Metabelian groups and elliptic curves

William Chen, Pierre Deligne

December 21, 2022

Abstract

In this paper we study 2-generated profinite metabelian groups from the perspective of arithmetic geometry and group theory. Motivated by the results and conjectures of Chen [Che18], we show that if $\mathcal{M}(1)_K$ denotes the moduli stack of elliptic curves over a number field K, then for any elliptic curve E/K with origin O and $x \in E - O$, the monodromy image of the arithmetic fundamental group $\pi_1(\mathcal{M}(1)_K, E_{\overline{\mathbb{Q}}})$ on the maximal pro-metabelian quotient of $\pi_1^{ét}(E_{\overline{\mathbb{Q}}} - O, x)$ maps isomorphically onto its monodromy image on $\pi_1^{ét}(E_{\overline{\mathbb{Q}}}) \cong \prod_\ell T_\ell(E)$. In particular, for any finite 2-generated metabelian group G, the moduli space $M(G)$ of elliptic curves with G-covers only ramified above the origin is a disjoint union of congruence modular curves. Our methods are mostly group theoretic – we study the outer automorphism group of the rank 2 free pro-metabelian group M, and introduce the use of Koszul homology in the study of 2-generated profinite metabelian groups G. This homology group controls the extent to which generating pairs of G are determined up to conjugation by their abelianizations together with their commutators, and yields bounds for the congruence level of components of $M(G)$.

Contents

The author's research was partly supported by National Science Foundation Award No. DMS-1803357, as well as the Minerva Research Foundation at the Institute for Advanced Study.

1 Introduction

1.1 Motivation and geometric results

In this paper we study 2-generated[1] finite metabelian groups G from the perspective of group theory and arithmetic geometry. Group theoretically, we are interested in understanding Nielsen equivalence classes of generating pairs of G, or equivalently the action of $\operatorname{Out}(\Pi)$ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi,G) := \mathrm{Epi}(\Pi,G)/\operatorname{Inn}(G)$, where Π denotes a free group of rank 2. Geometrically, we wish to understand the moduli stack $\mathcal{M}(G)$ (over $\mathbb{Q}$) of elliptic curves with G-structures[2] (or "Teichmüller structures of level G") in the sense of [Che18, DM69, PdJ95]. The connection between the two perspectives is provided by the Galois correspondence: $\mathcal{M}(G)$ is finite étale over the moduli stack of elliptic curves $\mathcal{M}(1)$ (over $\mathbb{Q}$), and fixing an elliptic curve $E/\mathbb{Q}$, the monodromy action of $\pi_1^{\acute{e}t}(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E_{\overline{\mathbb{Q}}})$ on a geometric fiber of the map $\mathcal{M}(G) \to \mathcal{M}(1)$ can be identified with the action of the profinite completion of $\operatorname{Out}^+(\Pi)$ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi,G)$, where $\operatorname{Out}^+(\Pi) \le \operatorname{Out}(\Pi)$ is the index 2 subgroup acting with determinant 1 on the abelianization $\Pi^{\mathrm{ab}} \cong \mathbb{Z}^2$. Here, if $O \in E$ denotes the origin and $E^\circ := E - O$, then Π is to be viewed as the topological fundamental group of the punctured torus $E^\circ(\mathbb{C})$.

By a classical theorem of Nielsen, a choice of basis for Π defines an isomorphism $\operatorname{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$. In [Che18], the first author used this to show that the quotient of the upper half plane $\mathcal{H}$ by any finite index, possibly noncongruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (hereafter called a *modular curve*) is a moduli space for elliptic curves equipped with "G-structures", for an appropriate finite group G. When G is abelian, the action of $\operatorname{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi,G) = \mathrm{Epi}(\mathbb{Z}^2,G)$ is induced by the canonical action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Z}^2$; in this case, G-structures are equivalent to classical congruence structures associated to the congruence subgroups $\Gamma(n), \Gamma_1(n), \ldots$etc, and accordingly the resulting moduli stacks $\mathcal{M}(G)_{\mathbb{C}}$ are disjoint unions of the classical congruence (stacky) modular curves $[\mathcal{H}/\Gamma(n)], [\mathcal{H}/\Gamma_1(n)], \ldots$etc. From this perspective, it is natural to ask:

> For which finite groups G are the components of $\mathcal{M}(G)$ congruence modular curves?

This question can be taken either geometrically, where one asks when the components of $\mathcal{M}(G)_{\mathbb{C}}$ are isomorphic to congruence modular curves, or arithmetically, where we require the isomorphism to respect the $\mathbb{Q}$-structure. Taken geometrically, it is equivalent to asking: when do the stabilizers of $\operatorname{Out}^+(\Pi) \circlearrowright \mathrm{Epi}^{\mathrm{ext}}(\Pi,G)$ correspond to

[1] By this we mean that the group can be generated by two elements.

[2] If k is an algebraically closed field of characteristic not dividing $|G|$, then a G-structure on an elliptic curve E/k is the same as a G-Galois cover $C \to E$, only branched over the origin, together with an isomorphism $\mathrm{Gal}(C/E) \xrightarrow{\sim} G$.

congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ via the isomorphism $\mathrm{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$? In the arithmetic form, this question can also be understood as asking: for an elliptic curve $E/\mathbb{Q}$ with origin O, $E^\circ := E - O$, and $x \in E^\circ(\overline{\mathbb{Q}})$,

> How much does the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cohomology of E tell us about its action on the fundamental group $\widehat{\Pi} := \pi_1^{\acute{e}t}(E^\circ_{\overline{\mathbb{Q}}}, x)$? (1)

We note that by the Grothendieck conjecture for affine hyperbolic curves [Tam97], the Galois action on $\pi_1^{\acute{e}t}(E^\circ, x)$ is enough to determine E° up to isomorphism, whereas the Galois action on cohomology is in general only enough to determine it up to isogeny.

The general philosophy, which is to a degree supported by computational data [Che18, Appendix B], is that the property of $\mathcal{M}(G)$ having congruence components should be related to G being in some sense "close to abelian". For example, in [Che18, Theorem 4.2.2], the first author shows that for dihedral groups, $\mathcal{M}(D_{2n})_{\overline{\mathbb{Q}}}$ is a disjoint union of congruence modular curves. In general, the problem seems to be remarkably subtle – for example, in a future work, we will show that there exist infinitely many nonabelian finite simple groups G such that $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ has a congruence component, which disproves a conjecture of the first author [Che18, Conjecture 4.4.1]. In this paper we will prove the "positive" result that for metabelian G, the components of $\mathcal{M}(G)$ are congruence in the strong arithmetic sense. For example, we will show

Theorem A (See 6.4)**.** *Let G be a 2-generated finite metabelian group of exponent e. Let e' be the exponent of the derived subgroup $G' = [G, G]$. Then the connected components of $\mathcal{M}(G)_{\mathbb{Q}}$ are all isomorphic, and every component is a quotient of $\mathcal{M}((\mathbb{Z}/ee')^2)_{\mathbb{Q}}$ by a subgroup of $\mathrm{GL}_2(\mathbb{Z}/ee')$.*

Here, we note that $\mathcal{M}((\mathbb{Z}/n)^2)_{\mathbb{Q}}$ is connected but not geometrically connected - upon base changing to $\mathbb{C}$ it is a disjoint union of $\phi(n)$ copies of the congruence modular stack $[\mathcal{H}/\Gamma(n)]$, where ϕ denotes the Euler totient function. Thus in the situation of the theorem we say that $\mathcal{M}(G)_{\mathbb{Q}}$ has *arithmetic congruence level* dividing ee'. Over $\mathbb{C}$, we are able to get a somewhat better bound for the congruence level:

Theorem B (See 6.10)**.** *Let $G^{\mathrm{ab}} := G/G'$ denote the abelianization, and let $n := \gcd(e, |G^{\mathrm{ab}}|)$. Then every component of $\mathcal{M}(G)_{\mathbb{C}}$ is isomorphic to the stack quotient of the upper half plane by a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level dividing n.*

The fact that the components of $\mathcal{M}(G)_{\mathbb{C}}$ are all congruence also allows us to recover a result of Ben-Ezra and Lubotzky [BEL17], that the automorphism group of a discrete rank 2 free metabelian group does not have the congruence subgroup property.

The proofs of the theorems above involve an analysis of the monodromy action of Γ on the set $\mathrm{Epi}^{\mathrm{ext}}(\widehat{\Pi}, G)$. This action is defined using the outer representation $\rho_{E^\circ/\mathbb{Q}} : \Gamma \longrightarrow \mathrm{Out}(\widehat{\Pi})$ associated to the universal family of elliptic curves over $\mathcal{M}(1)_{\mathbb{Q}}$. Since $\Gamma \cong \overline{\Gamma} \rtimes \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we must understand the topological monodromy action of $\overline{\Gamma}$ and the arithmetic monodromy action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Epi}^{\mathrm{ext}}(\widehat{\Pi}, G)$. Because G is metabelian, any surjection $\widehat{\Pi} \to G$ factors through the maximal pro-metabelian quotient, denoted $M := \widehat{\Pi}^{\mathrm{meta}}$, so it suffices to understand the outer actions of $\overline{\Gamma}$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the rank 2 free metabelian group M and the set $\mathrm{Epi}^{\mathrm{ext}}(M, G)$. Let $A := \widehat{\Pi}^{\mathrm{ab}} = M^{\mathrm{ab}}$ denote the abelianization of $\widehat{\Pi}$, and let $\mathrm{IOut}(M) := \mathrm{Ker}(\mathrm{Out}(M) \to \mathrm{Aut}(M))$. We have an exact sequence

$$1 \longrightarrow \mathrm{IOut}(M) \longrightarrow \mathrm{Out}(M) \xrightarrow{\mathrm{ab}_*} \underbrace{\mathrm{Aut}(A)}_{\cong \mathrm{GL}_2(\widehat{\mathbb{Z}})} \longrightarrow 1 \tag{2}$$

Theorem C (See 3.22, 6.1)**.** *The monodromy image of $\Gamma \cong \overline{\Gamma} \rtimes \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inside $\mathrm{Out}(M)$ maps isomorphically (via ab_*) onto $\mathrm{Aut}(A) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$. In particular, the sequence (2) is split.*

To prove this, we first note that the monodromy image of Γ inside $\mathrm{Out}(M)$ surjects onto $\mathrm{Aut}(A)$ and satisfies a certain compatibility relation between its actions on M' and A – if x_1, x_2 generate M, then its action on M' is determined by its action on the commutator $[x_1, x_2]$, on which it acts by exponentiating to the power of the cyclotomic character[3] $\chi : \Gamma \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times$, and on A its determinant is also given by χ. Outer

[3] This is because $[x_1, x_2]$ generates an inertia subgroup of $M \cong \pi_1^{\acute{e}t}(E^\circ_{\overline{\mathbb{Q}}}, x)^{\mathrm{meta}}$.

automorphisms satisfying such a compatibility relation will be called "inertia-preserving". Second, we show that the subgroup of inertia-preserving outer automorphisms map isomorphically onto $\mathrm{Aut}(A)$ (3.22). From this it follows that the monodromy image of Γ coincides with the subgroup of inertia-preserving outer automorphisms, as desired. Theorem C generalizes a result of Davis [Dav13].

Since $A = \widehat{\Pi}^{\mathrm{ab}}$ is canonically isomorphic to the fundamental group of the unpunctured elliptic curve E, and hence is the product of the ℓ-adic Tate modules $T_\ell(E)$ (over all primes ℓ), one consequence of the theorem is that the monodromy image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on $\prod_\ell T_\ell(E)$ is isomorphic to its image acting on $M = \pi_1^{\acute{e}t}(E^\circ_{\overline{\mathbb{Q}}}, x)^{\mathrm{meta}}$. In other words, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cohomology of E in some sense tells you everything about its action on the pro-metabelian fundamental group of $E^\circ_{\overline{\mathbb{Q}}}$. The splitting also implies that the components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ are all congruence, though it gives no control on the congruence level.

1.2 Rigidity, Koszul homology, and congruence level bounds

Let G be a profinite 2-generated metabelian group with derived subgroup G' and abelianization $\mathrm{ab} : G \to G^{\mathrm{ab}} := G/G'$. Note that G' admits a canonical structure as a module under the completed group algebra $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$, where the G^{ab}-action is given by the exact sequence $1 \to G' \to G \to G^{\mathrm{ab}} \to 1$. Because G is 2-generated, this module is moreover *cyclic*. Recall that M is a free profinite metabelian group of rank 2, and $A = M^{\mathrm{ab}}$.

A central technical question that we address in the paper is:

> Suppose $(g_1, g_2), (g_1', g_2')$ are two generating pairs for G whose images in G^{ab} agree and such that the commutator $[g_1, g_2]$ is conjugate to $[g_1', g_2']$. Must $(g_1, g_2), (g_1', g_2')$ be (simultaneously) conjugate? (3)

A group G for which the question has a positive answer will be called *rigid*. The usefulness of this notion lies in the fact that if $x_1, x_2 \in M$ are generators, then for rigid G, the action of Γ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G) = \mathrm{Epi}^{\mathrm{ext}}(M, G)$ is determined by its action on $[x_1, x_2]$ (where it acts via χ) and on A (which lies in the realm of the classical theory of Galois representations associated to elliptic curves [Ser89]). Thus for rigid G, arithmetic and geometric properties of $\mathcal{M}(G)$ are easily deduced from properties of $\mathcal{M}(G^{\mathrm{ab}})$. To be precise, let $\mathrm{Gens}(G')$ denote the set of $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module generators of G'. Fix generators x_1, x_2 of Π, and consider the map

$$\xi \times \kappa : \mathrm{Epi}^{\mathrm{ext}}(\Pi, G) = \mathrm{Epi}^{\mathrm{ext}}(M, G) \longrightarrow \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$$

sending $\varphi \mapsto (\mathrm{ab} \circ \varphi, \varphi([x_1, x_2])$.[4] Then, for example, we have

Theorem D (See 6.8)**.** *If G is rigid, then the map $\xi \times \kappa$ is a* bijection. *Geometrically, if G is finite then there is an integer m such that the components of $\mathcal{M}(G)_{\mathbb{Q}(\zeta_m)}$ are geometrically connected, and the restriction of the canonical map $\mathcal{M}(G)_{\mathbb{Q}(\zeta_m)} \to \mathcal{M}(G^{\mathrm{ab}})_{\mathbb{Q}(\zeta_m)}$ to any connected component is an isomorphism. Here we can take m to be the least common multiple of the exponent of G' and the order of the exterior square $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$.*

In general, we will show that the obstructions to rigidity lie in the group $\mathrm{IOut}_1(G)$ of outer automorphisms of G which act trivially on both G' and G^{ab} (up to conjugation). More precisely, the group $\mathrm{IOut}_1(G)$ acts freely and transitively on the fibers of $\xi \times \kappa$, and is a quotient of the homology group $H_1(A, G')$ where the A-module structure on G' is given by *any* surjection $A \to G^{\mathrm{ab}}$ (see §4.3, §4.4). We will call G *strictly rigid* if $H_1(A, G') = 0$.[5] The regularity of the action of $\mathrm{IOut}_1(G)$ on the fibers of $\xi \times \kappa_c$ comes from the very useful property that IA-endomorphisms of M preserve all closed normal subgroups, and hence descend to every quotient[6] (3.6). This is also responsible for the fact that the components of $\mathcal{M}(G)$ are all isomorphic.

An important calculation is that M' is a free $\widehat{\mathbb{Z}}[\![A]\!]$-module of rank 1 (3.10), and that $H_1(A, M') = 0$ (4.17), so M is strictly rigid. Since $H_1(A, \cdot)$ does preserve epimorphisms in general, this does not imply rigidity for all 2-generated profinite metabelian groups G. However, it does imply that all components of $\mathcal{M}(G)_{\mathbb{C}}$ are

[4] We will define ξ, κ individually in §4.2.

[5] There is also an interpretation of $H_i(A, G')$: $H_0(A, G')$ is the module of coinvariants $G'_{G^{\mathrm{ab}}}$, $H_2(A, G') \cong G' \cap Z(G)$, and $H_i(A, G') = 0$ for $i \notin \{0, 1, 2\}$ (Theorem 4.17).

[6] This comes from the observation that M' is a *cyclic* $\widehat{\mathbb{Z}}[\![A]\!]$-module and hence any $\widehat{\mathbb{Z}}[\![A]\!]$-linear endomorphism of M' descends to every quotient. In particular, the fact that G is 2-generated is crucial.

congruence, and is a key ingredient to the proof of the semidirect product decomposition of $\mathrm{Out}(M)$ (Theorem C). The calculation amounts to showing that if a_1, a_2 are generators of A, then the elements $a_1 - 1, a_2 - 1$ in the completed group algebra $\widehat{\mathbb{Z}}[\![A]\!]$ form a regular sequence in the sense of commutative algebra. This implies that the Koszul complex[7]

$$0 \longrightarrow M' \xrightarrow{d_2} M' \times M' \xrightarrow{d_1} M' \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0$$

associated to $a_1 - 1, a_2 - 1 \in \widehat{\mathbb{Z}}[\![A]\!]$ is a *free* $\widehat{\mathbb{Z}}[\![A]\!]$*-module resolution* of $\widehat{\mathbb{Z}}$, so $H_i(A, M') = 0$ for all i. Viewing G' as a $\widehat{\mathbb{Z}}[\![A]\!]$-module quotient of M', this allows us to calculate $H_i(A, G')$ as the homology of the complex $G' \overset{d_2}{\to} G' \times G' \overset{d_1}{\to} G'$, or equivalently as the group $\mathrm{Tor}_i^{\widehat{\mathbb{Z}}[\![A]\!]}(\widehat{\mathbb{Z}}, G')$. An immediate consequence of this theory is that $H_1(A, G')$ is a subquotient of $(G'_{G^{\mathrm{ab}}})^2$, and $G'_{G^{\mathrm{ab}}}$ is a quotient of the procyclic group $G^{\mathrm{ab}} \mathbin{\widehat{\wedge}} G^{\mathrm{ab}}$, where $\widehat{\wedge}$ denotes the completed exterior product. In particular, $\mathrm{IOut}_1(G)$ is controlled by all of these groups, which immediately yields a simple "Schur-Zassenhaus"-style criterion for rigidity:

Theorem E (See 4.27)**.** *Let G be a finite 2-generated metabelian group. If the orders of $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$ and $G'_{G^{\mathrm{ab}}}$ are coprime, then G is strictly rigid. In particular, if G^{ab} is cyclic or $G'_{G^{\mathrm{ab}}} = 0$, then G is strictly rigid.*[8]

In §4.7 we will compute $H_1(A, G'), \mathrm{IOut}_1(G)$ for various families of 2-generated finite metabelian groups.

Our main use of this homological theory is to obtain bounds on the congruence level of components of $\mathcal{M}(G)$. The arithmetic congruence level bound in Theorem A involves constructing a family of groups $M_{n,m}$ (for $n, m \geq 1$) such that every 2-generated finite metabelian group is a quotient of some $M_{n,m}$, and such that there is a map $M_{nm,m} \to M_{n,m}$ which induces the zero map on first homology. While $M_{n,m}$ is generally not rigid (see Example 4.30), inducing the 0 map on homology implies a weaker version of rigidity: if $(g_1, g_2), (g_1', g_2')$ are generating pairs which can be lifted to generating pairs of $M_{nm,m}$ which have the same images in $M^{\mathrm{ab}}_{nm,m}$ and conjugate commutators in $M'_{nm,m}$, then they are conjugate in $M_{n,m}$. This weaker version of rigidity is the essence of the arithmetic congruence level bound in Theorem A. We view this method as bounding $\mathcal{M}(G)$ *from above.*

We will also bound $\mathcal{M}(G)$ *from below* - that is, we bound the degree of the canonical (surjective) map $\mathcal{M}(G) \to \mathcal{M}(G^{\mathrm{ab}})$ induced by abelianization $G \to G^{\mathrm{ab}}$. In §6.2.2, we show that this map is Galois with Galois group isomorphic to a subgroup of $\mathrm{IOut}_1(G)$; in particular, it is abelian. Because congruence modular curves have relatively few congruence abelian covers, this puts additional restrictions on the congruence level of the components of $\mathcal{M}(G)_{\mathbb{C}}$. These considerations lead to the congruence level bound in Theorem B.

