l$. It remains to show that $\Gamma(kn)$ is not contained in Γ_l for any n.

Assume that $\Gamma(2^m kn) \subset \Gamma_l$ for some $m \geq 0$ and odd n. Since $2^m 5\, kn$ and $5kn - 4$ are relatively prime, there exists $s \in \mathbb{Z}$ such that

$$\begin{aligned} s(5kn - 4) &\equiv 1 \pmod{2^m 5\, kn} \\ s &\equiv 1 \pmod{5}. \end{aligned} \tag{2.1}$$

Rewrite s as $s = 5r + 1$ and consider the following matrices in F:

$$P = B^r ABA^{kn-1} = \begin{pmatrix} 5 & 2(5kn-4) \\ 2s & x \end{pmatrix}$$
$$Q = A^{5kn-4} B^s = \begin{pmatrix} y & 2(5kn-4) \\ 2s & 1 \end{pmatrix}.$$

for some x and some y. The conditions $\det(P) = 1$ and $\det(Q) = 1$ together with (2.1) give that $x \equiv 1 \pmod{2^m kn}$ and $y \equiv 5 \pmod{2^m kn}$. This implies that $P \equiv Q \pmod{2^m kn}$, i.e. $PQ^{-1} \in \Gamma(2^m kn)$. However, $E_A(PQ^{-1}) \equiv 4 \pmod{l}$, so $PQ^{-1} \notin \Gamma_l$. This contradicts our initial assumption.

Example 2.3.5. Consider the well-known homomorphism

$$1 \to \mathrm{Inn}(F) \to \mathrm{Aut}(F_2) \xrightarrow{\theta} GL_2(\mathbb{Z}) \to 1$$

and denote by $\mathrm{Aut}'(F_2)$ the preimage of the free group generated by

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

under the map θ, which we denote by $SL_2'(\mathbb{Z})$ (more details in Section 3.4). $\mathrm{Aut}'(F_2)$ is a subgroup of finite index in $\mathrm{Aut}(F_2)$ which contains the principal congruence subgroup

$$\ker\left(\; \mathrm{Aut}(F_2) \to GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/4\mathbb{Z}) = \mathrm{Aut}\left(F_2/\left({F_2}^4 {F_2}'\right)\right) \; \right).$$

It is therefore a congruence subgroup of $\mathrm{Aut}(F_2)$. It will play an important role both in the profinite proof of the congruence subgroup property of $\mathrm{Aut}(F_2)$, detailed in Section 3.4, and in the explicit construction of congruence subgroups given in Chapter 4.

Remark 2.3.6. The proof of the congruence subgroup property of $\mathrm{Aut}(F_2)$ relies on the fact that $SL_2(\mathbb{Z})$ has a free subgroup of finite index. It is interesting to note that this is exactly what prevents $SL_2(\mathbb{Z})$ from having the congruence subgroup property.

Chapter 3

Profinite Groups

We start by reviewing some basic facts about profinite groups (c.f. [9]) that are needed for the proof of the Main Theorem. Before restating the Main Theorem, we recall the standard formulation of the congruence subgroup problem in Section 3.2.

3.1 Basic Notions on Profinite Groups

Definition 3.1.1. We say that a profinite group $\mathfrak{G}$ is finitely generated if there exists $g_1, ..., g_n \in \mathfrak{G}$ such that the subgroup generated by those elements is dense in $\mathfrak{G}$. In other words, if N is an open subgroup of finite index in $\mathfrak{G}$, then the images of g_i in $\mathfrak{G}/N$ generate the finite quotient.

Then, if G is a finitely generated group, its profinite completion $\widehat{G}$ is finitely generated as a profinite group.

Definition 3.1.2. If $\mathfrak{G}$ is a profinite group, then $\mathrm{Aut}(\mathfrak{G})$ denotes the group of continuous automorphisms of $\mathfrak{G}$.

It is known however that if $\mathfrak{G}$ is a finitely generated profinite group, then every abstract automorphism of $\mathfrak{G}$ is also continuous. This result is stated in [8] as follows:

Lemma 3.1.3. Every finitely generated profinite group $\mathfrak{G}$ is strongly complete, i.e. it satisfies the equivalent following conditions:

(a) Every subgroup of finite index in $\mathfrak{G}$ is open,

(b) $\mathfrak{G}$ is equal to its own profinite completion,

(c) Every group homomorphism from $\mathfrak{G}$ to any profinite group is continuous.

Remark 3.1.4. It is natural to ask if the converse of Lemma 3.1.3 (a) holds true. In general, this remains an open problem. Yet, for some particular cases, it has been shown to be true. For instance, the converse holds for finitely generated pro-p groups.

Lemma 3.1.5. If $\mathfrak{G}$ is a finitely generated profinite group, then its automorphism group $\operatorname{Aut}\mathfrak{G}$ is profinite as well.

Proof. Let $\mathfrak{G}$ be a finitely generated profinite group and let U_n be the intersection of all its (open normal) subgroups of index less or equal to n. Since $\mathfrak{G}$ is profinite, U_n is itself a normal open subgroup. Moreover, U_n is invariant under automorphisms, so we get a homomorphism $\operatorname{Aut}(\mathfrak{G}) \to \operatorname{Aut}(\mathfrak{G}/U_n)$. The subgroups U_n form a neighbourhood basis for the identity in $\mathfrak{G}$, so the inverse system of finite groups $\mathfrak{G}/U_n$ converges to $\mathfrak{G}$. The automorphism group $\operatorname{Aut}(\mathfrak{G})$ can then be naturally identified with

$$\varprojlim \operatorname{Aut}(\mathfrak{G}/U_n),$$

making it a profinite group.

□

3.2 Profinite Formulation of the Congruence Subgroup Problem

Let G be a finitely generated group. It is standard to reformulate the congruence subgroup problem to turn it into a comparison of topologies of $\mathrm{Aut}(G)$. Consider the congruence subgroups associated to characteristic subgroups K of finite index in G :

$$\Gamma[K] = \ker(\,\mathrm{Aut}(G) \to \mathrm{Aut}(G/K)\,).$$

This family of subgroups forms a fundamental system of neighbourhoods of the identity for a topology on $\mathrm{Aut}(G)$. We denote this topology by τ_{c} and its completion by $\overline{\mathrm{Aut}(G)}$.

Similarly, the family of subgroups of finite index in $\mathrm{Aut}(G)$ forms a fundamental system of neighbourhoods of the identity for another topology on $\mathrm{Aut}(G)$, called the profinite topology. We denote it by τ_{pf} and its completion by $\widehat{\mathrm{Aut}(G)}$.