1.3 Future directions and related work

For nonrigid G, our methods say little about the problem of classifying the components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ (or equivalently the orbits of $\mathrm{Out}^+(\Pi)$ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$). If $\Sigma_{g,n}$ denotes the fundamental group of an n-punctured surface of genus g with fundamental group $\Pi_{g,n}$ (so $\Pi = \Pi_{1,1}$ and $\mathrm{Out}^+(\Pi)$ is isomorphic to the mapping class group $\mathrm{MCG}(\Sigma_{1,1})$), then this question can be viewed as classifying the connected components of Hurwitz spaces of G-covers of genus g curves, only ramified above n points. If one fixes G and allows g (resp. n) to be large, then there are a number of results which describe the connected components (equivalently $\mathrm{MCG}(\Sigma_{g,n})$-orbits on $\mathrm{Epi}^{\mathrm{ext}}(\Pi_{g,n}, G)$, going by the name of *genus stabilization* (see [DT06, §6] or [CLP16]) (resp. *branch stabilization* see [FV91, Appendix], [Lön20], [EVW16, Theorem 6.1], [LWZB19, Corollary 12.5]). The case where (g, n) are fixed and small (e.g. $(g, n) = (1, 1)$) seems to be more mysterious. In [Che18], the first author made some progress towards this problem in the case $G = \mathrm{SL}_2(\mathbb{F}_p)$, and applied the result to a conjecture of Bourgain, Gamburd, and Sarnak concerning the Diophantine geometry of the Markoff surface; however, the methods there are better suited to highly nonabelian groups, and seem to give little information for metabelian G.

Here we briefly describe a potential picture for the classification problem. Fix generators $x_1, x_2 \in \Pi$. For $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$, write φ^{ab} for the composition $\mathrm{ab} \circ \varphi : \Pi \to G^{\mathrm{ab}}$. The action of $\mathrm{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$ preserves the element $\varphi^{\mathrm{ab}}(x_1) \wedge \varphi^{\mathrm{ab}}(x_2)$ in the cyclic group $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$. As noted in §1.2 above, the action of $\mathrm{Out}^+(\Pi)$ also preserves the conjugacy class of $\varphi([x_1, x_2]) \in G$. In general, these two invariants together are not enough to classify the $\mathrm{Out}^+(\Pi)$-orbits on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$ – example, D_8 has two components even though there is only

[7] Here $d_2(r) = ((a_1 - 1)r, (a_2 - 1)r)$, and $d_1(r_1, r_2) = (1 - a_2)r_1 + (a_1 - 1)r_2$.

[8] This also holds for profinite G, if one uses the completed exterior square and the appropriate notion of "coprime orders" [RZ10, §2.3].

one choice for both invariants. However the two invariants can be simultaneously refined into a single invariant, namely the equivalence class of $\varphi(x_1) \wedge \varphi(x_2)$ in the *nonabelian exterior square* $G \wedge G$ [McD98], the equivalence relation being the one induced by conjugation in G. If $\tilde{G} \to G$ denotes a Schur cover, then this can also be identified with the class of $[\widetilde{\varphi(x_1)}, \widetilde{\varphi(x_2)}]$, where $\widetilde{\varphi(x_i)}$ denotes any lift of $\varphi(x_i)$ to $\tilde{G}$ (the commutator is independent of the choice of lift since $\tilde{G} \to G$ is a central extension). One can check that this refined invariant separates the orbits on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, D_8)$, and by computer search one can check that it also separates the orbits for all finite 2-generated metabelian groups of order ≤ 150. It is natural to ask:

Question 1.1. *For a finite 2-generated metabelian group, are the* $\mathrm{Out}^+(\Pi)$*-orbits on* $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$ *classified by the class of* $\varphi(x_1) \wedge \varphi(x_2) \in G \wedge G$*?*

1.4 Overview of the paper

Sections §3-§4 are entirely group-theoretic. Algebraic geometry does not enter until §5-6.

In §3 we prove some basic results on 2-generated metabelian groups. We define the canonical representation, determinant, and IA-endomorphisms. The first key result is that IA-endomorphisms are normal (Corollary 3.6), a result which will be used repeatedly in the rest of the paper. Next, we study the rank 2 free profinite metabelian group M; we show that its derived subgroup M' is a free $\widehat{\mathbb{Z}}[\![A]\!]$-module of rank 1 (3.10), that its IA outer automorphisms are totally characterized by the determinant (3.17), and the semidirect product decomposition of $\mathrm{Out}(M)$ (3.22).

In §4 we initiate a group-theoretic study of $\mathrm{Epi}(M, G)$, its quotient by $\mathrm{Inn}'(G)$ (the subgroup of $\mathrm{Inn}(G)$ defined by conjugation by elements of G'), and finally $\mathrm{Epi}^{\mathrm{ext}}(M, G) := \mathrm{Epi}(M, G)/\operatorname{Inn}(G)$. In each case we study the fibers of the map to $\mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$. It is a consequence of the normality of IA-endomorphisms of M that the map $\xi \times \kappa : \mathrm{Epi}(M, G)/\operatorname{Inn}'(G) \to \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$ is a torsor under the group $\mathrm{IOut}_1'(G) := \mathrm{IAut}_1(G)/\operatorname{Inn}'(G)$, where $\mathrm{IAut}_1(G)$ is the subgroup of IA-automorphisms of G which act trivially on G'. In §4.4 we identify $\mathrm{IOut}_1'(G)$ with the group homology $H_1(A, G')$, where A acts on G' via *any* surjection $A \to G^{\mathrm{ab}}$. In §4.7, we define the notion of *rigidity*, prove Theorem E, and calculate $H_1(A, G') \cong \mathrm{IOut}_1'(G)$ and $\mathrm{IOut}_1(G)$ for various families of metabelian groups.

In §5 we review the theory of the moduli stacks $\mathcal{M}(G)$, and how Galois theory connects the structure of $\mathcal{M}(G)$ with that of $\mathrm{Epi}^{\mathrm{ext}}(M, G)$. In §5.5 we give a summary of the notation that will be used in the following section to translate our group-theoretic results into statements regarding $\mathcal{M}(G)$. In §6, we bring everything together to prove Theorems A, B, C, D.

2 Conventions on profinite groups

When discussing profinite groups, rings, or monoids, all homomorphisms and cocycles will be by default assumed continuous and subgroups are assumed closed. In particular, for profinite objects, finite generation means topological finite generation, and commutator subgroup means the closure of the discrete commutator subgroup.

Usually profinite groups (including finite groups) will be denoted using Roman letters $G, M, A, \ldots$, whereas infinite discrete groups will generally be denoted by bold letters $\mathbf{G}, \mathbf{M}, \mathbf{A}, \ldots$.

3 Preliminaries on 2-generated metabelian groups

3.1 Canonical representations, determinants, and IA-endomorphisms

Let G be a metabelian group, with abelianization G^{ab} and derived subgroup G'. In this section, we describe the situation when G is a (discrete) group. Similar results hold for profinite G, mutatis mutandis: homomorphisms and cocycles are continuous, subgroups are closed (as in §2), and group algebras should be replaced by completed group algebras – if G is a profinite group, limit of G_α, then its complete group algebra $\widehat{\mathbb{Z}}[\![G]\!]$ is the limit of $(\mathbb{Z}/n)[G_\alpha]$. See [RZ10, §5.3].

We have an exact sequence

$$1 \longrightarrow G' \longrightarrow G \longrightarrow G^{\mathrm{ab}} \longrightarrow 1 \tag{4}$$

Since the inner action of G on G' restricts to the trivial action of G' on itself, the action factors through G^{ab}, and turns G' into a module over the group algebra $\mathbb{Z}[G^{\mathrm{ab}}]$.

Definition 3.1. The *canonical representation* of G is the action $\rho_G : G^{\mathrm{ab}} \to \mathrm{Aut}(G')$ induced by the inner action of G. The *canonical module* of G is the G^{ab}-module G'.

Now suppose G is 2-generated, with generators x_1, x_2. Let a_1, a_2 be their images in G^{ab} and $c := [x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$. If c vanishes, then G is abelian. The normal subgroup generated by c is generated as a subgroup by the G^{ab}-orbit of c; it is also the $\mathbb{Z}[G^{\mathrm{ab}}]$-module generated by c. The quotient is abelian, and hence we have

Proposition 3.2. *Let G be a metabelian group generated by x_1, x_2 with commutator c. Then the commutator subgroup G' is generated as a $\mathbb{Z}[G^{\mathrm{ab}}]$-module by c.*

Let R_G be the quotient of $\mathbb{Z}[G^{\mathrm{ab}}]$ by the annihilator ideal of c.

Notation. For $r \in \mathbb{Z}[G^{\mathrm{ab}}]$ and $z \in G'$, if we use multiplicative notation for G', then we will write z^r (or $\exp_z(r)$) for the image of z under the action of r. Sometimes we will use additive notation for G', in which case we will write $r \cdot z$ (or just rz). The former multiplicative notation will be the default – we will always explicitly note when we switch to additive notation. Despite the notation, we will always view G' as a left $\mathbb{Z}[G^{\mathrm{ab}}]$-module. Thus, if $g \in G$ has image $\overline{g} \in G^{\mathrm{ab}}$, beware that:

$$z^{\overline{g}} = gzg^{-1} \qquad \text{(or } \overline{g} \cdot z = gzg^{-1} \text{ in additive notation).}$$

For c as above, the map $\mathbb{Z}[G^{\mathrm{ab}}] \to G'$ sending $r \mapsto c^r$ factors through an isomorphism $\exp_c : R_G \xrightarrow{\sim} G'$. The inverse will be denoted $\log_c : G' \cong R_G$. The abelianization exact sequence (4) becomes

$$1 \longrightarrow (R_G, +) \xrightarrow{\exp_c} G \longrightarrow G^{\mathrm{ab}} \longrightarrow 1$$

An IA-endomorphism of G is an endomorphism which induces the identity on G^{ab}. Let $\mathrm{IAEnd}(G)$ (resp. $\mathrm{IAut}(G)$) denote the monoid (resp. group) of IA-endomorphisms (resp. IA-automorphisms) of G. If G is a 2-generated metabelian group and $\gamma \in \mathrm{IAEnd}(G)$, then γ acts G^{ab}-linearly on $R_G \cong G'$. Because $R_G \cong G'$ is a cyclic $\mathbb{Z}[G^{\mathrm{ab}}]$-module, it follows that γ acts by multiplication by an element of R_G.

Definition 3.3. For $\gamma \in \mathrm{IAEnd}(G)$, the *determinant* of γ is the unique element $\det(\gamma) \in R_G$ such that γ acts on G' by multiplication by $\det(\gamma)$. In a formula, we have

$$\gamma(z) = z^{\det(\gamma)} \qquad \text{for all } z \in G'$$

If $c \in G'$ is a R_G-basis, and $\alpha \in \mathrm{End}(G)$ any endomorphism, define

$$\det_c(\alpha) := \log_c(\alpha(c))$$

Note that $\det_c|_{\mathrm{IAEnd}(G)}$ coincides with det. However $\det_c$ is not multiplicative on $\mathrm{End}(G)$:

Proposition 3.4. *The map $\det_c : \mathrm{End}(G) \to R_G$ is a crossed monoid homomorphism, continuous if G is profinite. That is,*

$$\det_c(\gamma \circ \gamma') = \det_c(\gamma)\, {}^{\gamma}\det_c(\gamma') \qquad \textit{for all } \gamma, \gamma' \in \mathrm{End}(G) \tag{5}$$

Proof. If G is discrete, this follows from the identity

$$\gamma(\gamma'(c)) = \gamma(c^{\det_c(\gamma')}) = c^{\det_c(\gamma)\, {}^{\gamma}\det_c(\gamma')}. \tag{6}$$

If G is profinite, then by our conventions R_G is a quotient of $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$. Let $\mathbf{R}_G$ be the image of the discrete group algebra $\mathbb{Z}[G^{\mathrm{ab}}]$ in R_G. Then $\mathbf{R}_G$ is a dense subalgebra of R_G. The relation (5) follows from (6) if $\det_c(\gamma')$ lies in $\mathbf{R}_G$. The general case follows by writing $\det_c(\gamma')$ as a limit of elements of $\mathbf{R}_G$. □

The group of 1-cocycles $Z^1(G, G')$ consists of the functions $\delta : G \to G'$ satisfying

$$\delta(gh) = \delta(g)\delta(h)^g \quad \text{for all } g \in G$$

where as per our notation, $\delta(h)^g = g\delta(h)g^{-1}$. If G is profinite, we should only consider the *continuous* cocycles. To an IA-endomorphism $\gamma \in \mathrm{IAEnd}(G)$ we associate the 1-cocycle $\delta_\gamma : G \to G'$ given by $\delta_\gamma(g) = \gamma(g)g^{-1}$. One easily checks that the map $\gamma \mapsto \delta_\gamma$ defines a bijection

$$\mathrm{IAEnd}(G) \cong_{\underline{\mathbf{Sets}}} Z^1(G, G')$$

Since the R_G-action on G' commutes with the action of G, $Z^1(G, G')$ inherits the structure of an R_G-module.

Proposition 3.5. *Let G be a metabelian group generated by x_1, x_2. Write $c := [x_1, x_2]$.*

(a) The R_G-module of IA-endomorphisms, viewed as cocycles, is free of rank 2, with a basis consisting of the inner automorphisms $\mathrm{inn}(x_1), \mathrm{inn}(x_2)$.

(b) For any $z_1, z_2 \in G'$, there is a (unique) IA-endomorphism γ_{z_1,z_2} of G mapping x_i to $z_i x_i$ for $i = 1, 2$. Writing $z_i = c^{r_i}$ for $r_i \in R_G$, γ_{z_1,z_2} is given by the formula

$$\gamma_{z_1,z_2}(g) = [x_1, g]^{r_2}[x_2, g]^{-r_1} g \tag{7}$$

(c) For γ_{z_1,z_2} as in (b), writing $z_i = c^{r_i}$, we have

$$\det(\gamma_{z_1,z_2}) = 1 + r_2(a_1 - 1) - r_1(a_2 - 1) \tag{8}$$

Proof. For $i = 1, 2$, let δ_i denote the cocycle associated to $\mathrm{inn}(x_i)$, so $\delta_i(g) = [x_i, g]$ in G'. Let $c \in G'$ be an R_G-basis. Using the isomorphism $\exp_c : R_G \xrightarrow{\sim} G'$, it suffices to instead work with $Z^1(G, R_G)$. Then in R_G, $\delta_1(x_2) = 1$, $\delta_2(x_1) = -1$, and $\delta_i(x_i) = 0$ for $i = 1, 2$. It follows that the map

$$\begin{array}{rcl} \mathrm{ev}_{x_1,x_2} : Z^1(G, G') \cong Z^1(G, R_G) & \longrightarrow & R_G^2 \\ \delta & \mapsto & (\delta(x_1), \delta(x_2)) \end{array}$$

sends δ_1 to $(0, 1)$ and δ_2 to $(-1, 0)$, so it is an R_G-linear isomorphism. This proves (a). Writing $z_i = c^{r_i}$, the linear combination $r_2\delta_1 - r_1\delta_2 \in Z^1(G, R_G)$ sends $x_i \mapsto r_i$ (for $i = 1, 2$). The corresponding IA-endomorphism then takes the form (7) and sends $x_i \mapsto z_i x_i$ as desired. Since an endomorphism is determined by its values on generators, this endomorphism is unique. This proves (b).

For (8), note that for $g \in G$, $[g, c] = c^{\overline{g}-1}$ where $\overline{g}$ denotes the image of g in G^{ab}. Thus

$$\begin{array}{rcl} \gamma_{z_1,z_2}(c) & = & [x_1, c]^{r_2}[x_2, c]^{-r_1} c \\ & = & c^{(a_1-1)r_2} c^{-(a_2-1)r_1} c \\ & = & c^{1+(a_1-1)r_2-(a_2-1)r_1} \end{array}$$

This proves (c). □

Corollary 3.6. *Let $f : G \to H$ be a surjection of 2-generated metabelian groups. Then every IA-endomorphism of G descends to H, and moreover every IA-endomorphism of H is induced by an IA-endomorphism of G.*

Proof. For $z_1, z_2 \in G'$, the IA-endomorphism γ_{z_1,z_2} descends to $\gamma_{f(z_1),f(z_2)}$. Since f induces a surjection $G' \to H'$, every IA-endomorphism of H lifts to an IA-endomorphism of G. □

Remark 3.7. This property fundamentally uses the fact that G is 2-generated and the corollary that G' is a *cyclic* $\mathbb{Z}[G^{\mathrm{ab}}]$-module. Indeed, for an IA-endomorphism to descend to every quotient it must descend to every $\mathbb{Z}[G^{\mathrm{ab}}]$-quotient of G'.

3.2 The groups $M_{n,m}$

For integers $n, m \geq 1$, let $M_{n,m}$ denote the group with presentation

$$M_{n,m} = \langle x_1, x_2 \mid x_1^n = x_2^n = [x_1, x_2]^m = 1 \rangle$$

We call x_1, x_2 the *standard generators* of $M_{n,m}$. It is a 2-generated metabelian group with abelianization $A_{n,m} := M_{n,m}^{\mathrm{ab}} \cong (\mathbb{Z}/n)^2$. We write a_1, a_2 for the images of x_1, x_2 in $A_{n,m}$. The commutator subgroup $M'_{n,m}$ is a $(\mathbb{Z}/m)[A_{n,m}] = (\mathbb{Z}/m)[a_1, a_2]/\langle a_1^n - 1, a_2^n - 1\rangle$-module generated by $c := [x_1, x_2]$. We will write

$$R_{n,m} := R_{M_{n,m}} \cong_{\exp_c} M'_{n,m}$$

for the quotient of $(\mathbb{Z}/m)[A_{n,m}]$ by $\mathrm{Ann}_{(\mathbb{Z}/m)[A_{n,m}]}(M'_{n,m})$. In particular, $M_{n,m}$ is finite. Since $x_2^n = 1$, we also have $[x_1, x_2^n] = 1$. Applying (**??**) inductively, we see that c is killed by $\sum_{i=0}^{n-1} a_2^i$. Since $[x_1^n, x_2] = [x_2, x_1^n]^{-1}$, it is also killed by $\sum_{i=0}^{n-1} a_1^i$.

Proposition 3.8. *The annihilator of $M'_{n,m}$ is the ideal $I_{n,m} := \langle \sum_{i=0}^{n-1} a_1^i, \sum_{i=0}^{n-1} a_2^i \rangle$. In other words,*

$$R_{n,m} = (\mathbb{Z}/m)[a_1, a_2]/I_{n,m}.$$

Proof. Let $[a_1], [a_2]$ denote the images of a_1, a_2 in $(\mathbb{Z}/m)[A_{n,m}]/I_{n,m}$. We claim that $M_{n,m}$ is the semidirect product $S := ((\mathbb{Z}/m)[A_{n,m}]/I_{n,m} \rtimes \langle x_2 \rangle) \rtimes \langle x_1 \rangle$, where x_2 acts on $(\mathbb{Z}/m)[A_{n,m}]/I_{n,m}$ by multiplication by $[a_2]$, and x_1 acts on $(\mathbb{Z}/n)[A_{n,m}]/I_{n,m} \rtimes \langle x_2 \rangle$ by sending $(0, x_2) \mapsto (1, x_2)$ and $(r, 1) \mapsto ([a_2]r, 1)$. Here, $x_1, x_2 \in M_{n,m}$ corresponds to $(0, 1, x_1), (0, x_2, 1) \in S$. Thus, x_1 acts by sending

$$(r, x_2^k) = (r, 1)(0, x_2)^k \mapsto ([a_1]r, 1)(1, x_2)^k = ([a_1]r, 1)\left(\sum_{i=0}^{k-1} [a_2]^i, x_2^k\right) = \left([a_1]r + \sum_{i=0}^{k-1} [a_2]^i, x_2^k\right)$$

The relations $\sum_{i=0}^{n-1} a_1^i = \sum_{i=0}^{n-1} a_2^i = 0$ imply that x_1, x_2 each act with order n, and their images in the semidirect product S have order n. In S, the commutator $[x_1, x_2]$ becomes:

$$[x_1, x_2] = [(0, 1, x_1), (0, x_2, 1)] = (0, 1, x_1)(0, x_2, 1)(0, 1, x_1^{-1})(0, x_2^{-1}, 1) = (1, 1, 1)$$

which is identified with the order m element $1 \in (\mathbb{Z}/n)[A_{n,m}]/I_{m,n} \subset S$. This shows that $S' = R_{n,m}$, or equivalently that the $(\mathbb{Z}/m)[A_{n,m}]$-module annihilator of S' is $I_{n,m}$. Since x_1, x_2 satisfy the same relations in S as in $M_{n,m}$, S is a quotient of $M_{n,m}$. Thus S' is a $(\mathbb{Z}/m)[A_{n,m}]$-module quotient of $M'_{n,m}$, so we have

$$I_{n,m} \subset \mathrm{Ann}(M'_{n,m}) \subset \mathrm{Ann}(S') = I_{n,m}$$

so $I_{n,m} = \mathrm{Ann}(M'_{n,m})$ as desired. This also shows that $M_{n,m} \cong S$ as claimed. □

3.3 The free profinite metabelian group M

If G is a profinite group, the (projective) limit of finite groups G_α, the completed group algebra $\widehat{\mathbb{Z}}[\![G]\!]$ is defined to be the limit $\lim_{\alpha,n}(\mathbb{Z}/n)[G_\alpha]$. It is also the product of the rings $\mathbb{Z}_p[\![G]\!] := \lim_{k,\alpha}(\mathbb{Z}/p^r)[G_\alpha]$.

Abelianization and (closed) derived subgroups respect the limit structure: $G' = \lim_\alpha G'_\alpha$ and $G^{\mathrm{ab}} = \lim_\alpha G_\alpha^{\mathrm{ab}}$. Passing to the limit, we find that G' is a $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module, and that if G is generated by x_1, x_2, then G' is generated as a $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module by the commutator $[x_1, x_2]$. As in §3.1, we will denote by R_G the quotient of $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$ by the annihilator of c. Similarly, $\exp_c : r \mapsto c^r$ defines an isomorphism $R_G \xrightarrow{\sim} G'$, valid for any $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module generator c of G'.

Definition 3.9. We will write M for the free profinite metabelian group of rank 2. This is a profinite metabelian group which is free of rank 2 in the category of profinite metabelian groups. Moreover we will write A for the abelianization of M.

Proposition 3.10. *Let x_1, x_2 be generators of M, with images $a_1, a_2 \in A$. Then $(a_1, a_2) : \widehat{\mathbb{Z}}^2 \to A$ is an isomorphism, and M' is a free $\widehat{\mathbb{Z}}[\![A]\!]$-module of rank 1 generated by $c := [x_1, x_2]$. In particular, the determinant $\det_c$ on $\operatorname{End}(M)$ takes values in $\widehat{\mathbb{Z}}[\![A]\!]$.*

Proof. The profinite group M is the limit of the $M_{n,m}$'s of §3.2 (for $n, m \geq 1$), where $x_1, x_2 \in M$ maps to the standard generators of $M_{n,m}$. Each $M_{n,m}$ has abelianization $A_{n,m} \cong (\mathbb{Z}/n)^2$ and derived subgroup $M'_{n,m} \cong (\mathbb{Z}/m)[A_{n,m}]/I_{n,m}$, where $I_{n,m}$ is as in 3.8 and 1 is identified with (the image of) c. Thus we have $A = \lim A_{n,m} = \lim(\mathbb{Z}/n)^2 = \widehat{\mathbb{Z}}^2$. For each n, m, we have a short exact sequence

$$0 \longrightarrow I_{n,m} \longrightarrow (\mathbb{Z}/m)[A_{n,m}] \longrightarrow M'_{n,m} \longrightarrow 0$$

Since all groups involved are finite, the limit functor is exact, so we get an exact sequence

$$0 \longrightarrow \lim I_{n,m} \longrightarrow \widehat{\mathbb{Z}}[\![A]\!] \longrightarrow M' \longrightarrow 0.$$

It remains to show that $\lim I_{n,m} = 0$. Indeed, the map $I_{nm,m} \to I_{n,m}$ sends $\sum_{i=0}^{nm-1} a_1^i$ to $m \sum_{i=0}^{n-1} a_1^i = 0$, and similarly for a_2. □

3.4 Structure of $\widehat{\mathbb{Z}}[\![A]\!] \cong \widehat{\mathbb{Z}}[\![\widehat{\mathbb{Z}}^2]\!]$

Recall the following classical result (see [Wil98, Theorem 7.3.3])

Lemma 3.11. *The completed group algebra $\mathbb{Z}_p[\![\mathbb{Z}_p^n]\!]$ is isomorphic to the power series ring $\mathbb{Z}_p[\![s_1, \ldots, s_n]\!]$, where the ith canonical basis element of $\mathbb{Z}_p^n$ corresponds to $1 + s_i$ (for $i = 1, 2, \ldots, n$).*

Here we give the analogous result for $\widehat{\mathbb{Z}}[\![A]\!]$. Since $\widehat{\mathbb{Z}}[\![A]\!] = \prod_p \mathbb{Z}_p[\![A]\!]$, it suffices to study the rings $\mathbb{Z}_p[\![A]\!]$.

Lemma 3.12. *For each prime p, there is an (infinite) index set I and an isomorphism*

$$\mathbb{Z}_p[\![A]\!] \cong \mathbb{Z}_p[\![s_1, s_2]\!] \times \prod_{i \in I} R_{p,i}$$

satisfying

(a) Each $R_{p,i}$ is a 2-variable power series ring over the ring of Witt vectors $W(\mathbb{F}_q)$ for some prime power $q = p^r$, where $r \geq 2$ is coprime to p.

(b) For any generating pair $a_1, a_2 \in A$, the images of $a_1 - 1, a_2 - 1$ in $\mathbb{Z}_p[\![s_1, s_2]\!]$ generate the ideal $\langle s_1, s_2 \rangle$.

(c) For any generating pair $a_1, a_2 \in A$ and any $i \in I$, the images of $a_1 - 1, a_2 - 1$ in $R_{p,i}$ are nonzero, and at least one of them is a unit.

In particular, $a_1 - 1, a_2 - 1$ are regular elements of $\widehat{\mathbb{Z}}[\![A]\!]$, and

$$\widehat{\mathbb{Z}}[\![A]\!] \cong \widehat{\mathbb{Z}}[\![s_1, s_2]\!] \times \prod_{p,i} R_{p,i}$$

Remark 3.13. Geometrically, $\mathbb{Z}_p[\![A]\!]$ is the affine algebra of the ind-group-scheme $\varinjlim_{n \geq 1} \mu_n \times \mu_n$ over $\mathbb{Z}_p$, and the direct factor $\mathbb{Z}_p[\![s_1, s_2]\!]$ in the lemma is the affine algebra of the connected component of the identity.

Proof. Let $\mathbb{Z}^{(p')}$ be the prime-to-p part of $\widehat{\mathbb{Z}}$, so that $A = \mathbb{Z}_p^2 \times (\mathbb{Z}^{(p')})^2$. Let $\widehat{\otimes}$ denote the completed tensor product over $\mathbb{Z}_p$, then we have $\mathbb{Z}_p[\![A]\!] \cong \mathbb{Z}_p[\![\mathbb{Z}_p^2]\!] \widehat{\otimes} \mathbb{Z}_p[\![(\mathbb{Z}^{(p')})^2]\!]$. By Lemma 3.11, $\mathbb{Z}_p[\![\mathbb{Z}_p^2]\!] \cong \mathbb{Z}_p[\![s_1, s_2]\!]$, with a_i mapping to $1 + s_i$. It remains to study $\mathbb{Z}_p[\![(\mathbb{Z}^{(p')})^2]\!]$. The ring $\mathbb{Z}_p[\![(\mathbb{Z}^{(p')})^2]\!]$ is the limit of the finite étale $\mathbb{Z}_p$-algebras $S_n := \mathbb{Z}_p[x_1, x_2]/(x_1^n - 1, x_2^n - 1)$ for n coprime to p. Each S_n is the product of finite étale $\mathbb{Z}_p$-algebras $\mathbb{Z}_p[x_1, x_2]/(f_1(x_1), f_2(x_2))$, where $f_i \in \mathbb{Z}_p[x]$ ranges over monic irreducible factors of $x^n - 1$. Let $\operatorname{Cyc} \subset \mathbb{Z}_p[x]$

denote the set of all polynomials which are monic irreducible factors of $x^m - 1$ for some m coprime to p. Passing to the limit and tensoring with $\mathbb{Z}_p[\![\mathbb{Z}_p^2]\!] \cong \mathbb{Z}_p[\![s_1, s_2]\!]$, we have an isomorphism

$$\mathbb{Z}_p[\![A]\!] \cong \prod_{(f_1,f_2)\in\mathrm{Cyc}^2} \underbrace{\mathbb{Z}_p[x_1,x_2]/(f_1(x_1), f_2(x_2))[\![s_1,s_2]\!]}_{S_{f_1,f_2}}$$

where a_i maps to $x_i(1+s_i)$, and where each S_{f_1,f_2} will further split into finite étale $\mathbb{Z}_p[\![s_1,s_2]\!]$-algebras according to the degrees of f_1, f_2 (which are coprime to p). It follows that $\mathbb{Z}_p[\![A]\!]$ contains only one direct factor isomorphic to $\mathbb{Z}_p[\![s_1,s_2]\!]$, corresponding to $f_1 = f_2 = x - 1$, in which a_i maps to $1 + s_i$. This proves (a) and (b).

In the other direct factors, $a_i - 1$ maps to $x_i(1+s_i) - 1 = x_i s_i + (x_i - 1)$, where at least one of $x_1, x_2 \neq 1$. This proves (c). □

The *augmentation map*

$$\epsilon : \widehat{\mathbb{Z}}[\![A]\!] \longrightarrow \widehat{\mathbb{Z}}$$

is the $\widehat{\mathbb{Z}}$-linear map given by sending $A \mapsto 1$. For $s \in \widehat{\mathbb{Z}}$, let $\widehat{\mathbb{Z}}[\![A]\!]_{\epsilon=s}$ denote the subset with augmentation equal to s. If a_1, a_2 is a generating pair of A, then the kernel of ϵ is generated by $a_1 - 1, a_2 - 1$, and is called the *augmentation ideal* $I_A = \widehat{\mathbb{Z}}[\![A]\!]_{\epsilon=0}$. It follows from (8) that

Corollary 3.14. *The image of* $\det : \mathrm{IAEnd}(M) \to \widehat{\mathbb{Z}}[\![A]\!]$ *is* $1 + I_A = \widehat{\mathbb{Z}}[\![A]\!]_{\epsilon=1}$.

Corollary 3.15. *With notation as above, consider the sequence*

$$0 \longrightarrow \widehat{\mathbb{Z}}[\![A]\!] \xrightarrow{d_2} \widehat{\mathbb{Z}}[\![A]\!]^2 \xrightarrow{d_1} \widehat{\mathbb{Z}}[\![A]\!] \xrightarrow{\epsilon} \widehat{\mathbb{Z}} \longrightarrow 0 \tag{9}$$

where d_2 is given by $(a_1 - 1, a_2 - 1)$, and d_1 is given by $(1 - a_2, a_1 - 1)$. The sequence is exact.

Proof. This can be directly checked using Lemma 3.12. Alternatively, the first three nonzero terms of the sequence (9) is called the *Koszul complex* associated to the ring $\widehat{\mathbb{Z}}[\![A]\!]$ and the elements $a_1 - 1, a_2 - 1$. It follows from Lemma 3.12 that $a_1 - 1, a_2 - 1$ is a regular sequence for $\widehat{\mathbb{Z}}[\![A]\!]$. The exactness of (9) follows from the fact that the Koszul homology associated to a regular sequence vanishes in positive degrees, and the zeroth homology is the quotient by the ideal generated by the regular sequence [Mat89, Theorem 16.5]. □

Corollary 3.16. *Let $x_1, x_2 \in M$ be generators, $c := [x_1, x_2]$. Then*

(a) The center of M is trivial.

(b) Any automorphism of M which acts as the identity on A and which maps c to a conjugate is inner.

(c) Any automorphism of M which act as the identity on both A and M' is equal to $\mathrm{inn}(z)$ *for some $z \in M'$.*

Proof. For (a), suppose $z \in M$ is central, with image $\overline{z} \in A$. Since z conjugates c into $c^{\overline{z}}$, by freeness of M' (3.10), it follows that $\overline{z} = 1$, so $z \in M' \cong \widehat{\mathbb{Z}}[\![A]\!]$. Now note $1 = [x_1, z] = x_1 z x_1^{-1} z^{-1} = z^{a_1 - 1}$, so $a_1 - 1$ kills z, but since $a_1 - 1$ is regular it follows that $z = 1$. Now let γ be an automorphism with the properties stated in (c). For suitable $r_i \in \widehat{\mathbb{Z}}[\![A]\!]$, we have $\gamma(x_i) = c^{r_i} x_i$, and

$$\gamma(c) = [c^{r_1}x_1, c^{r_2}x_2] = c^{r_1}x_1c^{r_2}x_2x_1^{-1}c^{-r_1}x_2^{-1}c^{-r_2} = c^{r_1+a_1r_2-a_2r_1-r_2} = c^{(1-a_2)r_1+(a_1-1)r_2}$$

The assumption that $\gamma(c) = c$ implies, by Corollary 3.15, that there is an $r \in \widehat{\mathbb{Z}}[\![A]\!]$ such that $r_i = (1 - a_i)b$, in which case one easily checks that γ is just $\mathrm{inn}(c^b)$; this proves (c). Finally, let γ be an automorphism as in (b). Then $\gamma \circ \mathrm{inn}(\det(\gamma))^{-1}$ acts as the identity on M', and hence (b) follows from (c). □

Let $\widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1}$ be the group of units of $\widehat{\mathbb{Z}}[\![A]\!]$ which have augmentation 1. This contains A as a subgroup.

Corollary 3.17. *The determinant* $\det : \mathrm{IAut}(M) \to \widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1}$ *induces an isomorphism*

$$\overline{\det} : \mathrm{IOut}(M) \xrightarrow{\sim} \widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1}/A$$

Proof. The map $\mathrm{IAut}(M) \to \widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1}/A$ is surjective by Corollary 3.14, and has kernel $\mathrm{Inn}(M)$ by 3.16(b). □

This implies that $\mathrm{IOut}(M)$ isn't even topologically finitely generated. Contrast this with the discrete case, where this group vanishes:

Theorem 3.18 (Nielsen, Bachmuth)**.** *Let $\mathbf{F} = \mathbf{F}_2$ denote a (discrete) free group of rank 2, let $\mathbf{M} = \mathbf{M}_2 := \mathbf{F}_2/\mathbf{F}_2''$ denote a free (discrete) metabelian group of rank 2, and let $\mathbf{A} := \mathbf{F}/\mathbf{F}'$ be the abelianization. The canonical maps $\mathbf{F} \to \mathbf{M} \to \mathbf{A}$ induces surjections $\mathrm{Aut}(\mathbf{F}) \to \mathrm{Aut}(\mathbf{M}) \to \mathrm{GL}(\mathbf{A})$, and $\mathrm{IAut}(\mathbf{F}), \mathrm{IAut}(\mathbf{M})$ consist precisely of the inner automorphisms. In particular, $\mathrm{IOut}(\mathbf{F}) = \mathrm{IOut}(\mathbf{M}) = 1$, and the surjections above induce isomorphisms $\mathrm{Out}(\mathbf{F}) \cong \mathrm{Out}(\mathbf{M}) \cong \mathrm{GL}(\mathbf{A})$.*

Proof. The relation between $\mathrm{Aut}(\mathbf{F})$ and $\mathrm{GL}(\mathbf{A})$ is a classical result of Nielsen [MKS04, §3, Corollaries 3.5.1, N4]. The relation between $\mathrm{Aut}(\mathbf{M})$ and $\mathrm{GL}(\mathbf{A})$ follows from results of Bachmuth [Bac65, §4]. □

3.5 Splitting $\mathrm{Out}(M)$

Let x_1, x_2 be generators for M, with $c := [x_1, x_2]$. By the universal property of M, for any $x_1', x_2' \in M$, there is a unique endomorphism γ of M mapping $(x_1, x_2) \mapsto (x_1', x_2')$. Let γ^{ab} be the induced endomorphism of A.

The subgroup $\exp_c(I_A) \leq M'$ is characteristic in M. If U denotes the quotient, then we have a commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & \widehat{\mathbb{Z}}[\![A]\!] \arrow[r, "\exp_c"] \arrow[d, "\epsilon"] & M \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & U \arrow[r] & A \arrow[r] & 1
\end{tikzcd}$$

The group U is a free profinite class-2-nilpotent group of rank 2. In particular, U is a central extension of A by $\widehat{\mathbb{Z}}$. If we write $\gamma(c) = c^r$ for some $r \in \widehat{\mathbb{Z}}[\![A]\!]$, then the problem of calculating the image of r by the augmentation $\epsilon : \widehat{\mathbb{Z}}[\![A]\!] \to \widehat{\mathbb{Z}}$ takes place in U. On U, the commutator is a nondegenerate alternating bilinear form $U \times U \to U' \cong \widehat{\mathbb{Z}}$. This proves part (a) in the following

Proposition 3.19. *With notation as above,*

(a) The image of $\det_c(\gamma) \in \widehat{\mathbb{Z}}[\![A]\!]$ under the augmentation is $\det(\gamma^{\mathrm{ab}}) \in \widehat{\mathbb{Z}} \subset \widehat{\mathbb{Z}}[\![A]\!]$.

(b) If γ^{ab} is an automorphism of A, then there exist $r_1, r_2 \in \widehat{\mathbb{Z}}[\![A]\!]$ such that for the endomorphism γ' sending $(x_1, x_2) \mapsto (c^{r_1} x_1', c^{r_2} x_2')$, we have
$$\det_c(\gamma') = \det(\gamma^{\mathrm{ab}})$$
In particular, γ' is an automorphism, inducing γ^{ab} on A.

Proof. Part (a) was proven above. For the second part, let a_1', a_2' be the images of x_1', x_2' in A. By assumption, a_1', a_2' is a basis of A, so by lifting a_1', a_2' to generators of M [RZ10, Proposition 2.5.4], we find that there is an automorphism of M lifting γ^{ab}. Thus we may assume that γ is an automorphism, with determinant $\det_c(\gamma) = \det(\gamma^{\mathrm{ab}}) + s = \det(\gamma^{\mathrm{ab}})(1 + s \cdot \det(\gamma^{\mathrm{ab}})^{-1})$ for some $s \in I_A$. Note that $1 + s\det(\gamma^{\mathrm{ab}})^{-1}$ is a unit.

By 3.14, the determinant on $\mathrm{IAEnd}(M)$ surjects onto $1 + I_A$, so there is a $\delta \in \mathrm{IAut}(M)$ with $\det(\delta) = 1 + s\det(\gamma^{\mathrm{ab}})^{-1}$. Then $\gamma' := \gamma \circ \delta^{-1}$ has the desired properties. □

Definition 3.20. Let $\mathrm{Out}(M, \langle c\rangle)$ denote the subgroup of $\mathrm{Out}(M) := \mathrm{Aut}(M)/\mathrm{Inn}(M)$ which preserves the conjugacy class of the procyclic subgroup generated by c. Thus, its elements are represented by automorphisms which send c to a conjugate of c^u for some $u \in \widehat{\mathbb{Z}}^\times$.

Remark 3.21. Proposition 3.19(a) implies that for any $\gamma \in \mathrm{Out}(M, \langle c\rangle)$ inducing γ^{ab} on A, $\gamma(c)$ is conjugate to $c^{\det(\gamma^{\mathrm{ab}})}$. This implies that the group $\mathrm{Out}(M, \mathcal{I})$ admits a "canonical" determinant, simply denoted

$$\det : \mathrm{Out}(M, \mathcal{I}) \longrightarrow \widehat{\mathbb{Z}}^\times$$

which, for any generator $c' \in \langle c\rangle$, satisfies $\det(\gamma) = \det_c(\gamma) = \det_{c'}(\gamma) = \det(\gamma^{\mathrm{ab}})$.