Since a priori τ_{pf} is finer than τ_{c}, the identity map on $\mathrm{Aut}(G)$ induces a surjective homomorphism

$$\widehat{\mathrm{Aut}(G)} \to \overline{\mathrm{Aut}(G)}.$$

Then, an equivalent formulation of the congruence subgroup problem is whether or not this map is also injective, namely if the congruence kernel of $\mathrm{Aut}(G)$

$$C(G) = \mathrm{Ker}(\widehat{\mathrm{Aut}(G)} \to \overline{\mathrm{Aut}(G)})$$

is trivial or not. We can slightly weaken the congruence subgroup property by asking whether or not this kernel is finite.

Clearly, $\widehat{\mathrm{Aut}(G)}$ is the profinite completion of $\mathrm{Aut}(G)$. On the other hand, the pullback of the topology on $\mathrm{Aut}(\widehat{G})$ under the natural map $\mathrm{Aut}(G) \xrightarrow{\iota} \mathrm{Aut}(\widehat{G})$ can be identified with τ_c. It follows that $\overline{\mathrm{Aut}(G)}$ can be identified to the closure of $\mathrm{Im}\,\iota$ in $\mathrm{Aut}(\widehat{G})$. Then, the question

becomes if the natural homomorphism $\widehat{\mathrm{Aut}(G)} \to \mathrm{Aut}(\widehat{G})$ is injective.

Recall that for a profinite group $\mathfrak{G}$, $\mathrm{Aut}(\mathfrak{G})$ denotes the group of continuous automorphisms of $\mathfrak{G}$. However, as seen in Lemma 3.1.3, if $\mathfrak{G}$ is finitely generated, then every abstract automorphism of $\mathfrak{G}$ is also continuous. In this case, by Lemma 3.1.5, $\mathrm{Aut}(\mathfrak{G})$ is itself profinite. Therefore, the above homomorphism $\widehat{\mathrm{Aut}(G)} \to \mathrm{Aut}(\widehat{G})$ is a result of the universal property of profinite groups, applied to $\mathrm{Aut}(G) \to \mathrm{Aut}(\widehat{G})$.

We reformulate the congruence subgroup property of $\mathrm{Aut}(F_2)$ in the following way:

Main Theorem (Asada)**.** $\mathrm{Aut}(F_2)$ satisfies the congruence subgroup property, namely

$$\widehat{\mathrm{Aut}(F_2)} \to \mathrm{Aut}(\widehat{F}_2)$$

is injective.

3.3 More Facts about Profinite Groups

In this section, we recall some important properties of profinite groups (c.f. [5]), as they are needed to study this new version of the congruence subgroup problem.

Proposition 3.3.1. Let

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

be a short 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 profinite completions

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

is also exact.

Proof. We view G_1 as a normal subgroup of G_2. Note that the conjugation action of G_2 on G_1 extends to an action of G_2 on $\widehat{G}_1$, giving rise to a homomorphism $\varphi : G_2 \to \mathrm{Aut}(\widehat{G}_1)$. Now, since G_1 is finitely generated, it follows by Lemma 3.1.5 that $\mathrm{Aut}(\widehat{G}_1)$ is a profinite group. Then, $\varphi : G_2 \to \mathrm{Aut}(\widehat{G}_1)$ extends to a continuous homomorphism $\widehat{\varphi} : \widehat{G}_2 \to \mathrm{Aut}(\widehat{G}_1)$ so that the following diagram commutes:

$$\begin{array}{ccc} \widehat{G}_1 & \xrightarrow{\widehat{\alpha}} & \widehat{G}_2 \\ & \searrow^{\psi} & \downarrow{\scriptstyle \widehat{\varphi}} \\ & & \mathrm{Aut}(\widehat{G}_1) \end{array}$$

where ψ is the extension of the conjugation action of G_1 on $\widehat{G}_1$. Observe that $\ker(\psi)$ is precisely the center of $\widehat{G}_1$ which, by assumption, is trivial. It follows that $\widehat{\alpha}$ is injective.
Now, consider the following commutative diagram:

$$\begin{array}{ccc} G_2 & \xrightarrow{\beta} & G_3 \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ \widehat{G}_2 & \xrightarrow{\widehat{\beta}} & \widehat{G}_3 \end{array}$$

We have that $\widehat{\beta}(\widehat{G}_2) = \overline{(\iota\beta)(G_2)}$, where $\overline{(\iota\beta)(G_2)}$ denotes de closure of $(\iota\beta)(G_2)$ in $\widehat{G}_3$. By assumption $\beta(G_2) = G_3$, yielding the surjectivity of $\widehat{\beta}$.
Finally, β defines an isomorphism $G_2/\operatorname{Im}\alpha \xrightarrow{\simeq} G_3$, and its inverse gives rise to a natural map $G_3 \to \widehat{G}_2/\operatorname{Im}\widehat{\alpha}$. The latter satisfies the universal property for the completion of G_3 so it follows that $\operatorname{Im}\widehat{\alpha} = \ker\widehat{\beta}$, as required.

□

Proposition 3.3.2. Let F be the free group on a finite set $X = \{x_1, ..., x_n\}$, $n \geq 2$, and let $G = F/N$ be a finite quotient of F. Pick a prime p not dividing $|G|$ and let $M = N^p[N, N]$. Denote by $\gamma : F/M \to F/N$ the canonical homomorphism. Then,

(i) $\gamma(C_{F/M}(xM))$ coincides with the cyclic group $\langle xN \rangle$ for all $x \in X$;

(ii) for any abelian normal subgroup H of F/M, $\gamma(H) = \{e\}$.

Proof. Consider the $\mathbb{Z}[G]$-module $\mathcal{N} = N/[N,N]$. We recall the construction done in [6] of the following short exact sequence of $\mathbb{Z}[G]$-modules:

$$0 \to \mathcal{N} \xrightarrow{\sigma} \mathbb{Z}[G]^n \xrightarrow{\tau} \mathcal{G} \to 0 \tag{3.1}$$

where $\mathcal{G}$ is the augmentation ideal of $\mathbb{Z}[G]$. It is well-known that the augmentation ideal $\mathcal{F}$ of $\mathbb{Z}[F]$ is a left $\mathbb{Z}[F]$-module with basis $x_1 - 1, ..., x_n - 1$. Then, for every $w \in F$, we have

$$w = c_1(w)(x_1 - 1) + ... + c_n(w)(x_n - 1)$$

for some unique $c_1(w), \dots, c_n(w) \in \mathbb{Z}[F]$. Denote by $\overline{y}$ the image of $y \in \mathbb{Z}[F]$ in $\mathbb{Z}[G]$, and define σ by sending $w \in N$ to $(\overline{c_1(w)}, ..., \overline{c_n(w)}) \in \mathbb{Z}[G]^n$. Define τ by sending $(c_1, ..., c_n) \in \mathbb{Z}[G]^n$ to $\sum c_i(\overline{x_i} - 1)$.