Theorem 3.22. *With notation as above, the canonical maps*

$$\mathrm{Out}(M, \langle c\rangle) \longrightarrow \mathrm{Out}(U) \longrightarrow \mathrm{GL}(A)$$

are isomorphisms. In particular, if $\mathrm{IOut}(M) := \mathrm{IAut}(M)/\,\mathrm{Inn}(M)$*, then the sequence*

$$1 \longrightarrow \mathrm{IOut}(M) \longrightarrow \mathrm{Out}(M) \longrightarrow \mathrm{GL}(A) \longrightarrow 1 \tag{10}$$

is split exact, the splitting being given by $\mathrm{GL}(A) \cong \mathrm{Out}(M, \langle c\rangle) \le \mathrm{Out}(M)$*.*

Proof. By 3.19, any automorphism $\overline{\gamma}$ of A can be lifted to an automorphism γ of M sending $c \mapsto c^{\det \overline{\gamma}}$, which proves the surjectivity of $\mathrm{Out}(M, \langle c\rangle) \to \mathrm{GL}(A)$. If $\gamma \in \mathrm{Out}(M, \langle c\rangle)$ acts trivially on A, then by 3.19 it must in fact fix c, so by 3.16, it is inner. This shows the injectivity of $\mathrm{Out}(M, \langle c\rangle) \to \mathrm{GL}(A)$. Injectivity of $\mathrm{Out}(U) \to \mathrm{GL}(A)$ is similar. □

Corollary 3.23. *Let* $c \in M'$ *be a basis. Let* G *be a finite 2-generated metabelian group. The action of* $\mathrm{IOut}(G)$ *on* $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ *commutes with the* $\mathrm{Out}(M)$*-action, and permutes transitively the* $\mathrm{Out}(M, \langle c\rangle)$*-orbits. In particular the* $\mathrm{Out}(M, \langle c\rangle)$*-orbits on* $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ *are all* $\mathrm{Out}(M, \langle c\rangle)$*-equivariantly isomorphic to each other.*

Proof. The fact that $\mathrm{IOut}(G)$ commutes with the $\mathrm{Out}(M)$-action is just the associativity of function composition. By Gaschütz lemma [RZ10, Proposition 2.5.4], $\mathrm{Out}(M)$ acts transitively on $\mathrm{Epi}^{\mathrm{ext}}(M, G)$. Using the splitting of the sequence (10), for a fixed $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(M, G)$, every element of $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ can be written as $\varphi \circ u \circ \gamma$ for some $u \in \mathrm{IOut}(M), \gamma \in \mathrm{Out}(M, \langle c\rangle)$. By 3.5, we have a homomorphism $\varphi_* : \mathrm{IOut}(M) \longrightarrow \mathrm{IOut}(G)$ satisfying $\varphi \circ u = \varphi_*(u) \circ \varphi$. Thus every element of $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ can be written as

$$v \circ \varphi \circ \gamma \qquad \text{for some } v \in \mathrm{IOut}(G), \gamma \in \mathrm{Out}(M, \langle c\rangle)$$

This shows that $\mathrm{IOut}(G)$ acts transitively on the $\mathrm{Out}(M, \langle c\rangle)$-orbits, commuting with the $\mathrm{Out}(M, \langle c\rangle)$-action. Thus the $\mathrm{Out}(M, \langle c\rangle)$-orbits are all isomorphic. □

4 Nielsen equivalence and Koszul homology

4.1 The structure of $\mathrm{IAut}(G)$

Lemma 4.1. *Let* $f : R \to S$ *be a surjection of profinite rings, then* f *induces a surjection on groups of units.*

Proof. By considering induced maps on finite quotients, we are reduced to the case where R, S are finite. In this case, let $I := \ker f$ and let $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ be the maximal ideals of R not containing I. For a unit $u \in S^\times$, let $r \in f^{-1}(u)$. Since $I, \mathfrak{m}_1, \dots, \mathfrak{m}_r$ are pairwise comaximal, by the Chinese remainder theorem we can find $a \in R$ with $a \equiv 0 \mod I, a \equiv 1 - r \mod \mathfrak{m}_i$ for $i = 1, \dots, r$. Then $r + a \in R^\times$ and $f(r + a) = f(r) = u$, as desired.[9] □

Let G be a 2-generated profinite metabelian group. Let

$$\epsilon_G : G' \longrightarrow G'_{G^{\mathrm{ab}}} = H_0(G^{\mathrm{ab}}, G')$$

be the module of G^{ab}-coinvariants. Since G' is a free R_G-module of rank 1, ϵ_G is an analogue of the augmentation $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!] \to \widehat{\mathbb{Z}}$.

Definition 4.2. Let $\mathrm{IAut}_1(G) := \mathrm{Ker}(\mathrm{IAut}(G) \to \mathrm{Aut}(G'))$.

Theorem 4.3. *Let* G *be a 2-generated profinite metabelian group. The following sequence is exact*

$$1 \longrightarrow \underbrace{\mathrm{IAut}_1(G)}_{} \longrightarrow \mathrm{IAut}(G) \xrightarrow{\det} \underbrace{\mathrm{Aut}_{G^{\mathrm{ab}}}(G')}_{\cong R_G^\times} \xrightarrow{(\epsilon_G)_*} \mathrm{Aut}(\underbrace{H_0(G^{\mathrm{ab}}, G')}_{G'_{G^{\mathrm{ab}}}}) \longrightarrow 1$$

Moreover $G'_{G^{\mathrm{ab}}}$ *is a procyclic group.*

[9] More generally if $\ker f$ is contained all but finitely many maximal ideals of R, then f induces a surjection on unit groups.

Proof. Exactness at $\mathrm{IAut}_1(G)$ and $\mathrm{IAut}(G)$ is clear by definition, so it remains to prove procyclicity of $G'_{G^{\mathrm{ab}}}$ and exactness at the last two terms. Let $\pi : M \to G$ be a surjection, using which we view G' as a $\widehat{\mathbb{Z}}[\![A]\!]$-module. Let $\epsilon : M' \to M'_A$ be the canonical map. Then π induces a diagram

$$\begin{tikzcd}
M' \arrow[r, "\epsilon"] \arrow[d, "\pi"] & M'_A \arrow[d, "\pi"] \\
G' \arrow[r, "\epsilon_G"] & G'_{G^{\mathrm{ab}}}
\end{tikzcd}$$

Let $J_G := \mathrm{Ann}_{\widehat{\mathbb{Z}}[\![A]\!]}(G')$, then picking a $\widehat{\mathbb{Z}}[\![A]\!]$-basis for M', this diagram can be identified with the diagram

$$\begin{tikzcd}
\widehat{\mathbb{Z}}[\![A]\!] \arrow[r, "\epsilon"] \arrow[d, "\pi"] & \widehat{\mathbb{Z}} = \widehat{\mathbb{Z}}[\![A]\!]/I_A \arrow[d, "\pi"] \\
R_G = \widehat{\mathbb{Z}}[\![A]\!]/J_G \arrow[r, "\epsilon_G"] & S_G := \widehat{\mathbb{Z}}[\![A]\!]/\langle I_A, J_G\rangle
\end{tikzcd} \tag{11}$$

In particular, we find that $G'_{G^{\mathrm{ab}}} \cong S_G$ is procyclic, and ϵ_G can be identified with the surjection of profinite rings $R_G \to S_G$. Since the source is a free R_G-module of rank 1 and the target is a free S_G-module of rank 1, the induced map $(\epsilon_G)_*$ on automorphism groups is identified with

$$(\epsilon_G)_* : R_G^\times \to S_G^\times$$

which is surjective since surjections of profinite rings induce surjections on groups of units (Lemma 4.1).

Finally we prove exactness at $\mathrm{Aut}_{G^{\mathrm{ab}}}(G')$. By Theorem 3.6, any IA-automorphism of G lifts to an IA-endomorphism of M, whose determinant has augmentation 1 by (8). The commutativity of the above diagram then implies that $\mathrm{im}(\det) \subset \ker(\epsilon_G)_*$. It remains to show that $\ker(\epsilon_G)_* \subset \mathrm{im}\det$. Let $u \in R_G^\times$ satisfy $(\epsilon_G)_*(u) = 1 \in S_G^\times$. Then any lift of u to $\tilde{u} \in \widehat{\mathbb{Z}}[\![A]\!]$ must satisfy $\tilde{u} = 1 + i + j$ for $i \in I_A, j \in J_G$. Then $\tilde{u} - j = 1 + i$ is another lift which satisfies $\epsilon(\tilde{u} - j) = 1$, and hence by 3.14 we may find $\beta \in \mathrm{IAEnd}(M)$ with $\det(\beta) = \tilde{u} - j$. By 3.6, β descends to an IA-endomorphism of G, which must be an IA-automorphism because it acts on G' by multiplication by $u \in R_G^\times$. This completes the proof. □

Definition 4.4. Let $R^\times_{G,\epsilon=1} := \ker(\epsilon_G)_* \subset R_G^\times$. In particular, $R^\times_{M,\epsilon=1} = \widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1}$ is the group $(1 + I_A) \cap \widehat{\mathbb{Z}}[\![A]\!]^\times$ of units with augmentation 1.

Remark 4.5. Taking kernels of ϵ, ϵ_G in (11) and applying the snake lemma, we find that for any surjection $\pi : M \to G$, the induced map $\widehat{\mathbb{Z}}[\![A]\!] \to R_G$ induces a surjection $\widehat{\mathbb{Z}}[\![A]\!]^\times_{\epsilon=1} \twoheadrightarrow R^\times_{G,\epsilon=1}$.

4.2 The structure of $\mathrm{Epi}(M, G)$

Let G be a 2-generated profinite metabelian group. By Gaschütz's lemma [RZ10, Proposition 2.5.4], the abelianization $\mathrm{ab} : G \to G^{\mathrm{ab}}$ induces a surjection

$$\begin{array}{rcl} \xi : \mathrm{Epi}(M, G) & \longrightarrow & \mathrm{Epi}(M, G^{\mathrm{ab}}) \\ \varphi & \mapsto & \mathrm{ab} \circ \varphi \end{array}$$

Proposition 4.6. *The group* $\mathrm{IAut}(G)$ *acts freely and transitively on the fibers of* $\xi : \mathrm{Epi}(M, G) \to \mathrm{Epi}(M, G^{\mathrm{ab}})$. *That is to say,* ξ *is a* torsor *under* $\mathrm{IAut}(G)$.

Proof. Clearly $\mathrm{IAut}(G)$ acts freely on the fibers of ξ. Fixing a basis x_1, x_2 for M, if $(g_1, g_2), (g'_1, g'_2)$ are generating pairs of G with the same image in G^{ab}, then we have $g'_i = [g_1, g_2]^{r_i} g_i$ for some $r_i \in R_G$. Let $\pi : M \to G$ be the surjection sending $x_i \mapsto g_i$, inducing a surjection $\pi_* : \widehat{\mathbb{Z}}[\![A]\!] \to R_G$. Then for any lifts of r_1, r_2 to $\tilde{r_1}, \tilde{r_2}$ of $\widehat{\mathbb{Z}}[\![A]\!]$, the map sending $x_i \mapsto [x_1, x_2]^{\tilde{r_i}} x_i$ defines an IA-endomorphism of M which by 3.6 descends to an IA-endomorphism of G sending $g_i \mapsto g'_i$. Since (g'_1, g'_2) generates G, this endomorphism is surjective, hence an automorphism since finitely generated profinite groups are Hopfian [RZ10, Proposition 2.5.2]. □

Remark 4.7. The weaker statement that the fibers of ξ all have the same cardinality holds more generally by the proof of Gaschütz's lemma [RZ10, Proposition 2.5.4].

Corollary 4.8. *Let G be a 2-generated profinite metabelian group and $\varphi : M \to G$ be a surjection. Let $\mathrm{ab} : G \to G^{\mathrm{ab}}$ the abelianization. Then for any $\gamma \in \mathrm{Aut}(M)$, if $\mathrm{ab} \circ \varphi \circ \gamma = \mathrm{ab} \circ \varphi$, then there exists a uniquely determined $\alpha \in \mathrm{IAut}(G)$ such that $\varphi \circ \gamma = \alpha \circ \varphi$. Writing $\alpha = \varphi_*(\gamma)$, this defines a group homomorphism*

$$\varphi_* : \mathrm{Stab}_{\mathrm{Aut}(M)}(\mathrm{ab} \circ \varphi) \longrightarrow \mathrm{IAut}(G)$$

Proof. Follows immediately from Proposition 4.6. □

Let $\mathrm{Gens}(G')$ denote the set of R_G-module generators of G'; this is a torsor under $R_G^\times$, and hence any surjection $M \to G$ induces a surjection $\mathrm{Gens}(M') \to \mathrm{Gens}(G')$. If $c \in M'$ is a $\widehat{\mathbb{Z}}[\![A]\!]$-basis, we obtain a surjective map

$$\begin{array}{rcl} \kappa_c : \mathrm{Epi}(M, G) & \longrightarrow & \mathrm{Gens}(G') \\ \varphi & \mapsto & \varphi(c) \end{array}$$

In the following sections we will study the fibers of the map

$$\xi \times \kappa_c : \mathrm{Epi}(M, G) \longrightarrow \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$$

and its variations after imposing the equivalence relation generated by either conjugation by elements of G or conjugation by elements of G'. It follows from the above discussion that

Corollary 4.9. *For any choice of $\widehat{\mathbb{Z}}[\![A]\!]$-basis $c \in M'$, the map $\xi \times \kappa_c$ is a torsor under the group $\mathrm{IAut}_1(G)$.*

Proof. Follows immediately from the definitions and Proposition 4.6. □

Thus we will want to study appropriate quotients of the group $\mathrm{IAut}_1(G)$. If this quotient is trivial, then a generating pair of G is (up to equivalence) determined by its commutator and its image in G^{ab}.

4.3 Outer automorphism groups of G

Definition 4.10. For a group G, let $\mathrm{Inn}'(G) \subset \mathrm{Inn}(G)$ the subgroup of inner automorphisms realized by conjugation by an element of G'. Recall $\mathrm{IAut}_1(G) := \mathrm{Ker}(\mathrm{IAut}(G) \to \mathrm{Aut}(G'))$. Let $\mathrm{Inn}_1(G) := \mathrm{Inn}(G) \cap \mathrm{IAut}_1(G)$. We have the following notions of outer automorphism groups:

$$\begin{array}{rclrcl} \mathrm{Out}(G) & := & \mathrm{Aut}(G)/\,\mathrm{Inn}(G) & \mathrm{Out}'(G) & := & \mathrm{Aut}(G)/\,\mathrm{Inn}'(G) \\ \mathrm{IOut}(G) & := & \mathrm{IAut}(G)/\,\mathrm{Inn}(G) & \mathrm{IOut}'(G) & := & \mathrm{IAut}(G)/\,\mathrm{Inn}'(G) \\ \mathrm{IOut}_1(G) & := & \mathrm{IAut}_1(G)/\,\mathrm{Inn}_1(G) & \mathrm{IOut}'_1(G) & := & \mathrm{IAut}_1(G)/\,\mathrm{Inn}'(G) \end{array} \tag{12}$$

If G is profinite, we give these outer automorphism groups the quotient topology, and relative to this topology they are profinite groups. Now suppose G is a 2-generated profinite metabelian group. Since G' is a free R_G-module of rank 1, we may view the canonical representation as a homomorphism $\rho_G : G^{\mathrm{ab}} \to R_{G,\epsilon=1}^\times$ (see Definition 4.4). The determinant map $\det : \mathrm{IAut}(G) \to R_{G,\epsilon=1}^\times$ (surjective by 4.3) descends to a surjection $\mathrm{IOut}(G) \to R_{G,\epsilon=1}^\times/\rho_G(G^{\mathrm{ab}})$. Then we also have

$$\mathrm{IOut}_1(G) = \mathrm{Ker}\big(\mathrm{IOut}(G) \longrightarrow R_{G,\epsilon=1}^\times/\rho_G(G^{\mathrm{ab}})\big)$$

Let $\mathrm{ab} : G \to G^{\mathrm{ab}}$ denote the abelianization. We summarize the relationships between these various outer automorphism groups in the following diagram (all of whose rows and columns are exact)

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathrm{Ker}(\rho_G)/\mathrm{ab}(Z(G)) \arrow[r] \arrow[d] & \mathrm{Inn}(G)/\mathrm{Inn}'(G) \arrow[r, "\det"] \arrow[d] & \rho_G(G^{\mathrm{ab}}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{IOut}_1'(G) \arrow[r] \arrow[d] & \mathrm{IOut}'(G) \arrow[r, "\det"] \arrow[d] & R^\times_{G,\epsilon=1} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{IOut}_1(G) \arrow[r] \arrow[d] & \mathrm{IOut}(G) \arrow[r, "\det"] \arrow[d] & R^\times_{G,\epsilon=1}/\rho_G(G^{\mathrm{ab}}) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd} \tag{13}$$

Proposition 4.11. *The groups* $\mathrm{IAut}(G), \mathrm{IAut}_1(G), \mathrm{IOut}(G), \mathrm{IOut}'(G), \mathrm{IOut}_1(G), \mathrm{IOut}_1'(G)$ *are functorial for surjections of profinite 2-generated metabelian groups.*

Proof. Let $f : G_1 \to G_2$ be a surjection of profinite 2-generated metabelian groups. Then for any surjection $\pi : M \to G_1$, any $\alpha \in \mathrm{IAut}(G_1)$ can be lifted via π to an IA-automorphism of M, which descends to G_2 by 3.6. This shows that $\mathrm{IAut}(G)$ is functorial. Since derived subgroups and inner automorphisms are preserved by surjections of metabelian groups, the functoriality of the other groups follows from that of $\mathrm{IAut}(G)$. □

In sections §4.4, §4.6 below, we will give homological interpretations to the groups $\mathrm{IOut}_1'(G), \mathrm{IOut}_1(G)$.

4.4 Koszul homology and the structure of $\mathrm{Epi}(M, G)/\mathrm{Inn}'(G)$

By 4.6 and 4.9, the map

$$\xi' \times \kappa_c : \mathrm{Epi}(M, G)/\mathrm{Inn}'(G) \to \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$$

is a torsor under $\mathrm{IOut}_1'(G)$. In this section we will show that $\mathrm{IOut}_1'(G)$ can be identified with a certain homology group, and give criteria for it to vanish, or equivalently, for the map $\xi' \times \kappa_c$ to be a bijection.

4.4.1 $\mathrm{IOut}_1'(G)$ via continuous cohomology

Let G be a 2-generated profinite metabelian group, and let $\gamma \in \mathrm{IAEnd}(G)$. Recall from §3.1 that the map $\delta_\gamma : G \to G'$ defined by $\delta_\gamma(g) = \gamma(g)g^{-1}$ is a continuous 1-cocycle. If $Z^1(G, G')$ denotes the group of (continuous) cocycles, the map $\gamma \mapsto \delta_\gamma$ defines a continuous bijection of sets $\mathrm{IAEnd}(G) \cong_{\underline{\textbf{Sets}}} Z^1(G, G')$. Under this bijection, composition in $\mathrm{IAEnd}(G)$ becomes twisted pointwise multiplication in $Z^1(G, G')$: $\delta_{\gamma\circ\gamma'}(g) = \delta_\gamma(g)\delta_{\gamma'}(g)^{\det(\gamma)}$ for all $g \in G$.

For $\gamma \in \mathrm{IAut}_1(G)$, $\delta_\gamma : G \to G'$ factors through G^{ab}, and $\gamma \mapsto \delta_\gamma$ defines an isomorphism of groups

$$\mathrm{IAut}_1(G) \xrightarrow{\sim} Z^1(G^{\mathrm{ab}}, G'). \tag{14}$$

The subgroup of 1-coboundaries $B^1(G^{\mathrm{ab}}, G') \subset Z^1(G^{\mathrm{ab}}, G')$ consists of functions $\delta_z : G^{\mathrm{ab}} \to G'$ (for $z \in G^{\mathrm{ab}}$) defined by $\delta_z(a) = z^{a-1}$. The first cohomology of $G^{\mathrm{ab}} \circlearrowleft G'$ is [Tat76, §2]

$$H^1(G^{\mathrm{ab}}, G') := Z^1(G^{\mathrm{ab}}, G')/B^1(G^{\mathrm{ab}}, G').$$

Proposition 4.12. *Let G be a 2-generated profinite metabelian group.*

(a) The isomorphism $\delta : \mathrm{IAut}_1(G) \xrightarrow{\sim} Z^1(G^{\mathrm{ab}}, G')$ *induces an isomorphism* $\mathrm{IOut}'_1(G) \cong H^1(G^{\mathrm{ab}}, G')$.