Observe that all the terms in (3.1) are free $\mathbb{Z}$-modules. Then, by tensoring them with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we get the following exact-sequence of $\mathbb{F}_p[G]$-modules:

$$0 \to \mathcal{N}_p \xrightarrow{\sigma_p} \mathbb{F}_p[G]^n \xrightarrow{\tau_p} \mathcal{G}_p \to 0 \tag{3.2}$$

where $\mathcal{N}_p = \mathcal{N} \otimes_{\mathbb{Z}} \mathbb{F}_p$ and $\mathcal{G}_p = \mathcal{G} \otimes_{\mathbb{Z}} \mathbb{F}_p$. Observe that $\mathcal{N}_p = N/M$ and $\mathcal{G}_p$ is the augmentation ideal of $\mathbb{F}_p$. Then, since p does not divide the order of G, the exact sequence in (3.2) splits, yielding the following isomorphism of $\mathbb{F}_p[G]$-modules:

$$N/M \simeq \mathbb{F}_p[G]^{n-1} \oplus \mathbb{F}_p. \tag{3.3}$$

Moreover, since the order of G is coprime to the order of N/M, we can fix a semi-direct product decomposition $F/M \simeq N/M \rtimes G$. This allows us to see G as a subgroup of F/M.

To prove (i), fix $x \in X$ and consider its image $\overline{x}$ in G. Denote by d the order of the latter. Then, $h := \overline{x}^d M$ belongs to N/M. Now, consider $yM \in C_{F/M}(xM)$. Observe that under the canonical homomorphism $\gamma : F/M \to F/N$, the image of $\langle yM \rangle$ is equal to the image of $\langle y^{p^l} M \rangle$

for any $l \geq 1$. Therefore, it suffices to prove the claim when the order of yM is coprime to p. In this case, there exists $zM \in N/M$ such that $g := (z^{-1}y\,z)M$ is in G. Since yM commutes with $h = \overline{x}^{\,d}M$ and N/M is abelian, it follows that g commutes with h. In other words, when N/M is seen as a $\mathbb{F}_p$-module, $h \in N/M$, so $\sigma_p(h)$ is fixed by g. Explicitly, we have:

$$\sigma_p(h) = \left(\sum_{j=0}^{d-1} \overline{x}^{\,j},\, 0\,, \ldots, 0 \right) \in \mathbb{F}_p[G]^n.$$

So,

$$g \sum_{j=0}^{d-1} \overline{x}^{\,j} = \sum_{j=0}^{d-1} \overline{x}^{\,j}$$

which implies that $\gamma(yM) = g \in \langle xN \rangle$, as desired.

To prove (ii), consider an abelian subgroup H of F/M. Observe that for any $l \geq 1$, the subgroup H^{p^l} is also normal in F/M and $\gamma(H^{p^l}) = \gamma(H)$. We can therefore assume that the order of H is relatively prime to p. Then, there exists $y \in N/M$ such that $yHy^{-1} \subset G$. Since H is normal, it follows that $H \subset G$. Assume that $H \neq \{e\}$. Then, it follows by (3.3) that there exists $h \in H$ and $k \in N/M$ such that $hkh^{-1} \neq h$. However, this implies that

$$1 \neq hkh^{-1}k^{-1} \in H \cap N/M,$$

a contradiction.

□

Corollary 3.3.3. Let F be the free group on the finite set X, with $|X| \geq 2$. We denote by $\widehat{F}$ its profinite completion. Then,

(i) for any $x \in X$, the centralizer $C_{\widehat{F}}(x)$ coincides with the pro-cyclic group $\widehat{\langle x \rangle}$. In particular, $\widehat{F}$ has trivial center;

(ii) if H is an abelian normal subgroup of $\widehat{F}$ then $H = \{e\}$.

Proof. We view F as a (dense) subgroup of $\widehat{F}$. Assume (i) does not hold. Then, there exists an open normal subgroup U of $\widehat{F}$ such that the image of $C_{\widehat{F}}(x)$ in $\widehat{F}/U$ strictly contains $\langle x\,U \rangle$.

Let $N = F \cap U$ and denote by $\pi_N : \widehat{F} \to F/N$ the homomorphism induced by the natural isomorphism $\widehat{F}/U \simeq F/N$. It follows that $\langle xN \rangle$ is strictly contained in $\pi_N(C_{\widehat{F}}(x))$. Now, pick a prime p not dividing $|F/N|$. Let $M = N^p[N,N]$ and denote by $\pi_M : \widehat{F} \to F/M$ the canonical homomorphism. Observe that $\pi_M(C_{\widehat{F}}(x)) \subseteq C_{F/M}(xM)$. By Proposition 3.3.2 (i), the image of $C_{F/M}(xM)$ in F/N coincides with $\langle xN \rangle$. This implies that $\pi_N(C_{\widehat{F}}(x)) \subseteq \langle xN \rangle$, which contradicts our assumption. It follows that $\widehat{F}$ has trivial center since for $x, y \in X$, $x \neq y$, we have $\widehat{\langle x \rangle} \cap \widehat{\langle y \rangle} = \{e\}$.

To prove (ii), assume that H is a non-trivial abelian normal subgroup of $\widehat{F}$. Choose an open normal subgroup U of $\widehat{F}$ that does not contain H. Set $N = F \cap U$ and $M = N^p[N,N]$ where p is a prime not dividing F/N. Let V be the closure of M in $\widehat{F}$. Then HV/V is an abelian normal subgroup of $\widehat{F}/V \simeq F/M$. So, by Proposition 3.3.2 (ii), its image is trivial in F/N. Using the isomorphism $\widehat{F}/U \simeq F/N$ we conclude that $H \subseteq U$, which contradicts our assumption.

□

We recall now a classical result of Schreier:

Theorem 3.3.4. (cf. [7], Section 2.3) Let F be a free group on the set X, with $|X| = n$. Let H be a subgroup in F of index m, and let T be a right transversal to H in F with the Schreier property. In other words, T is a system of representatives of rights cosets of H containing the identity such that the initial segment of any element in T is again in T. Then:

(i) H is a free group on $m \cdot (n-1) + 1$ elements.

(ii) The set $\left\{ tx\,(\overline{tx})^{-1} \neq e \mid t \in T, x \in X \right\}$ is a free generating set for H, where $\overline{w}$ denotes the unique element in T that satisfies $Hw = H\overline{w}$, for any $w \in F$.

Lemma 3.3.5. Let F be the free group on $X = \{x_1, ..., x_n\}$, with $n \geq 2$. Let $G = F/N$ be a finite quotient of F and pick a prime not dividing $6\,|G|$. Set $L = N \cap F^6[F,F]$, $M = L^p[L,L]$ and denote by $\gamma : F/N \to F/M$ the canonical homomorphism. Then, for $x_{ij} = [x_i, x_j]$, $i \neq j$, we have $\gamma(C_{F/M}(x_{ij}M)) = \langle x_{ij}L \rangle$.

Proof. Let $H = F^2[F,F]$ and $K = F^3[F,F]$. The set

$$T_H = \{\, x_1^{\epsilon_1} ... x_n^{\epsilon_n} \mid \epsilon_i \in \{0,1\} \,\}$$

is a right Schreier transversal to H in F. Applying Schreier's method (Theorem 3.3.4), we get that H is a free group on a set containing x_{ij}. By Proposition 3.3.2 (i), we get that $\gamma(C_{H/M}(x_{ij}M)) = \langle x_{ij}L \rangle$. Observe that $F^2 \subset H$, therefore it follows that

$$\text{for any } t \in C_{F/M}(x_{ij}M) \text{ we have } \gamma(t)^2 \in \langle x_{ij}L \rangle. \tag{3.4}$$

Similarly,

$$T_K = \{\, x_1^{\epsilon_1} ... x_n^{\epsilon_n} \mid \epsilon_i \in \{0,1,2\} \,\}$$

is a right Schreier transversal to K in F. Applying again Theorem 3.3.4, we get that K is a free group on a set containing x_{ij}, so $\gamma(C_{K/M}(x_{ij}M)) = \langle x_{ij}L \rangle$. As $F^3 \subset K$, we obtain that

$$\text{for any } t \in C_{F/M}(x_{ij}M) \text{ we have } \gamma(t)^3 \in \langle x_{ij}L \rangle. \tag{3.5}$$

The result follows from (3.4) and (3.5).

□

Corollary 3.3.6. Let F be the free group on a finite set X with $|X| \geq 2$. Then, for any $x, y \in X$, $x \neq y$, the centralizer of $[x,y]$ in $\widehat{F}$ is $C_{\widehat{F}}([x,y]) = \widehat{\langle [x,y] \rangle}$, the closure of the cyclic group generated by $[x,y]$.

This is derived from Lemma 3.3.5 just as Corollary 3.3.3 (i) was derived from Proposition 3.3.2 (i).

We summarize the results of Corollary 3.3.3 and Corollary 3.3.6 in the following proposition:

Proposition 3.3.7. Let F be the free group on a finite set X, $|X| \geq 2$. Then:

(i) The center of $\widehat{F}$ is trivial.

(ii) If $x, y \in X$, $x \neq y$, then $C_{\widehat{F}}([x,y]) = \widehat{\langle [x,y] \rangle}$.

3.4 Congruence Subgroup Property of $\mathrm{Aut}(F_2)$

We now present a recent short proof of the congruence subgroup property for $\mathrm{Aut}\, F_2$ by Ben-Ezra and Lubotzky [4].

Observe that if G is a finitely generated group and $\Gamma \leq \mathrm{Aut}(G)$ is a congruence subgroup. Then,

$$\ker\left(\widehat{\mathrm{Aut}(G)} \to \mathrm{Aut}(\widehat{G})\right) = \ker\left(\widehat{\Gamma} \to \mathrm{Aut}(\widehat{G})\right).$$

In particular, the map $\widehat{\mathrm{Aut}(G)} \to \mathrm{Aut}(\widehat{G})$ is injective if and only if the map $\widehat{\Gamma} \to \mathrm{Aut}(\widehat{G})$ is injective. Therefore, to show the Main Theorem, it suffices to show that the latter homomorphism is injective.

Denote by F_2 the free group with generators x and y. It is well-known that the kernel of the canonical surjective homomorphism

$$\mathrm{Aut}(F_2) \to \mathrm{Aut}(F_2^{\mathrm{ab}})$$

corresponds to $\mathrm{Inn}(F_2)$, the inner automorphism group of F_2. Then, the identification $F_2^{\mathrm{ab}} \simeq \mathbb{Z}^2$ yields the following exact sequence:

$$1 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}(F_2) \xrightarrow{\theta} GL_2(\mathbb{Z}) \to 1.$$

Let $SL_2'(\mathbb{Z})$ denote the subgroup of finite index in $SL_2(\mathbb{Z})$ (freely) generated by

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

and consider the subgroup of finite index

$$\mathrm{Aut}'(F_2) := \theta^{-1}(SL_2'(\mathbb{Z}))$$

in $\mathrm{Aut}(F_2)$. Now, as seen in Example 2.3.5, it follows that $\mathrm{Aut}'(F_2)$ is a congruence subgroup of $\mathrm{Aut}\, F_2$ since it contains the following principal congruence subgroup :

$$\ker\left(\mathrm{Aut}(F_2) \xrightarrow{\theta} GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/4\mathbb{Z}) = \mathrm{Aut}(F_2/({F_2}^{\mathrm{ab}}\, {F_2}^4))\right).$$

Then, by the previous discussion, it is enough to show that $\widehat{\mathrm{Aut}'(F_2)} \to \mathrm{Aut}(\widehat{F_2})$ is injective to prove the Main Theorem.

Lemma 3.4.1. $\widehat{\mathrm{Aut}'(F_2)} = \widehat{\mathrm{Inn}(F_2)} \rtimes \widehat{\langle \alpha, \beta \rangle}$.

Proof. From the discussion above, we can derive the following exact sequence

$$1 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}'(F_2) \xrightarrow{\theta} SL_2'(\mathbb{Z}) \to 1.$$

Then, since $SL_2'(\mathbb{Z})$ is free, the following map corresponds to a section of θ, which we denote by ν_0:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \mapsto \alpha = \begin{cases} x & \mapsto x \\ y & \mapsto yx^2 \end{cases}$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \mapsto \beta = \begin{cases} x & \mapsto xy^2 \\ y & \mapsto y \end{cases}$$

giving $\mathrm{Aut}'(F_2) = \mathrm{Inn}(F_2) \rtimes \langle \alpha, \beta \rangle$. Then, by Proposition 3.3.1 and Proposition 3.3.7 (i), the exact sequence

$$1 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}'(F_2) \to \langle \alpha, \beta \rangle \to 1 \tag{3.6}$$

yields the following exact sequence

$$1 \to \widehat{\mathrm{Inn}(F_2)} \to \widehat{\mathrm{Aut}'(F_2)} \to \widehat{\langle \alpha, \beta \rangle} \to 1.$$

We get $\widehat{\mathrm{Aut}'(F_2)} = \widehat{\mathrm{Inn}(F_2)} \rtimes \widehat{\langle \alpha, \beta \rangle}$, as desired.