(b) For any basis $c \in M'$,

$$\xi' \times \kappa_c : \mathrm{Epi}(M, G)/\operatorname{Inn}'(G) \longrightarrow \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')$$

is a torsor under $H^1(G^{\mathrm{ab}}, G')$.

Proof. For $z \in G'$, conjugation by z^{-1} sends $g \mapsto z^{-1}gz = z^{\overline{g}-1}g$, which is exactly the IA-automorphism corresponding to the coboundary $\delta_z : G^{\mathrm{ab}} \to G'$ sending $a \mapsto z^{a-1}$. This proves (a). Part (b) follows from 4.9. □

Remark 4.13. A point of concern with the proposition is that there are some technical issues with cohomology with profinite coefficient modules; for example, the category of profinite $\widehat{\mathbb{Z}}[\![G]\!]$-modules generally does not have enough injectives, so it is unclear if continuous cohomology is the right derived functor of the G-invariants functor $M \mapsto M^G$ (there is no problem if G is finite).[10] In any case, there is a homological interpretation of $H^1(G^{\mathrm{ab}}, G') \cong \mathrm{IOut}'_1(G)$, which is easier to work with. Note that the category of profinite $\widehat{\mathbb{Z}}[\![G]\!]$-modules always has enough projectives, so there is a well behaved theory of homology with profinite coefficients, given as the left derived functor of the coinvariants $M \mapsto M_G$. For more details, see [RZ10, §5-6].

4.4.2 $\mathrm{IOut}'_1(G)$ via Koszul homology

Let G be a profinite 2-generated metabelian group. Let $g_1, g_2 \in G$ be generators, with images $\overline{g}_1, \overline{g}_2 \in G^{\mathrm{ab}}$. Then any $\alpha \in \mathrm{IAEnd}(G)$ sends $g_i \mapsto \delta_\alpha(\overline{g_i})g_i$. Let λ denote the map (of sets)

$$\begin{array}{rcl} \lambda = \lambda_{g_1,g_2} : \mathrm{IAEnd}(G) & \longrightarrow & G' \times G' \\ \alpha & \mapsto & (\delta_\alpha(\overline{g_1}), \delta_\alpha(\overline{g_2})) \end{array} \tag{15}$$

Proposition 4.14. *The map* λ *is a continuous bijection. If* $\lambda(\alpha) = (z_1, z_2)$ *and* $\lambda(\beta) = (w_1, w_2)$, *then in additive notation for* G', *we have the composition formula*

$$\lambda(\alpha \circ \beta) = (z_1 + \det(\alpha) \cdot w_1, z_2 + \det(\alpha) \cdot w_2). \tag{16}$$

In particular, λ *restricts to an injective homomorphism* $\mathrm{IAut}_1(G) \to G' \times G'$.

Remark 4.15. A consequence of the bijectivity of λ is that for any $(z_1, z_2) \in G' \times G'$, there is a unique 1-cocycle $\gamma_{z_1,z_2} \in Z^1(G, G')$ with $\gamma_{z_1,z_2}(g_i) = z_i$.

Proof. Continuity, injectivity, and the composition formula are easy to check. To see that λ is surjective, lift g_1, g_2 to generators x_1, x_2 of M. Then for any $(z_1, z_2) \in G' \times G'$, we lift z_1, z_2 to elements $\tilde{z}_1, \tilde{z}_2 \in M'$. The map $(x_1, x_2) \mapsto (\tilde{z}_1 x_1, \tilde{z}_2 x_2)$ defines an IA-endomorphism of M which by 3.6 descends to an IA-endomorphism $\alpha \in \mathrm{IAut}_1(G)$ satisfying $\lambda(\alpha) = (z_1, z_2)$. □

For $\alpha \in \mathrm{IAut}(G)$ with $\lambda(\alpha) = (z_1, z_2) \in G' \times G'$, using the relation $gz = z^{\overline{g}}g$ (for $z \in G', g \in G$), we have

$$\alpha([g_1, g_2]) = z_1 g_1 z_2 g_2 g_1^{-1} z_1^{-1} g_2^{-1} z_2^{-1} = z_1^{1-\overline{g}_2} z_2^{\overline{g}_1 - 1}[g_1, g_2]$$

Since $[g_1, g_2]$ generates G' as a $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module, by (8) we find that $\alpha \in \mathrm{IAut}_1(G)$ if and only if we have (using additive notation for G')

$$(1 - \overline{g}_2) \cdot z_1 + (\overline{g}_1 - 1) \cdot z_2 = 0$$

If $\alpha \in \mathrm{IAut}_1(G)$ is given by conjugation by an element $c^{-1} \in G'$, then $z_i g_i = c^{-1} g_i c = c^{\overline{g}_i - 1} g_i$, so written additively in this case we have $z_i = (\overline{g}_i - 1) \cdot c$. This implies that $\mathrm{IOut}'_1(G) = \mathrm{IAut}_1(G)/\operatorname{Inn}'(G)$ is precisely the first homology of the Koszul complex of $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-modules (with terms in homological degrees 2,1,0)

$$\mathrm{Kos}_\bullet(g_1, g_2) : \quad G' \xrightarrow{d_2} G' \times G' \xrightarrow{d_1} G' \tag{17}$$

[10] In our situation this is likely ok, using the work of Boggi and Cook, see Appendix 7.2.

where the maps are given by (using additive notation)

$$\begin{array}{rrcl} d_2: & z & \mapsto & ((\overline{g}_1-1)z, (\overline{g}_2-1)z) \\ d_1: & (z_1,z_2) & \mapsto & (1-\overline{g}_2)z_1 + (\overline{g}_1-1)z_2 \end{array}$$

Note that the maps d_1, d_2 depend only on the images of g_1, g_2 in G^{ab}.[11] Thus, to construct this Koszul complex, one only needs to know the canonical representation of G - one does not need to know the particular extension of G^{ab} by G' that is realized by G.

In the case $G = M$ with generators x_1, x_2, the image of d_1 is $I_A M'$, so $M'/d_1(M') \cong \widehat{\mathbb{Z}}$ (with trivial A-action). In this case we may extend the associated Koszul complex $\mathrm{Kos}_\bullet(x_1,x_2)$ to obtain

$$0 \longrightarrow M' \xrightarrow{d_2} M' \times M' \xrightarrow{d_1} M' \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0 \tag{18}$$

The following observation implies that the Koszul complex computes group homology:

Proposition 4.16. *The complex* (18) *is a free $\widehat{\mathbb{Z}}[\![A]\!]$-module resolution of $\widehat{\mathbb{Z}}$.*

Proof. Since M' is a free $\widehat{\mathbb{Z}}[\![A]\!]$-module of rank 1, this follows immediately from Corollary 3.15. □

Theorem 4.17. *Let x_1, x_2 be generators of M, and let $\pi : M \to G$ be a surjection, inducing $\pi^{\mathrm{ab}} : A \to G^{\mathrm{ab}}$. Let $H_i(A, G')$ denote the ith group homology relative to the $\widehat{\mathbb{Z}}[\![A]\!]$-module structure on G induced by π^{ab}. Let $J_G := \mathrm{Ann}_{\widehat{\mathbb{Z}}[\![A]\!]}(G')$. We have*

- *(a) $H_i(A,G') \cong H_i(\mathrm{Kos}_\bullet(\pi(x_1),\pi(x_2))) \cong \mathrm{Tor}_i^{\widehat{\mathbb{Z}}[\![A]\!]}(\widehat{\mathbb{Z}}[\![A]\!]/I_A, \widehat{\mathbb{Z}}[\![A]\!]/J_G)$ for any i,*
- *(b) $H_0(A,G') = G'_A = G'_{G^{\mathrm{ab}}} = H_0(G^{\mathrm{ab}}, G')$,*
- *(c) $H_1(A,G') \cong \mathrm{IOut}'_1(G) \cong H^1(G^{\mathrm{ab}}, G')$,*
- *(d) $H_2(A,G') \cong G' \cap Z(G) \cong H^0(G^{\mathrm{ab}}, G')$,*
- *(e) $H_i(A,G') = 0$ for $i \notin \{0,1,2\}$, and*
- *(f) when $G = M$ we have*
$$H_0(A,M') = \widehat{\mathbb{Z}} \quad \textit{and} \quad H_1(A,M') = H_2(A,M') = 0.$$

In particular the homology groups $H_i(A,G'), H_i(\mathrm{Kos}_\bullet(\pi(x_1),\pi(x_2))$ only depend on the $\widehat{\mathbb{Z}}[\![G^{\mathrm{ab}}]\!]$-module structure of G', and are independent of the choice of surjection π or generators of M or G.

Remark 4.18. For a 2-generated profinite metabelian group G, we will often write $H_i(A, G')$ without mentioning the choice of surjection $\pi : M \to G$. By the theorem, this is not ambiguous.

Proof. Part (b) is the definition of H_0. Let a_1, a_2 be the images of x_1, x_2 in A. Note that $\mathrm{Kos}_\bullet(\pi(x_1),\pi(x_2)) = \mathrm{Kos}_\bullet(x_1,x_2) \widehat{\otimes}_{\widehat{\mathbb{Z}}[\![A]\!]} G'$, so $H_i(A,G') = \mathrm{Tor}_i^{\widehat{\mathbb{Z}}[\![A]\!]}(\widehat{\mathbb{Z}}, G') = \mathrm{Tor}_i^{\widehat{\mathbb{Z}}[\![A]\!]}(\widehat{\mathbb{Z}}[\![A]\!]/I_A, \widehat{\mathbb{Z}}[\![A]\!]/J_G) = H_i(\mathrm{Kos}_\bullet(G', \overline{g}_1, \overline{g}_2))$ by Lemma 4.16. This immediately implies (a) and (e), and the discussion preceding Theorem 4.16 together with 4.12 implies (c). Next, we have $H_2(A,G') \cong H_2(\mathrm{Kos}_\bullet(G,\pi,a_1,a_2))$ which consists of the elements of G' fixed by G^{ab}, which is just $H^0(G^{\mathrm{ab}}, G') = G' \cap Z(G)$, which proves (d). The description of $H_i(A, M')$ follows from Proposition 4.16. □

[11] We use g_1, g_2 in the notation for convenience, since it simultaneously encodes $\overline{g}_1, \overline{g}_2, G$ as well as G'.

4.5 Explicit coeffaceability of $H_1(A, G')$ by finite modules

Recall the groups $M_{n,m} = \langle z_1, z_2 | z_1^n = z_2^n = [z_1, z_2]^m = 1\rangle$, defined in §3.2. From Proposition 3.8, we have

$$R_{n,m} := R_{M_{n,m}} \cong \widehat{\mathbb{Z}}[\![A]\!]/\langle m, \sum_{i=0}^{n-1} a_1^i, \sum_{i=0}^{n-1} a_2^i\rangle$$

In this section we will show that for any 2-generated finite metabelian group G, there are integers n, m such that there is a surjection $M_{n,m} \to G$ which induces the zero map $H_1(A, M'_{n,m}) \to H_1(A, G')$.

For $n \mid n'$, there is a natural surjection $M_{n',m} \to M_{n,m}$ respecting canonical generators. For $x \in M_{n',m}$, let $\bar{x}$ denote its image in $M_{n,m}$.

Proposition 4.19. *Let $n, m \in \mathbb{Z}_{\geq 1}$. The natural map $f : M_{nm,m} \to M_{n,m}$ induces the zero map*

$$H_1(A, f) : H_1(A, M'_{nm,m}) \xrightarrow{0} H_1(A, M_{n,m})$$

In particular, f induces the zero map $\mathrm{IOut}'_1(M_{nm,m}) \to \mathrm{IOut}'_1(M_{n,m})$.

Before we give the proof, we give an alternative statement of the proposition:

Corollary 4.20. *Let $(g_1, g_2), (g'_1, g'_2) \in M_{n,m}$ be two generating pairs with $[g_1, g_2]$ conjugate to $[g'_1, g'_2]$. If there exist lifts $(\tilde{g}_1, \tilde{g}_2), (\tilde{g}'_1, \tilde{g}'_2)$ to $M_{nm,m}$ such that*

(a) $(\tilde{g}_1, \tilde{g}_2)$ and $(\tilde{g}'_1, \tilde{g}'_2)$ have the same images in $M^{\mathrm{ab}}_{nm,m} \cong (\mathbb{Z}/nm\mathbb{Z})^2$, and

(b) $[\tilde{g}_1, \tilde{g}_2]$ is conjugate to $[\tilde{g}'_1, \tilde{g}'_2]$ in $M_{nm,m}$.

Then $(g_1, g_2), (g'_1, g'_2)$ are (simultaneously) conjugate in $M_{n,m}$.

Proof. Possibly conjugating $(\tilde{g}'_1, \tilde{g}'_2)$, we may assume that $[\tilde{g}_1, \tilde{g}_2] = [\tilde{g}'_1, \tilde{g}'_2]$. Proposition 4.14 then implies that there is a unique IA-automorphism mapping α $(\tilde{g}_1, \tilde{g}_2)$ to $(\tilde{g}'_1, \tilde{g}'_2)$. By Proposition 4.19, α descends to an inner automorphism of $M_{n,m}$, so (g_1, g_2) is conjugate to (g'_1, g'_2). □

Proof of Proposition 4.19. By Theorem 4.17(a), we wish to show that the map

$$\mathrm{Kos}_\bullet(f) : \mathrm{Kos}_\bullet(M_{nm,m}, z_1, z_2) \longrightarrow \mathrm{Kos}_\bullet(M_{n,m}, z_1, z_2)$$

induces the zero map on first homology. This map can be described as the map on total complexes induced by the natural map of double complexes in homological bidegree $\{0, 1\}^2$:

$$\begin{tikzcd} R_{nm,m} \arrow[r, "a_2-1"] & R_{nm,m} & & R_{n,m} \arrow[r, "a_2-1"] & R_{n,m} \\ & & \longrightarrow & & \\ R_{nm,m} \arrow[uu, "a_1-1"] \arrow[r, "a_2-1"'] & R_{nm,m} \arrow[uu, "a_1-1"'] & & R_{n,m} \arrow[uu, "a_1-1"] \arrow[r, "a_2-1"'] & R_{n,m} \arrow[uu, "a_1-1"'] \end{tikzcd} \tag{19}$$

For any integer $k \geq 1$, let $R_k := \mathbb{Z}[a_1, a_2]/(1 + a_1 + \cdots + a_1^{k-1}, 1 + a_2 + \cdots + a_2^{k-1})$, so $R_{k,\ell} = R_k/\ell R_k$. Then the morphism (19) is just the reduction mod m of the "same" map between double complexes:

$$\begin{tikzcd} R_{nm} \arrow[r, "a_2-1"] & R_{nm} & & R_{n} \arrow[r, "a_2-1"] & R_{n} \\ & & \longrightarrow & & \\ R_{nm} \arrow[uu, "a_1-1"] \arrow[r, "a_2-1"'] & R_{nm} \arrow[uu, "a_1-1"'] & & R_{n} \arrow[uu, "a_1-1"] \arrow[r, "a_2-1"'] & R_{n} \arrow[uu, "a_1-1"'] \end{tikzcd} \tag{20}$$

Let $S_k := \mathbb{Z}[a]/(1 + a + \cdots + a^{k-1})$, then the total complexes associated to the double complexes of (20) are isomorphic to the tensor squares of $S_{nm} \xrightarrow{a-1} S_{nm}$ (in degrees $0, 1$), and similarly with $S_n \to S_n$. Since $S_k \xrightarrow{a-1} S_k$

is a $\mathbb{Z}$-free resolution of $\mathbb{Z}/k$, it is homotopy equivalent to the simpler complex $\mathbb{Z} \overset{k}{\to} \mathbb{Z}$. The morphism of complexes

$$(S_{nm} \xrightarrow{a-1} S_{nm}) \quad \to \quad (S_n \xrightarrow{a-1} S_n) \tag{21}$$

whose tensor squares induce (20) induces the natural map $\mathbb{Z}/nm \twoheadrightarrow \mathbb{Z}/n$. Therefore, by the "homotopy functoriality" of projective resolutions [Mat89, p278], (21) is homotopy equivalent to any morphism of complexes $(\mathbb{Z} \overset{nm}{\to} \mathbb{Z}) \to (\mathbb{Z} \overset{n}{\to} \mathbb{Z})$ inducing $\mathbb{Z}/nm \to \mathbb{Z}/n$ on cokernels. In particular, since the desired result is about homology, we may replace (21) with the simpler morphism

$$(\mathbb{Z} \xrightarrow{nm} \mathbb{Z}) \quad \xrightarrow{(m,1)} \quad (\mathbb{Z} \xrightarrow{n} \mathbb{Z})$$

Taking tensor squares and reducing mod m, the map on homology induced by $\mathrm{Kos}_\bullet(f)$ (equivalently, by (19)) can thus be identified with the map on homology induced by

$$\begin{tikzcd} & & \mathbb{Z}/m \arrow[r, "nm"] & \mathbb{Z}/m & & \mathbb{Z}/m \arrow[r, "n"] & \mathbb{Z}/m \\ \left[\begin{smallmatrix} m & 1 \\ m^2 & m \end{smallmatrix}\right] & : & & & \longrightarrow & & \\ & & \mathbb{Z}/m \arrow[uu, "nm"] \arrow[r, "nm"'] & \mathbb{Z}/m \arrow[uu, "nm"'] & & \mathbb{Z}/m \arrow[uu, "n"] \arrow[r, "n"'] & \mathbb{Z}/m \arrow[uu, "n"'] \end{tikzcd} \tag{22}$$

Since this map is clearly 0 on 1-chains of the total complex, this completes the proof. □

4.6 The structure of $\mathrm{Epi}^{\mathrm{ext}}(M, G) = \mathrm{Epi}(M, G)/\mathrm{Inn}(G)$

In this section we extend the results of §4.4 to the case where we work modulo $\mathrm{Inn}(G)$ instead of $\mathrm{Inn}'(G)$. Let G be a 2-generated profinite metabelian group. In this case by 4.6, we find that

$$\overline{\xi} : \mathrm{Epi}^{\mathrm{ext}}(M, G) \longrightarrow \mathrm{Epi}(M, G^{\mathrm{ab}})$$

is a torsor under $\mathrm{IOut}(G) = \mathrm{IAut}(G)/\mathrm{Inn}(G)$. Accordingly, for any $\widehat{\mathbb{Z}}[\![A]\!]$-basis $c \in M'$, the map

$$\overline{\xi} \times \kappa_c : \mathrm{Epi}^{\mathrm{ext}}(M, G) \longrightarrow \mathrm{Epi}(M, G^{\mathrm{ab}}) \times \mathrm{Gens}(G')/\mathrm{Inn}(G)$$

is a torsor under $\mathrm{IOut}_1(G)$. In certain cases we will have $\mathrm{IOut}_1(G) \cong \mathrm{IOut}_1'(G) \cong H_1(A, G')$:

Proposition 4.21. *Let G be a 2-generated profinite metabelian group. Consider the following conditions on G*

(a) G is a split extension of G^{ab} by G'.

(b) The canonical representation $\rho_G : G^{\mathrm{ab}} \to R_{G,\epsilon=1}^{\times}$ is faithful.

Then (a) implies (b), and in both cases, we have $\mathrm{IOut}_1(G) \cong \mathrm{IOut}_1'(G) \cong H_1(A, G')$.