□

It remains to show that the following map is injective:

$$\widehat{\mathrm{Inn}(F_2)} \rtimes \widehat{\langle \alpha, \beta \rangle} \to \mathrm{Aut}(\widehat{F}_2).$$

Clearly, $\widehat{\mathrm{Inn}(F_2)} \to \mathrm{Aut}(\widehat{F}_2)$ is injective as $\widehat{\mathrm{Inn}(F_2)} \simeq \widehat{F}_2 \simeq \mathrm{Inn}(\widehat{F}_2)$. We will show next that the map $\rho : \widehat{\langle \alpha, \beta \rangle} \to \mathrm{Aut}(\widehat{F}_2)$ is injective as well and that $\mathrm{Inn}(\widehat{F}_2) \cap \mathrm{Im}\,\rho = \{e\}$.

Lemma 3.4.2. The map $\rho : \widehat{\langle \alpha, \beta \rangle} \to \mathrm{Aut}(\widehat{F}_2)$ is injective.

Proof. Define the subgroup $H = \ker(F_2 \to (\mathbb{Z}/2\mathbb{Z})^2)$ of F_2. Then H is a characteristic subgroup of index 4 in F_2. Observe that $\widehat{H} = \ker(\widehat{F}_2 \to (\mathbb{Z}/2\mathbb{Z})^2)$, so we have a canonical homomorphism $\varphi : \mathrm{Aut}(\widehat{F}_2) \to \mathrm{Aut}(\widehat{H})$.

We next construct a homomorphism $\mathrm{Aut}(\widehat{H}) \to \mathrm{Aut}(\widehat{\langle \alpha, \beta \rangle})$. To show that ρ is injective, it will suffice to show that the composition of the latter map with $\varphi \circ \rho : \widehat{\langle \alpha, \beta \rangle} \to \mathrm{Aut}(\widehat{H})$ is injective.

Consider the right Schreier transversal of H in F_2, $T = \{e, x, y, xy\}$. Then, by Schreier's method (Theorem 3.3.4), it follows that H is isomorphic to F_5 and is freely generated by

$$x_1 = x^2, \quad x_2 = yxy^{-1}x^{-1}, \quad x_3 = y^2, \quad x_4 = xyxy^{-1}, \quad x_5 = xy^2x^{-1}.$$

Define a surjective map $\pi : H \to \langle \alpha, \beta \rangle \simeq F_2$ in the following way:

$$\pi = \begin{cases} x_1 \mapsto \alpha \\ x_2 \mapsto 1 \\ x_3 \mapsto \beta \\ x_4 \mapsto \alpha^{-1} \\ x_5 \mapsto \beta^{-1} \end{cases} .$$

Observe that α and β act on H as follows:

$$\alpha = \begin{cases} x_1 = x^2 \mapsto x^2 & = x_1 \\ x_2 = yxy^{-1}x^{-1} \mapsto yxy^{-1}x^{-1} & = x_2 \\ x_3 = y^2 \mapsto yx^2yx^2 & = x_2x_4x_3x_1 \\ x_4 = xyxy^{-1} \mapsto xyxy^{-1} & = x_4 \\ x_5 = xy^2x^{-1} \mapsto xyx^2yx & = x_4x_2x_5x_1 \end{cases}$$

$$\beta = \begin{cases} x_1 = x^2 \mapsto xy^2xy^2 & = x_5x_1x_3 \\ x_2 = yxy^{-1}x^{-1} \mapsto yxy^{-1}x^{-1} & = x_2 \\ x_3 = y^2 \mapsto y^2 & = x_3 \\ x_4 = xyxy^{-1} \mapsto xy^3xy & = x_5x_4x_3 \\ x_5 = xy^2x^{-1} \mapsto xy^2x^{-1} & = x_5 \end{cases} .$$

This implies that $N = \ker(\pi)$ is generated as a normal subgroup of H by x_2, x_1x_4 and x_3x_5, and that N is invariant under the action of the automorphisms α and β. Indeed, α and β act

on N as follows:

$$\alpha = \begin{cases} x_2 & \mapsto \ x_2 \in N \\ x_1x_4 & \mapsto \ x_1x_4 \in N \\ x_3x_5 & \mapsto \ x_2x_4x_3x_1x_4x_2x_5x_1 \in N \end{cases},$$

$$\beta = \begin{cases} x_2 & \mapsto \ x_2 \in N \\ x_1x_4 & \mapsto \ x_5x_1x_3x_5x_4x_3 \in N \\ x_3x_5 & \mapsto \ x_3x_5 \in N \end{cases}.$$

Then, π induces a natural map $\mathrm{Aut}(\widehat{H}) \to \mathrm{Aut}(\widehat{\langle\alpha,\beta\rangle})$, which induces the homomorphism $\widehat{\langle\alpha,\beta\rangle} \to \mathrm{Aut}(\widehat{\langle\alpha,\beta\rangle})$. It remains to show that the latter is injective. Observe that α and β act on $\langle\alpha,\beta\rangle$ in the following way:

$$\alpha = \begin{cases} \alpha = x_1N & \mapsto \ \alpha(x_1N) = \alpha(x_1)N = x_1N = \alpha \\ \beta = x_3N & \mapsto \ \alpha(x_3N) = \alpha(x_3)N = x_2x_4x_3x_1N = \alpha^{-1}\beta\alpha \end{cases},$$

$$\beta = \begin{cases} \alpha = x_1N & \mapsto \ \beta(x_1N) = \beta(x_1)N = x_5x_1x_3N = \beta^{-1}\alpha\beta \\ \beta = x_3N & \mapsto \ \beta(x_3N) = \beta(x_3)N = x_3N = \beta \end{cases}.$$

Thus, $\widehat{\langle\alpha,\beta\rangle}$ is mapped by isomorphically to $\mathrm{Inn}(\widehat{\langle\alpha,\beta\rangle})$. It follows that $\widehat{\langle\alpha,\beta\rangle} \to \mathrm{Aut}(\widehat{\langle\alpha,\beta\rangle})$ is injective, so $\rho : \widehat{\langle\alpha,\beta\rangle} \to \mathrm{Aut}(\widehat{F}_2)$ is injective as well.

□

Lemma 3.4.3. $\mathrm{Inn}(\widehat{F}_2) \cap \mathrm{Im}\,\rho = \{e\}$.

Proof. Let $x_2 = yxy^{-1}x^{-1}$, where x and y are the generators of F_2. From the previous lemma, we know that both α and β fix x_2. Then, Proposition 3.3.7 (ii) implies that $C_{\widehat{F}_2}(x_2) = \widehat{\langle x_2\rangle}$. Therefore, we get that

$$\mathrm{Inn}(\widehat{F}_2) \cap \mathrm{Im}\,\rho \subset C_{\widehat{F}_2}(x_2) = \widehat{\langle x_2\rangle}.$$

Let $\pi : H \to \langle \alpha, \beta \rangle$ be defined as in the previous lemma. Then, since $x_2 \in \ker \pi$, the image of $\widehat{\langle x_2 \rangle}$ in $\mathrm{Inn}(\widehat{\langle \alpha, \beta \rangle})$ is trivial. It follows that the image of $\mathrm{Inn}(\widehat{F}_2) \cap \mathrm{Im}\, \rho$ in $\widehat{\langle x_2 \rangle}$ is trivial, and isomorphic to $\mathrm{Inn}(\widehat{F}_2) \cap \mathrm{Im}\, \rho$ as $\mathrm{Im}\, \rho$ is mapped isomorphically to $\mathrm{Inn}(\widehat{\langle \alpha, \beta \rangle})$. We get the desired result.

□

Chapter 4

Explicit construction of a congruence subgroup of $\mathrm{Aut}(F_2)$

Bux, Ershov and Rapinchuk revise in [5] the proof of the Main Theorem in a way that involves only finite free quotients of free groups, instead of free profinite groups. This leads to a direct procedure for constructing, for a fixed normal subgroup N of finite index in $\mathrm{Aut}(F_2)$, a normal subgroup K of finite index in F_2 such that $\Gamma[K] \subset N$. We present their proof in this chapter.

As before, F_2 denotes the free group on generators x and y, and $\mathrm{Aut}'(F_2)$ denotes the preimage of the free subgroup in $GL_2(\mathbb{Z})$ generated by

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

under the canonical homomorphism $\mathrm{Aut}(F_2) \to GL_2(\mathbb{Z})$ (refer to Section 3.4).

Lemma 4.0.1. Assume that for every finite-index normal subgroup $N \subset \mathrm{Aut}(F_2)$ with $\mathrm{Inn}(F_2) \subset N$, there exists a finite-index normal subgroup $K \subset F_2$ such that $\Gamma[K] \subset N$. Then, there exists an explicit procedure to find principal congruence subgroups for *all* finite-index normal subgroups of $\mathrm{Aut}(F_2)$.

Proof. Let N be an arbitrary finite-index normal subgroup of $\mathrm{Aut}(F_2)$, and consider the characteristic subgroup $Q \subset F_2 \simeq \mathrm{Inn}(F_2)$ corresponding to $\mathrm{Inn}(F_2) \cap N$. Pick a prime p not dividing $|F/Q|$ and define $R = Q^p\,[\,Q, Q\,]$. Then, since p does not divide $|F/Q|$, there is a semi-direct product

$$F_2/R \simeq Q/R \rtimes F_2/Q.$$

By an analog of (3.3) in Proposition 3.3.2, we have

$$Q/R \simeq \mathbb{F}_p[F_2/Q] \oplus \mathbb{F}_p$$

as (F_2/Q)-modules, where $\mathbb{F}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$. This implies that $C_{F_2/R}(Q/R) = Q/R$. Now, observe that if $\mathrm{Inn}(h) \in \Gamma[R]$ then $\mathrm{Inn}(h)$ acts on F_2/Q trivially, implying that $hR \in C_{F_2/R}(Q/R)$. Therefore, $h \in Q$.

By assumption, we can find a finite-index normal subgroup $K \subset F_2$ such that

$$\Gamma[K] \subset (N \cap \Gamma[R]) \cdot \mathrm{Inn}(F_2).$$

We claim that $\Gamma[R \cap K] \subset N$. Indeed, any $\sigma \in \Gamma[R \cap K]$ can be written as $\sigma = \tau \cdot \mathrm{Inn}(h)$ for some $\tau \in N \cap \Gamma[R]$ and some $h \in F_2$. Then, $\mathrm{Inn}(h) \in \Gamma[R]$, so $h \in Q$, which implies that $\mathrm{Inn}(h) \in \mathrm{Inn}(F_2) \cap N$. It follows that $\sigma \in N$, as required.

□

Remark 4.0.2. Consider a normal subgroup N of finite index in $\mathrm{Aut}(F_2)$. Then, by replacing N with the normal subgroup $N \cap \mathrm{Aut}'(F_2)$, whose index divides 12 $[\mathrm{Aut}(F_2) : N]$, we can assume that $N \subset \mathrm{Aut}'(F_2)$.

Theorem 4.0.3. Let N be a normal subgroup of finite index in $\mathrm{Aut}(F_2)$ such that $\mathrm{Inn}(F_2) \subset N \subset \mathrm{Aut}'(F_2)$. Let p and q be odd primes that do not divide $n := [\mathrm{Aut}'(F_2) : N]$, and let $m = n\,p^{n+1}$. Then, we can construct a normal subgroup $K \subset F_2$ of finite index dividing $144\,m^4\,q^{36m^4+1}$ such that $\Gamma[K] \subset N$.

Proof. Recall from Section 3.4 the following split exact sequence:

$$1 \to \mathrm{Inn}(F_2) \to \mathrm{Aut}'(F_2) \xrightarrow{\theta} \langle A, B\rangle \to 1 \tag{4.1}$$

It induces an isomorphism between $\mathrm{Aut}'(F_2)/\mathrm{Inn}(F_2)$ and $\langle A, B\rangle$. Let $\mathcal{N}$ denote the image of N in $\langle A, B\rangle$, and let $\mathcal{M} := \mathcal{N}^p[\mathcal{N}, \mathcal{N}]$. Now, since p does not divide $|\langle A, B\rangle/\mathcal{N}|$, it follows by Proposition 3.3.2 that

$$\text{any normal subgroup of } \langle A, B\rangle/\mathcal{M} \text{ has trivial image in } \langle A, B\rangle/\mathcal{N}. \tag{4.2}$$

Then, by (3.3), we also have $\mathcal{N}/\mathcal{M} \simeq \mathbb{F}_p[\langle A, B\rangle/\mathcal{N}] \oplus \mathbb{F}_p$, which implies that $|\langle A, B\rangle/\mathcal{M}| = m$. Then, it suffices to construct a subgroup $K \subset F_2$ of finite index dividing $144\, n^4\, q^{36m^4+1}$ that satisfies the conditions of the following lemma.