Proof. Suppose G is a split extension of G^{ab} by G'. We will show that any inner automorphism of G which acts trivially on G' must lie in $\mathrm{Inn}'(G)$. Indeed, any $g, h \in G$ can be written as $g = za, h = wb$ with $z, w \in G'$ and a, b in the split image of G^{ab}. Then g centralizes G' if and only if a does, in which case we have

$$ghg^{-1} = zawba^{-1}z^{-1} = zawa^{-1}bz^{-1} = zwbz^{-1}$$

so conjugation by g is the same as conjugation by $z \in G'$, which shows that (a) implies (b). The isomorphism $\mathrm{IOut}_1'(G) \cong H_1(A, G')$ is Theorem 4.17. Finally, by (13), $\mathrm{IOut}_1(G)$ is the quotient of $H_1(A, G')$ by $\ker(\rho_G)/\mathrm{ab}(Z(G))$, so we find that in both cases $\mathrm{IOut}_1(G) = H_1(A, G')$. □

Proposition 4.22. *If G_1, G_2 are profinite 2-generated metabelian groups with isomorphic canonical representations, then $\mathrm{IOut}_1(G_1) \cong \mathrm{IOut}_1(G_2)$.*

Proof. Let $G = G_1$. Since the Koszul complex depends only on the canonical representation of G, it will suffice to show that one can compute $\mathrm{IOut}_1(G) = \mathrm{IAut}_1(G)/\operatorname{Inn}_1(G)$ from a Koszul complex for G. Let $\overline{g}_1, \overline{g}_2 \in G^{\mathrm{ab}}$ be generators. By Gaschütz' lemma [RZ10, Proposition 2.5.4], we may find generators g_1, g_2 of G lifting $\overline{g}_1, \overline{g}_2$. Let $c := [g_1, g_2]$. Then we know that $\mathrm{IAut}_1(G)$ is isomorphic to the group of Koszul 1-cycles $Z^1(\mathrm{Kos}_\bullet(g_1, g_2))$.

We wish to show that the subgroup $\operatorname{Inn}_1(G)$ can be described purely in the language of the canonical representation and the Koszul complex. This can be done using the map $\lambda = \lambda_{g_1,g_2}$ of (15). Explicitly, for $g \in G$, let inn_g be the inner automorphism $x \mapsto gxg^{-1}$. Writing G' in additive notation, note that $\lambda(\mathrm{inn}_{g_1}) = (0, c)$, and $\lambda(\mathrm{inn}_{g_2}) = (-c, 0)$. Using the composition formula (16), we compute:

$$\begin{aligned}
\lambda(\mathrm{inn}_{g_1^n}) &= \big(0, (1 + \overline{g}_1 + \overline{g}_1^2 + \cdots + \overline{g}_1^{n-1}) \cdot c\big) \\
\lambda(\mathrm{inn}_{g_2^n}) &= \big(-(1 + \overline{g}_2 + \overline{g}_2^2 + \cdots + \overline{g}_2^{n-1}) \cdot c, 0\big) \\
\lambda(\mathrm{inn}_{g_1^n g_2^m}) &= (-\overline{g}_1^n(1 + \overline{g}_2 + \overline{g}_2^2 + \cdots + \overline{g}_2^{m-1}) \cdot c, (1 + \overline{g}_1 + \overline{g}_1^2 + \cdots + \overline{g}_1^{n-1}) \cdot c)
\end{aligned}$$

Letting $\lambda(n, m)$ denote the final expression, $\lambda(n, m)$ depends only on the choice of generators $\overline{g}_1, \overline{g}_2$ of G^{ab}, so $\lambda(n, m)$ depend only on the canonical representation. It follows that under λ, elements of $\operatorname{Inn}_1(G)$ correspond to precisely the elements

$$\overline{\{\zeta \in \mathrm{Kos}_1(g_1, g_2) \mid \zeta = \lambda(n, m) \text{ for some } n, m \in \mathbb{Z}\}} \cap Z^1(\mathrm{Kos}_\bullet(g_1, g_2))$$

where $\overline{\{\cdots\}}$ denotes closure. This gives the desired result. □

Remark 4.23. Note that the two propositions above do not necessarily imply that $\mathrm{IOut}_1(G) \cong H_1(A, G')$ for any 2-generated profinite metabelian group. This is because not every extension of G^{ab} by G' (realizing the representation ρ_G) actually has abelianization G^{ab}.

This leads to the question of determining whether or not a profinite extension G of a profinite abelian group B by a profinite abelian group N satisfies $G^{\mathrm{ab}} = B$ (equivalently $G' = N$). This will also be relevant in §4.7.

Proposition 4.24. *Let G be a 2-generated profinite group extension of a 2-generated profinite abelian group B by a profinite B-module N. Let $I_B \subset \widehat{\mathbb{Z}}[\![B]\!]$ be the augmentation ideal, and let $N_B := N/I_BN$ be the module of B-coinvariants. Then I_BN is normal inside G, and G/I_BN is a central extension of B by N_B. The commutator map $B \times B \to N$ sending $(b, b') \mapsto [b, b']$ induces a homomorphism*

$$[*, *] : B \mathbin{\widehat{\wedge}} B \longrightarrow N_B$$

where $B \mathbin{\widehat{\wedge}} B$ denotes the quotient of the completed tensor product $B \mathbin{\widehat{\otimes}} B$ by the subgroup generated by $\{b \otimes b \mid b \in B\}$ (i.e., the "completed exterior square"). The following are equivalent

(a) G satisfies $G^{\mathrm{ab}} = B$ and $G' = N$.

(b) $(G/I_BN)' = N_B$

(c) The homomorphism $[*, *] : B \mathbin{\widehat{\wedge}} B \longrightarrow N_B$ is surjective.

Proof. First suppose that G is a *central* extension of B by N, then its commutator map $[*, *] : G \times G \longrightarrow G' \subset N$ factors through a bilinear map $[*, *] : B \times B \longrightarrow N$, and since it is alternating, it further factors through a *homomorphism*

$$[*, *] : B \mathbin{\widehat{\wedge}} B \longrightarrow N$$

In this case we find that $G^{\mathrm{ab}} = B$ if and only if this commutator map is surjective. In the general case, since N is abelian, and $I_BN \le N$ is a $\widehat{\mathbb{Z}}[\![B]\!]$-submodule, it follows that $I_BN \subset G$ is normal and G/I_BN is a central extension of B by N_B, so $[*, *] : B \mathbin{\widehat{\wedge}} B \to N_B$ is a homomorphism. Note that since $I_BN \subset N \subset G'$, the map $G \to G/I_BN$ induces an isomorphism on abelianizations. Thus

$$G' = N \iff G^{\mathrm{ab}} = B \iff (G/I_BN)^{\mathrm{ab}} = B \iff (G/I_BN)' = N_B \tag{23}$$

Thus (a) is equivalent to (b). Since $(G/I_BN)' \subset N_B$, (c) implies (b); the converse holds because $[*, *]$ is a homomorphism, so (b) $\iff$ (c). □

4.7 Commutator rigidity

Definition 4.25. Let G be a 2-generated profinite metabelian group. We say that G is *commutator rigid* (or just rigid) if $\mathrm{IOut}_1(G) = 0$. We say that G is *strictly rigid* if $H_1(A, G') = 0$.

As explained in the introduction, the arithmetic and geometric structure of $\mathcal{M}(G)$ is particularly simple when G is a rigid group. In this section we give criteria for rigidity, and compute $\mathrm{IOut}_1(G), H_1(A, G')$ for various families of 2-generated finite metabelian groups.

Proposition 4.26. *Let G be a profinite 2-generated metabelian group. Fixing a surjection $\pi : M \to G$ and using the associated $\widehat{\mathbb{Z}}[\![A]\!]$-module structure on G', let $J_G := \mathrm{Ann}_{\widehat{\mathbb{Z}}[\![A]\!]}(G')$. Then we have*

(a) For all $i \geq 0$, $H_i(A, G')$ is annihilated by both I_A and J_G.

(b) $H_1(A, G')$ is a subquotient of $(G'_{G^{\mathrm{ab}}})^2$, and $H_2(A, G')$ is a subquotient of $G'_{G^{\mathrm{ab}}} = H_0(A, G')$.

(c) $G'_{G^{\mathrm{ab}}}$ is a quotient of the completed exterior square $G^{\mathrm{ab}} \mathbin{\widehat{\wedge}} G^{\mathrm{ab}}$, and hence is procyclic.

(d) $H_1(A, G') \cong \frac{I_A \cap J_G}{I_A J_G}$.

This immediately implies

Corollary 4.27. *If $G'_{G^{\mathrm{ab}}} = 0$, or if $G^{\mathrm{ab}} \mathbin{\widehat{\wedge}} G^{\mathrm{ab}}$ has order coprime to $|G'|$, then $H_i(A, G') = 0$ for all $i \geq 0$.*

Proof of Proposition 4.26. Part (a) follows from the Tor-theoretic description of $H_i(A, G')$ given by Theorem 4.17(a). By the Koszul theoretic description of $H_i(A, G')$ given by the same result, $H_1(A, G')$ is a subquotient of $G' \times G'$, and $H_0(A, G'), H_2(A, G')$ are subquotients of G'. Since they by part (a) they are killed by $I_A + J_G$, since $G'_{G^{\mathrm{ab}}} \cong \widehat{\mathbb{Z}}[\![A]\!]/\langle I_A, J_G\rangle$, part (b) follows. Part (c) follows from Proposition 4.24.

For (d), the exact sequence of $\widehat{\mathbb{Z}}[\![A]\!]$-modules

$$0 \longrightarrow J_G \longrightarrow \widehat{\mathbb{Z}}[\![A]\!] \longrightarrow \widehat{\mathbb{Z}}[\![A]\!]/J_G \longrightarrow 0$$

induces a long exact sequence of $H_1(A, -)$, the first five terms of which are

$$\underbrace{H_1(A, \widehat{\mathbb{Z}}[\![A]\!])}_{=0} \longrightarrow \underbrace{H_1(A, \widehat{\mathbb{Z}}[\![A]\!]/J_G)}_{\cong H_1(A,G')} \longrightarrow J_G \otimes \widehat{\mathbb{Z}}[\![A]\!]/I_A \xrightarrow{f} \widehat{\mathbb{Z}}[\![A]\!]/I_A \longrightarrow \widehat{\mathbb{Z}}[\![A]\!]/\langle I_A, J_G\rangle \longrightarrow 0$$

Thus $H_1(A, G') \cong \ker(f) = \frac{I_A \cap J_G}{I_A J_G}$. □

Remark 4.28. Let $\pi : M \to G$ be a surjection. Then $H_1(A, G') = 0$ if and only if π induces a surjection $0 = H_1(A, M') \twoheadrightarrow H_1(A, G')$. By Theorem 4.17(c), using (13) and Remark 4.5, this is equivalent to the surjectivity of $\mathrm{IOut}'(M) \to \mathrm{IOut}'(G)$, or equivalently the surjectivity of $\mathrm{IAut}(M) \to \mathrm{IAut}(G)$. Thus the failure of strict rigidity is precisely the failure of surjectivity for $\mathrm{IAut}(M) \to \mathrm{IAut}(G)$. Note that every IA-automorphism of G can be lifted to an IA-endomorphism of M (by Proposition 3.5), or to an automorphism of M (by Gaschütz's lemma); the issue is that the lifting IA-endomorphism may not be an automorphism, and the lifting automorphism may not be IA.

Example 4.29 (Dihedral groups)**.** The dihedral group D_{2n} is the semidirect product of $\mu_2 := \{\pm 1\}$ by $\mathbb{Z}/n$ acting by inversion. If n is odd, then $D_{2n}^{\mathrm{ab}} = \mu_2$ is cyclic, and hence by Corollary 4.27, D_{2n} is strictly rigid in this case. If n is even, then $D'_{2n} = 2\mathbb{Z}/n\mathbb{Z}$ is cyclic of order $n/2$, $Z(D_{2n}) = \{[0], [n/2]\} \leq D'_{2n}$, and $D_{2n}^{\mathrm{ab}} \cong \mu_n \times \{[0] \mod D'_{2n}, [1] \mod D'_{2n}\}$, where $[x]$ denotes the class of $x \mod n$. In this case if $n/2$ is odd, then $D_{2n}^{\mathrm{ab}}, D'_{2n}$ have coprime orders and hence again we find D_{2n} is strictly rigid. If $n/2$ is even, then the Koszul complex (relative to the generators $(-1, [1])$ of D_{2n}^{ab} becomes:

$$2\mathbb{Z}/n \xrightarrow{d_2} 2\mathbb{Z}/n \times 2\mathbb{Z}/n \xrightarrow{d_1} 2\mathbb{Z}/n$$

where $d_2(r) = (-2r, 0)$, and $d_1(r_1, r_2) = -2r_2$. From this we get $H_1(A, D'_{2n}) = \mathbb{Z}/2 \times \mathbb{Z}/2$. Since $[1] \in D_{2n}^{\mathrm{ab}}$ acts trivially on D'_{2n}, by (13) we find that $\mathrm{IOut}_1(D_{2n}) \cong \mathbb{Z}/2$, so D_{2n} is not rigid in this case.

Example 4.30 (The groups $M_{n,m}$)**.** Let $M_{n,m}$ be the groups defined in §3.2, with canonical generators z_1, z_2. We will calculate $H_i(A, M_{n,m})$ using the Koszul complex.

Since the case $n = 1$ is trivial, we assume $n \geq 2$. Let $R_{n,m} := (\mathbb{Z}/m)[a_1, a_2]/(1 + a_1 \cdots + a_1^{n-1}, 1 + a_2 \cdots + a_2^{n-1})$ as in Proposition 3.8, so $R_{n,m} \cong M'_{n,m}$ as $M^{\mathrm{ab}}_{n,m}$-modules. We wish to calculate the homology of the Koszul complex (see (17))

$$\mathrm{Kos}_\bullet(z_1, z_2) : R_{n,m} \longrightarrow R_{n,m} \times R_{n,m} \longrightarrow R_{n,m}$$

Write $S_n := \mathbb{Z}[a]/(1 + a + \cdots + a^{n-1})$, and let $C_\bullet$ be the complex $S_n \xrightarrow{a-1} S_n$. As in Proposition 4.19, the Koszul complex is the reduction mod m the tensor square $C_\bullet \otimes_{\mathbb{Z}} C_\bullet$. We clearly have $H_0(C_\bullet) = \mathbb{Z}/n$. Since $n \geq 2$, $a - 1$ and $1 + a + \cdots + a^{n-1}$ are distinct primes in the polynomial ring $\mathbb{Z}[a]$, which implies $H_1(C_\bullet) = 0$. Thus the Künneth formula [Wei94, Theorem 3.6.3] gives a short exact sequence

$$0 \longrightarrow 0 \longrightarrow H_1(C_\bullet^{\otimes 2}) \longrightarrow \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n) \longrightarrow 0$$

hence $H_1(C_\bullet^{\otimes 2}) = \mathbb{Z}/n$. Similarly we can compute $H_0(C_\bullet^{\otimes 2}) = \mathbb{Z}/n$, and $H_2(C_\bullet^{\otimes 2}) = 0$. Next we apply Künneth again to compute $H_1((C_\bullet)^{\otimes 2} \otimes \mathbb{Z}/m)$, where $\mathbb{Z}/m$ is placed in degree 0. Since $C_\bullet^{\otimes 2}$ consists of $\mathbb{Z}$-free modules, Künneth gives a *split* exact sequence

$$0 \longrightarrow \underbrace{H_1(C_\bullet^{\otimes 2})}_{\mathbb{Z}/n} \otimes \underbrace{H_0(\mathbb{Z}/m)}_{\mathbb{Z}/m} \longrightarrow H_1(C_\bullet^{\otimes 2} \otimes \mathbb{Z}/m) \longrightarrow \underbrace{\mathrm{Tor}_1^{\mathbb{Z}}(H_0(C_\bullet^{\otimes 2}), H_0(\mathbb{Z}/m))}_{\{x \in \mathbb{Z}/n \mid mx = 0\}} \longrightarrow 0$$

Hence we find $H_1(A, M_{n,m}) = H_1(\mathrm{Kos}_\bullet(z_1, z_2)) = H_1(C_\bullet^{\otimes 2}) = (\mathbb{Z}/d)^2$, where $d := \gcd(n, m)$. Similarly we may compute $H_0(A, M_{n,m}) = H_2(A, M_{n,m}) = \mathbb{Z}/d$. We note that in this case the homology groups are the largest possible given the restrictions provided by Proposition 4.26. This is not surprising since every finite 2-generated metabelian group is a quotient of $M_{n,m}$ for appropriate n, m. ♠♠♠ NOTE: [It is an interesting question to ask if any finite 2-generated metabelian group is a quotient of $M_{n,m}$ such that the induced map on H_1 is *surjective*.]

Example 4.31 (Central extensions are (non-strictly) rigid)**.** Let G be a 2-generated finite metabelian group which is a central extension of G^{ab} by G'. Let $\mathrm{ab} : G \to G^{\mathrm{ab}}$ be the abelianization. Then we will show that $H_1(A, G') \cong \mathrm{IOut}'_1(G) \cong G' \times G'$, $\mathrm{ab}(Z(G))$ has order $|G^{\mathrm{ab}}|/|G'|^2$, and $\mathrm{IOut}_1(G) = 0$.

Since G is a central extension, the maps in the Koszul complex $G' \to G' \times G' \to G'$ are all 0, so $H_1(A, G') = G' \times G'$. This also implies that $\mathrm{Ker}\,\rho_G = G^{\mathrm{ab}}$. By (13), showing that $\mathrm{IOut}_1(G) = 1$ is equivalent to showing that $|\mathrm{ab}(Z(G))| = |G^{\mathrm{ab}}|/|G'|^2$. Since G is a central extension, by 4.24, we have a surjective commutator map

$$[*, *] : G^{\mathrm{ab}} \wedge G^{\mathrm{ab}} \longrightarrow G'$$

which is a homomorphism, and a lifts to a central element $\tilde{a} \in Z(G)$ if and only if $[*, *](a \wedge b) = 0$ (in additive notation) for all $b \in G^{\mathrm{ab}}$. In particular G' is cyclic; let $e' := |G'|$. We claim that a lifts to a central element if and only if a is an e'th multiple in G^{ab}. Let a_1, a_2 be a basis for G^{ab}, then since $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$ is cyclic, $\mathrm{Ker}[*, *] = \langle e'(a_1 \wedge a_2) \rangle$. If a is an e'th multiple, then we may write $a = e'c_1a_1 + e'c_2a_2$ for some $c_1, c_2 \in \mathbb{Z}$, so

$$a \wedge a_1 = e'c_2(a_2 \wedge a_1) = -e'c_2(a_1 \wedge a_2), \qquad a \wedge a_2 = e'c_1(a_1 \wedge a_2)$$

so $a \wedge b \in \mathrm{Ker}[*, *]$ for any $b \in G^{\mathrm{ab}}$. Now suppose a is not an e'th multiple, then writing $a = c_1a_1 + c_2a_2$, assume without loss of generality that $c_1 \not\equiv 0 \mod e'$. Then $a \wedge a_2 = c_1(a_1 \wedge a_2) \notin \mathrm{Ker}[*, *]$, so a does not lift to a central element.

Write $G^{\mathrm{ab}} = \mathbb{Z}/n \times \mathbb{Z}/nm$ for some $n, m \in \mathbb{Z}_{\geq 1}$, then $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}} \cong \mathbb{Z}/n$, and $e' \mid n$. Since there are $\frac{n}{e'} \cdot \frac{nm}{e'}$ e'-multiples in G^{ab}, we get $|\mathrm{ab}(Z(G)| = \frac{n^2m}{e'} = \frac{|G^{\mathrm{ab}}|}{|G'|^2}$ as desired.

5 Mondromy actions and the Galois theory of $\mathcal{M}(G)$

In this section we make precise the setup needed to make the translations between algebra and geometry. The notation $\pi_1(X, x)$ will by default denote the étale fundamental group of X. Whenever it makes sense, topological fundamental groups will be denoted $\pi_1^{\mathrm{top}}(X, x)$.

5.1 Fundamental groups, inertia groups

Let K be a field with an embedding $\iota : K \hookrightarrow \mathbb{C}$. Let $\overline{K}$ be its algebraic closure inside $\mathbb{C}$. Let E be an elliptic curve over K with origin O, $E^\circ := E - O$ the punctured curve, and $E_{\overline{K}}, E^\circ_{\overline{K}}, E_{\mathbb{C}}, E^\circ_{\mathbb{C}}$ their base changes to via ι. If b is a base point, then by the Riemann existence theorem [Sza09, Theorem 5.7.4] we have an injective group homomorphism

$$\Pi_b := \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), b) \longrightarrow \pi_1(E^\circ_{\mathbb{C}}, b) \cong \pi_1(E^\circ_{\overline{K}}, b)$$

where the isomorphism is induced by ι. Letting $*^\wedge$ denote profinite completion, this injection induces an isomorphism $\widehat{\Pi_b} = \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), b)^\wedge \cong \pi_1(E^\circ_{\overline{K}}, b)$. The group Π_b is free on two generators. Let $x_1, x_2 \in \Pi_b$ be a basis with positive intersection number (a "positively oriented basis"), then the conjugacy class of $[x_1, x_2]$ can be represented by a small loop winding once clockwise around the puncture – the cyclic subgroup it generates (or its closure inside $\pi_1(E^\circ_{\overline{K}}, b)$) is called an *inertia subgroup* at O, and is well-defined up to conjugation.