Lemma 4.0.4. If K is an $(\mathrm{Aut}'(F_2))$-invariant subgroup of F_2 such that $\Gamma[K] \subset \mathrm{Aut}'(F_2)$ and the image of $\theta(\Gamma[K])$ in $\langle A, B\rangle/\mathcal{M}$ is cyclic, then $\Gamma[K] \subset N$.

Proof. Since K is an $(\mathrm{Aut}'(F_2))$-invariant subgroup of F_2 and $\Gamma[K] \subset \mathrm{Aut}'(F_2)$, the image of $\theta(\Gamma[K])$ in $\langle A, B\rangle/\mathcal{M}$ is a normal subgroup. Then, it follows by (4.2) that $\theta(\Gamma[K])$ has trivial image in $\langle A, B\rangle/\mathcal{N}$. Hence, the image of $\Gamma[K]$ in $\mathrm{Aut}'(F_2)/\mathrm{Inn}(F_2)$ is contained in the image of $\mathcal{N}$ in $\mathrm{Aut}'(F_2)/\mathrm{Inn}(F_2)$. As $\mathrm{Inn}\, N \subset N$, we get that $\Gamma[K] \subset N$.

□

Now, let $\mathcal{L} = \mathcal{M}^q[\mathcal{M}, \mathcal{M}]$. By a similar argument as the one in Lemma 4.0.3, we get that

$$C_{\langle A,B\rangle/\mathcal{L}}(\mathcal{M}/\mathcal{L}) = \mathcal{M}/\mathcal{L},$$

and since q is odd, for any subgroup $\mathcal{G} \subset \langle A, B\rangle/\mathcal{L}$ of index ≤ 2,

$$\text{the centralizer } C_{\langle A,B\rangle/\mathcal{L}}(\mathcal{G}) \text{ has trivial image in } \langle A, B\rangle/\mathcal{M}. \tag{4.3}$$

Consider the group $\Psi = \langle\, z_1, z_2, z_3 \,|\, z_1^2 = z_2^2 = z_3^2 = e \,\rangle$. Let Θ be the kernel of the following composite homomorphism:

$$\Psi \xrightarrow{\varepsilon} \Psi^{\,\mathrm{ab}} \xrightarrow{\sigma} \mathbb{Z}/2\mathbb{Z}$$

where σ sends each z_i to 1 (mod 2). Consider the right transversal $\{1, z_1\}$ to Θ in Ψ. Then by Schreier's method (Theorem 3.3.4), it follows that Θ is generated by z_2z_1, z_3z_1, z_1z_2 and z_1z_3. Since Θ is non-abelian, it follows that it is a free group on z_1z_2 and z_2z_3.

Now, identify F_2 with Θ by letting $x = z_1z_2$ and $y = z_2z_3$, and let F_3 be the free group on $u = z_1z_2z_3$, $v = z_2z_3z_1$, $w = z_3z_1z_2$. Define the homomorphism $\varkappa_0 : \langle A, B\rangle \to \operatorname{Aut} F_3$ in the following way:

$$A \mapsto \begin{cases} z_1 \;\to\; (z_1z_2)^{-1}z_1(z_1z_2) & \\ z_2 \;\to\; (z_1z_2)^{-1}z_2(z_1z_2) & \text{restricted to } F_3 \\ z_3 \;\to\; (z_1z_2)^{-2}z_3(z_1z_2)^2 & \end{cases}$$

$$B \mapsto \begin{cases} z_1 \;\to\; z_1 & \\ z_2 \;\to\; (z_2z_3)^{-1}z_2(z_2z_3) & \text{restricted to } F_3 \\ z_3 \;\to\; (z_2z_3)^{-1}z_3(z_2z_3) & \end{cases}$$

Now, consider the surjective homomorphism $\rho : F_3 \to \langle A, B\rangle$ defined by $u \mapsto B$, $v \mapsto 1$, and $w \mapsto B^{-1}A$. Since $\ker\rho$ is invariant under $\varkappa_0(\langle A, B\rangle)$, the induced action of $\varkappa_0(w)$ for $w \in \langle A, B\rangle$ coincides with $\operatorname{Inn} w$.

Similarly to $\varkappa_0$, we can define a homomorphism $\nu_0 : \langle A, B\rangle \to \mathrm{Aut}'(F_2)$ as follows:

$$A \mapsto \alpha = \begin{cases} x \to x \\ y \to yx^2 \end{cases}$$

$$B \mapsto \beta = \begin{cases} x \to xy^2 \\ y \to y \end{cases}$$

Observe that ν_0 corresponds to $\varkappa_0$ restricted to F_2. It also corresponds to the cross-section of (4.1) (refer to the proof of Lemma 3.4.1).

Let $M = \rho^{-1}(\mathcal{M}) \cap F_2$, and $L' = \rho^{-1}(\mathcal{L})$, $L = L' \cap F_2$. By construction, M and L are normal and $\varkappa_0(\langle A, B\rangle)$-invariant, or equivalently $\nu_0(\langle A, B\rangle)$-invariant, subgroups of $F_2 \cap F_3$. Now, set

$$S = \bigcap_{g \in F_2} (gMg^{-1}),$$
$$T = S \cap {F_2}^6 [F_2, F_2],$$
$$U = T^p [T, T].$$

Lemma 4.0.5. We have:

(i) U is $(\mathrm{Aut}'(F_2))$-invariant and is contained in L;

(ii) if $h \in \langle A, B\rangle$ is such that $\nu_0(h)$ acts on F_2/U as $\mathrm{Inn}(s)$ for some $s \in \langle A, B\rangle$, then $h \in \mathcal{M}$;

(iii) $[F : U]$ divides $36m^4\, q^{36m^4+1}$.

Proof. (i) By construction, S is $\nu_0(\langle A, B\rangle)$-invariant. Then, since $\mathrm{Aut}'(F_2) \simeq \mathrm{Inn}(F_2) \rtimes \nu_0(\langle A, B\rangle)$ by (4.1), S is also $\mathrm{Aut}'(F_2)$-invariant. It follows that T and U are $\mathrm{Aut}'(F_2)$-invariant. Now, $S \subset M$ implies that $\rho(S) \subset \mathcal{M}$. We get $\rho(U) \subset \mathcal{L}$, so $U \subset L$.