Sometimes it will be convenient to take as base point a *tangential base point* at O [Del89, §15] (also see [Che21, §4.2]). Let t be a K-rational tangential base point, then we again have an injective group homomorphism

$$j : \Pi_t := \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), t) \longrightarrow \pi_1(E^\circ_{\mathbb{C}}, t) \cong \pi_1(E^\circ_{\overline{K}}, t)$$

which induces an isomorphism $\widehat{\Pi_t} \cong \pi_1(E^\circ_{\overline{K}}, t)$. However in this case $\pi_1(E^\circ_{\overline{K}}, t)$ is moreover equipped with a *canonical* inertia subgroup $\mathcal{I}_t \cong \widehat{\mathbb{Z}}$, which is topologically generated by $j([x_1, x_2])$ for some positively oriented basis x_1, x_2 of Π_t as above. In particular the subgroup of $\pi_1(E^\circ_{\overline{K}}, t)$ generated by $j([x_1, x_2])$ *does not depend on the choice of embedding* $\iota : K \hookrightarrow \mathbb{C}$. If t' is another tangential base point at O, then there is an isomorphism $\pi_1(E^\circ_{\overline{K}}, t) \xrightarrow{\sim} \pi_1(E^\circ_{\overline{K}}, t')$ which is canonical up to conjugation by $\mathcal{I}_t$ (equivalently, $\mathcal{I}_{t'}$).

5.2 Monodromy actions

The maps $E^\circ_{\overline{K}} \to E^\circ \to \operatorname{Spec} K$ induce an exact sequence of fundamental groups [Sza09, Proposition 5.6.1]

$$1 \longrightarrow \pi_1(E^\circ_{\overline{K}}, t) \longrightarrow \pi_1(E^\circ, t) \longrightarrow \mathrm{Gal}(\overline{K}/K) \longrightarrow 1 \tag{24}$$

which is split by t; from this we get an action of $\mathrm{Gal}(\overline{K}/K)$ on $\pi_1(E^\circ_{\overline{K}}, t)$. Note that while this action depends on the choice of tangential base point t, the induced outer representation

$$\rho^{\mathrm{Gal}}_{E^\circ/K} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Out}(\pi_1(E^\circ_{\overline{K}}, t))$$

is canonically determined by (24).[12] For any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and any $c \in \mathcal{I}_t \subset \pi_1(E^\circ_{\overline{K}}, t)$, we have

$$\sigma(c) = c^{\chi(\sigma)}$$

where $\chi : \mathrm{Gal}(\overline{K}/K) \longrightarrow \widehat{\mathbb{Z}}^\times$ is the cyclotomic character.

Let $\mathcal{M}(1)$ be the moduli stack of elliptic curves (over $\mathbb{Z}$). Let $\pi_1^{\mathrm{top}}(\mathcal{M}(1)_{\mathbb{C}}, E_{\mathbb{C}})$ be the topological fundamental group (of the analytification of $\mathcal{M}(1)_{\mathbb{C}}$). The universal elliptic curve over $\mathcal{M}(1)_{\mathbb{C}}$ gives rise to a *geometric monodromy representation* [BBCL22, §2.1]

$$\rho^{\mathrm{top}}_{E^\circ(\mathbb{C})} : \pi_1^{\mathrm{top}}(\mathcal{M}(1)_{\mathbb{C}}, E_{\mathbb{C}}) \longrightarrow \mathrm{Out}(\Pi_t)$$

which is an *isomorphism* onto the index 2 subgroup $\mathrm{Out}^+(\Pi_t) \leq \mathrm{Out}(\Pi_t)$ consisting of outer automorphisms which act with determinant 1 on the abelianization. Recall that the abelianization $\Pi_t \to \Pi_t^{\mathrm{ab}}$ induces an isomorphism $\mathrm{Out}^+(\Pi_t) \cong \mathrm{SL}(\Pi_t^{\mathrm{ab}})$; if we choose an isomorphism $\Pi_t^{\mathrm{ab}} \cong \mathbb{Z}^2$, then we have $\mathrm{Out}^+(\Pi_t) \cong \mathrm{SL}_2(\mathbb{Z})$ (Theorem 3.18). The group $\pi_1({}^{\mathrm{top}}(\mathcal{M}(1)_{\mathbb{C}}, E_{\mathbb{C}})$, and hence $\mathrm{Out}^+(\Pi_t)$ can be identified with the mapping class group of $E^\circ_{\mathbb{C}}$, and as such it preserves the conjugacy class of a loop winding around the puncture. That is to say,

Proposition 5.1. *Let x_1, x_2 be generators of* Π_t. *Then* $\mathrm{Out}^+(\Pi_t)$ *preserves the conjugacy class of* $c := [x_1, x_2]$.

[12] In fact if one restricts to only considering tangential base points, the action of $\mathrm{Gal}(\overline{K}/K)$ on $\pi_1(E^\circ_{\overline{K}}, t)$ is canonically determined up to conjugation by elements of $\mathcal{I}_t$.

Proof. This can also be checked algebraically: the group $\mathrm{Aut}(\Pi_t)$ is generated by the automorphisms [MKS04, §3]

$$\begin{array}{rcl} r:(x_1,x_2) & \mapsto & (x_1^{-1},x_2) \\ s:(x_1,x_2) & \mapsto & (x_2,x_1) \\ t:(x_1,x_2) & \mapsto & (x_1^{-1},x_1x_2) \end{array}$$

Each generator acts by inverting $[x_1,x_2]$ (up to conjugation), and since they all act with determinant -1 on Π_t^{ab}, 3.18 implies that $\mathrm{Out}^+(\Pi_t)$ preserves $[x_1,x_2]$. □

The two monodromy representations $\rho^{\mathrm{Gal}}_{E^\circ/K},\rho^{\mathrm{top}}_{E^\circ(\mathbb{C})}$ can be combined into a single representation as follows. The embedding $\iota: K\hookrightarrow\overline{K}\subset\mathbb{C}$ also induces an injective map

$$i:\underbrace{\pi_1^{\mathrm{top}}(\mathcal{M}(1)_{\mathbb{C}},E_{\mathbb{C}})}_{\cong\mathrm{Out}^+(\Pi_t)}\longrightarrow\pi_1(\mathcal{M}(1)_{\mathbb{C}},E_{\mathbb{C}})\cong\pi_1(\mathcal{M}(1)_{\overline{K}},E_{\overline{K}})$$

which identifies the target with the profinite completion of the source. There is a homotopy exact sequence

$$1\longrightarrow\pi_1(\mathcal{M}(1)_{\overline{K}},E_{\overline{K}})\longrightarrow\pi_1(\mathcal{M}(1)_K,E)\longrightarrow\mathrm{Gal}(\overline{K}/K)\longrightarrow 1\quad\text{[Zoo01, Corollary 6.6]}$$

which is split by the K-point of $\mathcal{M}(1)_K$ corresponding to E. In particular $\pi_1(\mathcal{M}(1)_K,E_{\overline{K}})$ is isomorphic to the semidirect product $\widehat{\mathrm{Out}^+(\Pi_t)}\rtimes\mathrm{Gal}(\overline{K}/K)$. The universal elliptic curve $\mathcal{E}\to\mathcal{M}(1)_K$ induces an exact sequence

$$1\longrightarrow\pi_1(E^\circ_{\overline{K}},t)\longrightarrow\pi_1(\mathcal{E}^\circ,t)\longrightarrow\pi_1(\mathcal{M}(1)_K,E_{\overline{K}})\longrightarrow 1$$

from which we obtain an *arithmetic monodromy representation*

$$\rho_{E^\circ/K}:\ \underbrace{\pi_1(\mathcal{M}(1)_K,E_{\overline{K}})}_{\cong\widehat{\mathrm{Out}^+(\Pi_t)}\rtimes\mathrm{Gal}(\overline{K}/K)}\longrightarrow\mathrm{Out}(\pi_1(E^\circ_{\overline{K}},t))\qquad(25)$$

whose restrictions to $\mathrm{Out}^+(\Pi_t)$ and $\mathrm{Gal}(\overline{K}/K)$ recovers $\rho^{\mathrm{top}}_{E^\circ(\mathbb{C})},\rho^{\mathrm{Gal}}_{E^\circ/K}$ respectively.

5.3 Moduli of elliptic curves with G-structures - the stacks $\mathcal{M}(G)$

Let G be a finite group. Let $\mathcal{M}(1)$ denote the moduli stack of elliptic curves over $\mathbb{Q}$ and let $M(1)$ be its coarse scheme. In [Che17] the first author studied the moduli stacks $\mathcal{M}(G)$ of "elliptic curves with G-structures". Precisely, let $\mathcal{T}_G$ be the sheafification of the functor $\mathcal{M}(1)\to\underline{\mathbf{Sets}}$ which to an elliptic curve E/S associates the set of isomorphism classes of G-torsors on $E^\circ:=E-O$ which are geometrically connected over S. Then $\mathcal{M}(G)$ is the stack over $\mathcal{M}(1)$ associated to the sheaf $\mathcal{T}_G$. Let $M(G)$ denote the coarse scheme of $\mathcal{M}(G)$. Thus an object of $\mathcal{M}(G)$ is a pair $(E/S,\alpha)$ where E is an elliptic curve over some $\mathbb{Q}$-scheme S and $\alpha\in\mathcal{T}_G(E/S)$ is a "G-structure", and morphisms of pairs are morphisms of elliptic curves respecting the G-structures. For more details, see [BBCL22, §2.2], [Che18, §2.2], or [Che21, §2.5]. Here we review some of the basic properties of $\mathcal{M}(G)$ that we will need.

(a) Let $\mathcal{M}(1)$ denote the moduli stack of elliptic curves over $\mathbb{Q}$. The map forgetting the G-structure

$$\mathfrak{f}:\mathcal{M}(G)\longrightarrow\mathcal{M}(1)$$

is *finite étale.*

(b) Let E be an elliptic curve over K, where K is as in §5.1. Let t be a base point on E° (possibly tangential), and $\Pi_t:=\pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}),t)$. The geometric fiber of $\mathfrak{f}:\mathcal{M}(G)\to\mathcal{M}(1)$ above $E_{\overline{K}}$ is in bijection with the set

$$\mathfrak{f}^{-1}(E)=\mathrm{Epi}^{\mathrm{ext}}(\pi_1(E^\circ_{\overline{K}},t),G):=\mathrm{Epi}(\pi_1(E^\circ_{\overline{K}},t),G)/\,\mathrm{Inn}(G)\cong\mathrm{Epi}^{\mathrm{ext}}(\Pi_t,G)$$

where the second bijection is induced by the isomorphism $\widehat{\Pi_t}\cong\pi_1(E^\circ_{\overline{K}},t)$. The monodromy action of $\pi_1(\mathcal{M}(1),E_{\overline{K}})\cong\widehat{\mathrm{Out}^+(\Pi_t)}\rtimes\mathrm{Gal}(\overline{K}/\mathbb{Q})$ on $\mathfrak{f}^{-1}(E)$ can be described in terms of the outer actions of the complementary subgroups $\mathrm{Gal}(\overline{K}/K)$ and $\widehat{\mathrm{Out}^+(\Pi_t)}$ in $\pi_1(\mathcal{M}(1), E_{\overline{K}})$. The action of $\mathrm{Gal}(\overline{K}/K)$ is given by the canonical outer action on $\pi_1(E^\circ_{\overline{K}}, t)$ as above. The action of $\widehat{\mathrm{Out}^+(\Pi_t)}$ is given by the tautological outer action of $\mathrm{Out}^+(\Pi_t)$ on Π_t, which defines an outer action on $\pi_1(E^\circ_{\overline{K}}, t)$ via the dense injection $\Pi_t \hookrightarrow \pi_1(E^\circ_{\overline{K}}, t)$. Finally the set of G-structures on E is in bijection with the set of $\mathrm{Gal}(\overline{K}/K)$-invariant elements of $\mathfrak{f}^{-1}(E)$.

(c) The stack $\mathcal{M}(G)$ is typically not connected. The map $\mathcal{M}(G)_{\mathbb{C}} \to \mathcal{M}(G)_{\overline{K}}$ induced by ι induces a bijection on connected components. By the Galois correspondence these connected components are in bijection with the $\mathrm{Out}^+(\Pi_t)$-orbits on $\mathrm{Epi}^{\mathrm{ext}}(\Pi_t, G)$. In particular, the (profinite completion of the) stabilizer of this action is the fundamental group of the corresponding component, and so we can construct this component explicitly as a quotient of the universal covering $\mathcal{H}$ of $\mathcal{M}(1)_{\mathbb{C}}$. Explicitly, let $x_1, x_2 \in \Pi_t$ be a positively oriented basis, using which we identify $\mathrm{Out}^+(\Pi_t) = \mathrm{SL}_2(\mathbb{Z})$. Then the component of $\mathcal{M}(G)_{\mathbb{C}}$ corresponding to the $\mathrm{Out}^+(\Pi)$-orbit of $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(\Pi_t, G)$ is isomorphic to $[\mathcal{H}/\Gamma_\varphi]$, where $\Gamma_\varphi := \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\varphi)$. Similarly $M(G)_{\mathbb{C}}$ is the disjoint union of the Riemann surfaces $\mathcal{H}/\Gamma_\varphi$.

5.4 Congruence subgroups

Recall that a subgroup $\Gamma \le \mathrm{SL}_2(\mathbb{Z})$ is *congruence* if it contains

$$\Gamma(n) := \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))$$

for some $n \ge 1$. In this case the congruence level of Γ is the minimum n for which we have $\Gamma \supset \Gamma(n)$. Let $\mathbf{F}$ be a free group of rank 2. We say that a subgroup $\Gamma \le \mathrm{Out}^+(\mathbf{F})$ is *linearly congruence* if relative to some isomorphism $\mathbf{F}^{\mathrm{ab}} \cong \mathbb{Z}^2$, Γ maps under the induced isomorphism $\mathrm{SL}(\Pi_t^{\mathrm{ab}}) = \mathrm{SL}_2(\mathbb{Z})$ to a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We note that this definition does not depend on the choice of isomorphism $\mathbf{F}^{\mathrm{ab}} \cong \mathbb{Z}^2$. This can also be characterized in another way: by the universal property of profinite completion, the canonical map $\mathrm{SL}_2(\mathbb{Z}) \hookrightarrow \mathrm{SL}_2(\widehat{\mathbb{Z}})$ factors through a surjection

$$p : \widehat{\mathrm{SL}_2(\mathbb{Z})} \longrightarrow \mathrm{SL}_2(\widehat{\mathbb{Z}})$$

The fact that there exist noncongruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ is precisely to say that p is *not injective*. The kernel of p is the intersection of the closures of congruence subgroups inside $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ and is called the "congruence kernel".[13] A subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is congruence if and only if its closure in $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ contains the congruence kernel. The linear congruence kernel of $\mathrm{Out}^+(\mathbf{F})$ is the subgroup of $\widehat{\mathrm{Out}^+(\mathbf{F})}$ corresponding to the congruence kernel of $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ under the isomorphism $\mathrm{Out}^+(\mathbf{F}) \cong \mathrm{SL}_2(\mathbb{Z})$ induced by any isomorphism $\mathbf{F}^{\mathrm{ab}} \cong \mathbb{Z}^2$.

We may apply the above discussion in the case $\mathbf{F} = \Pi_t$, where Π_t is as in §5.3. In this case we choose an isomorphism $\Pi_t^{\mathrm{ab}} \cong \mathbb{Z}^2$ defined using a positively oriented basis of Π_t, from which we get an isomorphism $\mathrm{Out}^+(\Pi_t) \cong \mathrm{SL}_2(\mathbb{Z})$.

Definition 5.2. Let G be a finite group. We say that a component $\mathcal{M} \subset \mathcal{M}(G)_{\mathbb{C}}$ is *congruence* if for some choice of base point x, the image of the map $\pi_1^{\mathrm{top}}(\mathcal{M}, x) \to \pi_1^{\mathrm{top}}(\mathcal{M}(1)_{\mathbb{C}}, E_{\mathbb{C}}) = \mathrm{Out}^+(\Pi_t)$ induced by the cover $\mathcal{M} \subset \mathcal{M}(G)_{\mathbb{C}} \to \mathcal{M}(1)_{\mathbb{C}}$ is a linearly congruence subgroup of $\mathrm{Out}^+(\Pi_t)$. The *congruence level* of $\mathcal{M}$ is congruence level of the corresponding subgroup of $\mathrm{SL}_2(\mathbb{Z})$. If $K, \overline{K}$ are as in §5.1, then we say a component of $\mathcal{M}(G)_{\overline{K}}$ is congruence if the corresponding component of $\mathcal{M}(G)_{\mathbb{C}}$ is so.

Proposition 5.3. *Let G be a finite group. Let $K, \overline{K}$ be as in §5.1. Let E be an elliptic curve over K, with tangential base point t at $O \in E$, and topological fundamental group $\Pi_t := \pi_1^{top}(E^\circ(\mathbb{C}), t)$. We have a natural action of* $\mathrm{Out}^+(\Pi_t)$ *on* $\mathrm{Epi}^{\mathrm{ext}}(\Pi_t, G) := \mathrm{Epi}(\Pi_t, G)/\mathrm{Inn}(G)$. *Since the latter is a finite set, this action extends uniquely to an action of* $\widehat{\mathrm{Out}^+(\Pi_t)}$. *The following are equivalent.*

(a) Every component of $\mathcal{M}(G)_{\overline{K}}$ is congruence.

(b) The kernel of the $\mathrm{Out}^+(\Pi_t)$*-action on* $\mathrm{Epi}^{\mathrm{ext}}(\Pi_t, G)$ *is linearly congruence.*

[13] This is a free profinite group of countably infinite rank. See [RZ10, Theorem 8.8.1] or [Mel76].

(c) The kernel of the $\widehat{\mathrm{Out}^+(\Pi_t)}$*-action on* $\mathrm{Epi}^{\mathrm{ext}}(\Pi_t, G)$ *contains the linear congruence kernel.*

Proof. Follows immediately from the description of the components of $\mathcal{M}(G)$ in §5.3. □

We chose to use the term "linearly congruence" to distinguish it from another notion of congruence subgroups:

Definition 5.4 (c.f. [BER11])**.** Let B be a finitely generated, residually finite group. For any finite index characteristic subgroup $K \leq B$, let $\Gamma[K] := \mathrm{Ker}(\mathrm{Aut}(B) \to \mathrm{Aut}(B/K))$. A subgroup of $\mathrm{Aut}(B)$ is a *congruence subgroup* if it contains $\Gamma[K]$ for some such K. We say that $\mathrm{Aut}(B)$ has the *congruence subgroup property* if every finite index subgroup of $\mathrm{Aut}(B)$ is congruence.

Let τ_{pf} denote the full profinite topology on $\mathrm{Aut}(B)$, and let τ_c denote the profinite topology generated by the finite index subgroups $\Gamma[K]$ as K ranges over finite index characteristic subgroups of B. Then $\mathrm{Aut}(B)$ satisfies the congruence subgroup property if and only if $\tau_c = \tau_{pf}$.[14] By [RZ10, Lemma 3.2.6], the congruence subgroup property for $\mathrm{Aut}(B)$ is also equivalent to the injectivity of the canonical map

$$\widehat{\mathrm{Aut}(B)} \longrightarrow \mathrm{Aut}(\widehat{B})$$

induced by the inclusion $\mathrm{Aut}(B) \hookrightarrow \mathrm{Aut}(\widehat{B})$. When $B = \mathbf{F} \cong \Pi_t$ is a free group of rank 2, a theorem of Asada [Asa01, BER11] shows that $\mathrm{Aut}(\Pi_t)$ *has the congruence subgroup property* in sense of Definition 5.4. Extending this notion in the natural way to $\mathrm{Out}(\Pi_t)$ and $\mathrm{Out}^+(\Pi_t)$, this implies that $\mathrm{Out}^+(\Pi_t)$ "has the congruence subgroup property", even though the isomorphic group $\mathrm{SL}_2(\mathbb{Z})$ does not. This explains why we use the terminology "linearly congruence". This also implies that the components of $\mathcal{M}(G)_{\mathbb{C}}$ form a cofinal set amongst the finite étale covers of $\mathcal{M}(1)_{\mathbb{C}}$.