(ii) Let $h \in \langle A, B\rangle$ be such that $\nu_0(h)$ acts on F_2/U as $\mathrm{Inn}(s)$ for some $s \in \langle A, B\rangle$. Since $S \subset M$, there exists $m \in \mathcal{M}$ such that $\rho(m) = s$. Let $g = hm^{-1}$. Since $U \subset L$, by (i), it follows by assumption that $\nu_0(h)$ acts on $(F_2 \cap F_3)/L'$ as $\mathrm{Inn}(s)$. Now, consider the isomorphism

$$\langle A, B\rangle/\mathcal{L} \simeq F_3/L',$$

where, for $r \in \langle A, B\rangle$, the action of $\mathrm{Inn}(r)$ agrees with the action of $\nu_0(r)$ on F_3/L'. That implies that the action of $\nu_0(m)$ on F_3/L' coincides with that of $\mathrm{Inn}(s)$, and therefore $\nu_0(g)$ acts on $(F_2 \cap F_3)L'/L'$ trivially. Observe that $(F_2 \cap F_3)L'/L'$ is a subgroup of index less or equal to 2 in F_3/L', so $\mathrm{Inn}(g)$ acts trivially on a subgroup $\mathcal{G}$ of $\langle A, B\rangle/\mathcal{L}$ having index less or equal to 2. Therefore, by (4.3), we can conclude that $g \in \mathcal{M}$, as desired.

(iii) Observe that $F_2/(F_2 \cap F_3)$ is isomorphic to the Klein group $(\mathbb{Z}/2\mathbb{Z})^2$. Then, since the normalizer $N_{F_2}(M)$ contains $F_2 \cap F_3$, $(F_2 \cap F_3)/S$ is contained into a product of at most 4 copies of $(F_2 \cap F_3)/M$. We get that $[F : S]$ divides $4m^4$. Now, observe that

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

Since $S \subset F_2 \cap F_3 = F^2[F, F]$, we get that $[F : T]$ must divide $36m^4$. Now, analog to the proof of Proposition 3.3.2, we have that

$$T/U \simeq \mathbb{F}_q[F/T] \oplus \mathbb{F}_q,$$

so $[F : U]$ divides $36m^4\, q^{36m^4+1}$, as desired.

□

We claim that

$$K = U \cap K_0$$

satisfies all the conditions of Lemma 4.0.4, where $K_0 = {F_2}^4[F_2, F_2]$. Since $U \subset F_2 \cap F_3$, it follows that $[F_2 : K]$ divides $4 \cdot 36m^4\, q^{36m^4+1}$.

Clearly, K is a $(\mathrm{Aut}'(F_2))$-invariant subgroup of F_2. It is well known that $\langle A, B\rangle \subset SL_2(\mathbb{Z})$ contains $SL_2(\mathbb{Z}/4\mathbb{Z})$, which coincides with $\theta(\Gamma[K_0])$ (c.f. Example 2.3.5). We have $\Gamma[K_0] \subset \mathrm{Aut}'(F_2)$, which implies $\Gamma[K] \subset \mathrm{Aut}'(F_2)$. It remains to show that the image of $\theta(\Gamma[K])$ in $\langle A, B\rangle / \mathcal{M}$ is cyclic.

Take $\sigma \in \Gamma[K]$. Since $\mathrm{Aut}(F_2) = \mathrm{Inn}(F_2) \rtimes v_0(\langle A, B\rangle)$, we have $\sigma = \mathrm{Inn}(g) \cdot v_0(h)$ for some $g \in F_2$, and $h \in \langle A, B\rangle$. σ acts trivially on F_2/K, hence $v_0(h)$ coincides with $\mathrm{Inn}\, g^{-1}$. It also fixes $[x, y]$, so we can deduce by Proposition 3.3.2 that $g \in \langle c\rangle \langle A, B\rangle$.

Let W be a subgroup of $\mathrm{Aut}(F_2/K)$ induced by $\mathrm{Inn}\, s$, for some $s \in \langle A, B\rangle$. Define Ω as the preimage of W under $\langle A, B\rangle \xrightarrow{v_0} \mathrm{Aut}'(F_2) \to \mathrm{Aut}(F_2/K)$.

$\Gamma[K] \cap (\mathrm{Inn}(F_2) \rtimes v_o(\Omega))$ is then cyclic, so by Lemma 4.0.5, $\theta(\Gamma[K] \cap (\mathrm{Inn}(F_2) \rtimes v_o(\Omega)))$ is cyclic in $\langle A, B\rangle / \mathcal{M}$. This implies that the image of $\theta(\Gamma[K])$ is cyclic. Then, by Lemma 4.0.4, $\Gamma[K] \subset N$, as desired.

□

Remark 4.0.6. In [4], Ben-Ezra and Lubotzky give a simpler explicit construction of a congruence subgroup with a better bound for the index of K. Indeed, for a finite-index normal subgroup $N \subset \mathrm{Aut}(F_2)$ under the same conditions as in Theorem 4.0.3, they are able to construct a normal subgroup $K \subset F_2$ of finite index dividing $144n^4\, p^{36n^4+1}$ such that $\Gamma[K] \subset N$.

Remark 4.0.7. In [3], Ben-Ezra showed that, although a large part of Bux, Ershov and Rapinchuk's proof worked for the free metabelian group on two generators Φ_2, this group does not have the congruence subgroup property. This case is of interest in this context since we can interpret Φ_2 as an intermediate group between the free abelian group $\mathbb{Z}^2$ and the free group F_2.

Bibliography

[1] Mamoru Asada. The faithfulness of the monodromy representations associated with certain families of algebraic curves. *Journal of Pure and Applied Algebra*, 159(2-3):123–147, 2001.

[2] Hyman Bass, Michel Lazard, and Jean-Pierre Serre. Sous-groupes d'indice fini dans $SL(n, \mathbb{Z})$. *Bulletin of the American mathematical society*, 70(3):385–392, 1964.

[3] David El-Chai Ben-Ezra. The congruence subgroup problem for the free metabelian group on two generators. *arXiv preprint arXiv:1312.3480*, 2013.

[4] David El-Chai Ben-Ezra and Alexander Lubotzky. The congruence subgroup problem for low rank free and free metabelian groups. *Journal of Algebra*, 500:171–192, 2018.

[5] Kai-Uwe Bux, Mikhail Ershov, and Andrei Rapinchuk. The congruence subgroup property for $\mathrm{Aut}(F_2)$: A group-theoretic proof of Asada's theorem. *arXiv preprint arXiv:0909.0304*, 2009.

[6] Karl W Gruenberg. *Cohomological topics in group theory*, volume 143. Springer, 2006.

[7] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory: Presentations of groups in terms of generators and relations*. Courier Corporation, 2004.

[8] Nikolay Nikolov, Dan Segal, and Nikolay Nikolav. On finitely generated profinite groups, i: strong completeness and uniform bounds. *Annals of mathematics*, pages 171–238, 2007.

[9] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Springer, 2000.

[10] B Sury. *The Congruence Subgroup Problem: An Elementary Approach Aimed at Applications*. Number 24. Hindustan Book Agency and Indian National Science Academy, 2003.