The group $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ is further discussed in the Appendix §7.1.

5.5 Summary of notation

We summarize the notation used in the discussion above.

Situation 5.5. In this situation we use the following notation:

(a) Let K be a field with an embedding $\iota : K \hookrightarrow \mathbb{C}$. Let $\overline{K}$ be the algebraic closure of K inside $\mathbb{C}$.

(b) Let E be an elliptic curve over K with origin O, let $E^\circ := E - O$, and let $E_{\overline{K}}, E^\circ_{\overline{K}}, E_{\mathbb{C}}, E^\circ_{\mathbb{C}}$ be the base changes via ι.

(c) Let t be a tangential base point at O.

(d) Let $\Pi = \Pi_t := \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), t)$.

(e) Let $F := \pi_1(E^\circ_{\overline{K}}, t)$, $M := F/F''$ its metabelianization, $A = F/F' = M/M'$ the abelianization.

(f) Let $j : \Pi \hookrightarrow F = \pi_1(E^\circ_{\overline{K}}, t)$ the canonical injection which induces an isomorphism $\widehat{\Pi} \cong F$.

(g) Let $\mathcal{I} = \mathcal{I}_t \leq F = \pi_1(E^\circ_{\overline{K}}, t)$ be the associated canonical inertia subgroup. It is isomorphic to $\widehat{\mathbb{Z}}$ with $\mathrm{Gal}(\overline{K}/K)$ acting via the cyclotomic character $\chi : \mathrm{Gal}(\overline{K}/K) \longrightarrow \widehat{\mathbb{Z}}^\times$.

(h) Let x_1, x_2 be a positively oriented basis of Π such that $j([x_1, x_2])$ generates $\mathcal{I}$.

(i) Let $\mathrm{Out}(M, \mathcal{I})$ be the subgroup of $\mathrm{Out}(M)$ preserving the conjugacy class of the subgroup $\mathcal{I}$.

(j) The pair x_1, x_2 defines maps $\Pi \overset{j}{\hookrightarrow} F \to \widehat{\mathbb{Z}}^2$ sending $(x_1, x_2) \mapsto ((1,0),(0,1))$. This in turn induces maps

$$\mathrm{Out}(\Pi) \hookrightarrow \mathrm{Out}(F) \twoheadrightarrow \mathrm{Out}(M) \twoheadrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

and isomorphisms $\mathrm{Out}(\Pi) \cong \mathrm{GL}_2(\mathbb{Z})$, $\mathrm{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$ (Theorem 3.18).

[14] The importance of the congruence subgroup topology is that its natural extension to $\mathrm{Aut}(\widehat{B})$ agrees with the compact-open topology on $\mathrm{Aut}(\widehat{B})$, and this makes $\mathrm{Aut}(\widehat{B})$ into a profinite group [RZ10, 4.4.2, 4.4.3].

(k) Let $\rho_{E^\circ/K} : \widehat{\mathrm{Out}^+(\Pi)} \rtimes \mathrm{Gal}(\overline{K}/K) \cong \pi_1(\mathcal{M}(1)_K, E) \longrightarrow \mathrm{Out}(F)$ be the arithmetic monodromy representation (25).

(l) The restrictions of $\rho_{E^\circ/K}$ to $\mathrm{Out}^+(\Pi), \mathrm{Gal}(\overline{K}/K)$ recovers the representations $\rho^{\mathrm{top}}_{E^\circ(\mathbb{C})}, \rho^{\mathrm{Gal}}_{E^\circ/K}$ respectively.

6 Geometric applications

In this section we apply the algebraic results of the previous sections to study the stacks $\mathcal{M}(G)_{\mathbb{Q}}$ when G is metabelian. Throughout this section G is a finite 2-generated metabelian group. Let $\mathrm{ab} : G \to G^{\mathrm{ab}}$ be the abelianization. Let $(E, K, t, \Pi, \mathcal{I}, F, M, A, x_1, x_2, \ldots)$ be as in Situation 5.5. The maps $\mathrm{Out}(\Pi) \hookrightarrow \mathrm{Out}(F) \twoheadrightarrow \mathrm{Out}(M) \twoheadrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}})$ induce an isomorphism $\mathrm{Out}(M, \mathcal{I}) \xrightarrow{\sim} \mathrm{GL}_2(\widehat{\mathbb{Z}})$ by Theorem 3.22 and isomorphisms $\mathrm{Out}(\Pi) \cong \mathrm{GL}_2(\mathbb{Z})$, $\mathrm{Out}^+(\Pi) \cong \mathrm{SL}_2(\mathbb{Z})$. We will often use these isomorphisms to identify subgroups of $\mathrm{Out}(M, \mathcal{I})$ with their images in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Recall that $\mathrm{Out}(M, \mathcal{I})$ admits a canonical determinant map (Remark 3.21)

$$\det : \mathrm{Out}(M, \mathcal{I}) \longrightarrow \widehat{\mathbb{Z}}^\times$$

satisfying $\det(\gamma) = \det(\gamma^{\mathrm{ab}}) = \det_c(\gamma)$ for any generator $c \in \mathcal{I}$. Let

$$\mathrm{Out}^+(M, \mathcal{I}) := \{\gamma \in \mathrm{Out}(M, \mathcal{I}) \mid \det(\gamma) = 1\}$$

Thus $\mathrm{Out}^+(M, \mathcal{I}) \leq \mathrm{Out}(M, \mathcal{I})$ is mapped isomorphically onto the subgroup $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. For any $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(\Pi, G) = \mathrm{Epi}^{\mathrm{ext}}(M, G)$ and integer $n \geq 1$, let

$$\begin{aligned}
\widehat{G\Gamma}_\varphi &:= \mathrm{Stab}_{\mathrm{Out}(M,\mathcal{I})}(\varphi) \\
\Gamma_\varphi &:= \mathrm{Stab}_{\mathrm{Out}^+(\Pi)}(\varphi) \\
\widehat{G\Gamma}(n) &:= \widehat{G\Gamma}_{M \to (\mathbb{Z}/n)^2} = \mathrm{Ker}\left(\mathrm{Out}(M, \mathcal{I}) \xrightarrow{\sim} \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n)\right) \\
\Gamma(n) &:= \Gamma_{\Pi \to (\mathbb{Z}/n)^2} = \mathrm{Ker}\left(\mathrm{Out}^+(\Pi) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/n)\right)
\end{aligned}$$

We note that our definition of $\Gamma(n)$ in this section differs from the classical definition given in §5.4. However, under the isomorphism $\mathrm{Out}^+(\Pi) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})$ defined by x_1, x_2, our $\Gamma(n) \leq \mathrm{Out}^+(\Pi)$ is sent isomorphically onto the classical principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of §5.4, so there is little ambiguity.

6.1 Image of the pro-metabelian monodromy representation

Theorem 6.1. *The image of the metabelian arithmetic monodromy representation*

$$\rho^{meta}_{E^\circ/K} : \pi_1(\mathcal{M}(1)_K, E_{\overline{K}}) \xrightarrow{\rho_{E^\circ/K}} \mathrm{Out}(F) \twoheadrightarrow \mathrm{Out}(M)$$

is contained in the subgroup $\mathrm{Out}(M, \mathcal{I})$*, and hence is isomorphic to its image in* $\mathrm{Out}(F^{\mathrm{ab}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$*. In particular, for any finite metabelian group G, the components of $\mathcal{M}(G)_{\overline{K}}$ are all congruence (equivalently, the groups Γ_φ are linearly congruence).*

Proof. For the first statement, using the decomoposition $\pi_1(\mathcal{M}(1)_K, E) \cong \widehat{\mathrm{Out}^+(\Pi)} \rtimes \mathrm{Gal}(\overline{K}/K)$, we must show that each of the semidirect factors maps to $\mathrm{Out}(M, \mathcal{I})$. Let

$$\overline{\det_c} : \mathrm{Out}(M) \longrightarrow \widehat{\mathbb{Z}}[\![A]\!]^\times / A$$

be the map induced by $\det_c : \mathrm{Aut}(M) \to \widehat{\mathbb{Z}}[\![A]\!]^\times$. By Proposition 5.1, $\mathrm{Out}^+(\Pi)$ preserves the conjugacy class of elements of $\mathcal{I}$, so its image in $\mathrm{Out}(M)$ satisfies $\overline{\det_c} = 1$. Since $\overline{\det_c}$ is continuous, the image of $\widehat{\mathrm{Out}^+(\Pi)}$ also satisfies $\overline{\det_c} = 1$. Thus $\widehat{\mathrm{Out}^+(\Pi)}$ maps to $\mathrm{Out}(M, \mathcal{I})$. Since $\mathrm{Gal}(\overline{K}/K)$ acts on $\mathcal{I}$ via the cyclotomic character $\chi : \mathrm{Gal}(\overline{K}/K) \to \widehat{\mathbb{Z}}^\times$, we have $\overline{\det_c}(\sigma) = \chi(\sigma)$ for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, so $\mathrm{Gal}(\overline{K}/K)$ also maps to $\mathrm{Out}(M, \mathcal{I})$.

For the final statement, since G is a finite metabelian group, the action of $\widehat{\mathrm{Out}^+(\Pi)}$ on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$ factors through its action on $\Pi/\Pi'' = M$. Since its action on M is isomorphic to its action on A, the kernel of this action contains the congruence kernel, so by Proposition 5.3, the components of $\mathcal{M}(G)_{\overline{K}}$ are all congruence. □

We summarize the content of Theorem 6.1 in the following commutative diagram:

$$\begin{tikzcd}
\pi_1(\mathcal{M}(1)_K, E_{\overline{K}}) \arrow[r, "\sim"] & \pi_1(\mathcal{M}(1)_{\overline{K}}, E_{\overline{K}}) \rtimes \mathrm{Gal}(\overline{K}/K) \arrow[r] \arrow[rr, bend left, "\rho^{\mathrm{meta}}_{E^\circ/K}"] & \mathrm{Out}(M,\mathcal{I}) \arrow[r, hook] \arrow[dr, "\sim"] & \mathrm{Out}(M) \arrow[d, two heads] \\
\mathrm{Gal}(\overline{K}/K) \arrow[ur, hook] \arrow[drrr, bend right, "\chi"'] & \underbrace{\pi_1(\mathcal{M}(1)_{\overline{K}}, E_{\overline{K}})}_{\widehat{\mathrm{Out}^+(\Pi)}} \arrow[u, hook] \arrow[r, two heads] & \mathrm{SL}(A) \arrow[u, hook] \arrow[r, hook] & \mathrm{GL}(A) \arrow[d, two heads, "\det"] \\
 & & & \widehat{\mathbb{Z}}^\times
\end{tikzcd} \tag{26}$$

In particular, the representation $\rho^{\mathrm{meta}}_{E^\circ/K}$ surjects onto the subgroup $\mathrm{Out}(M,\mathcal{I})$ if and only if the cyclotomic character $\chi : \mathrm{Gal}(\overline{K}/K) \longrightarrow \widehat{\mathbb{Z}}^\times$ is surjective.

Corollary 6.2. *The action of* $\mathrm{Gal}(\overline{K}/K)$ *on the connected components of* $\mathcal{M}(G)_{\overline{K}}$ *factors through an action of* $\widehat{\mathbb{Z}}^\times$ *via the cyclotomic character* $\chi : \mathrm{Gal}(\overline{K}/K) \longrightarrow \widehat{\mathbb{Z}}^\times$*.*

Proof. By Galois theory the action of $\mathrm{Gal}(\overline{K}/K)$ on connected components is given by its action on the orbits of $\pi_1(\mathcal{M}(1)_{\overline{K}}, E_{\overline{K}})$ acting on $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G) = \mathrm{Epi}^{\mathrm{ext}}(M, G)$ via $\rho^{\mathrm{meta}}_{E^\circ/K}$. The statement then follows from the diagram (26). □

As a corollary we recover a result of Ben-Ezra and Lubotzky [BEL17]. Recall that $\mathbf{M}$ is a discrete free metabelian group of rank 2, and for a finitely generated group G, $\mathrm{Aut}(G)$ (reps. $\mathrm{Out}(G)$) satisfies the congruence subgroup property if every finite index subgroup of $\mathrm{Aut}(G)$ (resp. $\mathrm{Out}(G)$) contains $\Gamma[K] := \mathrm{Ker}(\mathrm{Aut}(G) \to \mathrm{Aut}(G/K))$ (resp. $\Delta[K] := \mathrm{Ker}(\mathrm{Out}(G) \to \mathrm{Out}(G/K))$) for some finite index characteristic subgroup K.

Corollary 6.3 (Ben-Ezra, Lubotzky)**.** $\mathrm{Aut}(\mathbf{M})$ *does not have the congruence subgroup property.*[15]

Proof. By 3.16(a) M has trivial center, so it suffices to show the result for $\mathrm{Out}(\mathbf{M})$ [BER11, Lemma 3.1]. Let $K \leq \mathbf{M}$ be a finite index characteristic subgroup. Then 6.1 and 5.3 together imply that $\Delta[K] := \mathrm{Ker}(\mathrm{Out}(\mathbf{M}) \to \mathrm{Out}(\mathbf{M}/K))$ is a linearly congruence subgroup of $\mathrm{Out}(\mathbf{M})$. Since $\mathrm{Out}(\mathbf{M}) \cong \mathrm{SL}_2(\mathbb{Z})$ has finite index subgroups which are not linearly congruence, it follows that $\mathrm{Out}(\mathbf{M})$, and hence $\mathrm{Aut}(\mathbf{M})$, does not have the congruence subgroup property. □

6.2 The structure of $\mathcal{M}(G)$

We maintain the notation described in the beginning of §6. In this section we study the stacks $\mathcal{M}(G)_{\mathbb{Q}}$, which amounts to understanding the stabilizers $\widehat{G\Gamma}_\varphi$ and Γ_φ for $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(M, G)$. Our main objective is to study the congruence level of components of $\mathcal{M}(G)$, both arithmetically and geometrically. We will do this by first bounding $\mathcal{M}(G)$ "from above" (§6.2.1), by showing that every component is covered by a component of $\mathcal{M}(B)$ for some finite abelian group B. Next, in §6.2.2, we will bound $\mathcal{M}(G)$ "from below", by using $\mathrm{IOut}_1(G)$ to control the degree of the map $\mathcal{M}(G) \to \mathcal{M}(G^{\mathrm{ab}})$, which provides additional bounds on the congruence level.

6.2.1 Bounding $\mathcal{M}(G)$ from above

Theorem 6.4. *Suppose* G *is a quotient of* $M_{n,m}$ *for some integers* $n, m \geq 1$ *(see §3.2). The group* $\mathrm{Out}(G)$ *acts as automorphisms of the cover* $\mathcal{M}(G)_{\mathbb{Q}} \to \mathcal{M}(1)_{\mathbb{Q}}$*, and we have*

- *(a)* $\mathrm{IOut}(G)$ *permutes transitively the connected components of* $\mathcal{M}(G)_{\mathbb{Q}}$*, which are hence all isomorphic as covers of* $\mathcal{M}(G)_{\mathbb{Q}}$*.*

[15] See Defintion 5.4 for the definition of the congruence subgroup property.

(b) *Every connected component $\mathcal{M} \subset \mathcal{M}(G)_{\mathbb{Q}}$ is a quotient of $\mathcal{M}((\mathbb{Z}/nm)^2)_{\mathbb{Q}}$ by a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/nm)$.

(c) *If G has exponent e, then every connected component $\mathcal{M} \subset \mathcal{M}(G)_{\overline{K}}$ is a quotient of a connected component of $\mathcal{M}((\mathbb{Z}/e)^2)_{\overline{K}}$ by a subgroup of* $\mathrm{SL}_2(\mathbb{Z}/e)$. *In particular, $\mathcal{M}$ has congruence level dividing e.*

Note that part (c) immediately implies:

Example 6.5 (Free metabelian groups of exponent e)**.** Let M_e denote the free 2-generated metabelian group of exponent e.[16] Let $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(M, G)$. Clearly $M_e^{\mathrm{ab}} \cong \mathbb{Z}/e \times \mathbb{Z}/e$, so we have $\Gamma_\varphi \subset \Gamma_{\mathrm{ab}\circ\varphi} = \Gamma(e)$. On the other hand Theorem 6.4(c) implies that $\Gamma_\varphi \supset \Gamma(e)$, so we must have $\Gamma_\varphi = \Gamma(e)$. In particular $\mathcal{M}(M_e)_{\mathbb{C}}$ is a disjoint union of copies of $[\mathcal{H}/\Gamma(n)]$.

Remark 6.6. We make some observations regarding Theorem 6.4.

(i) Note that if e' denotes the exponent of G', G is a quotient of $M_{e,e'}$, so we can always take $(n, m) = (e, e')$.

(ii) Group-theoretically, (a) says that the action of $\mathrm{IOut}(G)$ on $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ commutes with the $\mathrm{Out}(M, \mathcal{I})$-action and acts transitively on the $\mathrm{Out}(M, \mathcal{I})$-orbits; (b) says that $\widehat{G\Gamma}_\varphi \supset \widehat{G\Gamma}(nm)$; and (c) says that $\Gamma_\varphi \supset \Gamma(e)$.

(iii) Part (a) implies that the connected components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ are all Galois conjugates of each other. To be precise, for any two components $\mathcal{M}, \mathcal{M}' \subset \mathcal{M}(G)_{\overline{\mathbb{Q}}}$, there is a $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and an isomorphism $\tilde{\sigma} : \mathcal{M} \xrightarrow{\sim} \mathcal{M}'$ making the following diagram commute

$$\begin{tikzcd}
\mathcal{M} \arrow[r, "\tilde{\sigma}"] \arrow[d] & \mathcal{M}' \arrow[d] \\
\operatorname{Spec}\overline{\mathbb{Q}} \arrow[r, "\sigma"] & \operatorname{Spec}\overline{\mathbb{Q}}
\end{tikzcd}$$

Thus, part (a) implies that the connected components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ are all isomorphic as stacks, but not necessarily as covers of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$. The components are all isomorphic as covers of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ if and only if the centralizer of the $\mathrm{Out}^+(M, \mathcal{I})$-action on $\mathrm{Epi}^{\mathrm{ext}}(M, G)$ acts transitively on the $\mathrm{Out}^+(M, \mathcal{I})$-orbits. Since the centralizer contains $\mathrm{IOut}(G)$, the components lying over a given component of $\mathcal{M}(G^{\mathrm{ab}})_{\overline{\mathbb{Q}}}$ are all isomorphic. The set of components of $\mathcal{M}(G^{\mathrm{ab}})_{\overline{\mathbb{Q}}}$ can be identified with the set of generators of the cyclic group $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$. Using the basis $x_1, x_2 \in M$, this set of generators can in turn be identified with $(\mathbb{Z}/n)^\times$, where $n = |G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}|$. For $u \in (\mathbb{Z}/n)^\times$, write $\mathcal{M}_u$ for the component of $\mathcal{M}(G^{\mathrm{ab}})_{\overline{\mathbb{Q}}}$ corresponding to u. Since the centralizer contains the center of $\mathrm{Out}(M, \mathcal{I}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$, for any $u, u' \in (\mathbb{Z}/n)^\times$ satisfying $u^2 = (u')^2$, the components lying over $\mathcal{M}_u \cup \mathcal{M}_{u'}$ are all isomorphic. Thus to show that the components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ are all isomorphic as covers of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$, it would suffice to show that the centralizer induces as transitive action on the quotient of $(\mathbb{Z}/n)^\times$ by its subgroup of squares. An natural guess is to wonder if this holds for the action of $\mathrm{Out}(G)$, but unfortunately this is false. The smallest example is for a group G, a non-split extension of $G^{\mathrm{ab}} \cong (\mathbb{Z}/3)^2$ by $G' \cong (\mathbb{Z}/3)^3$, with $Z(G) \cong (\mathbb{Z}/3)^2 \leq G'$.[17] For this group G, the image of $\mathrm{Aut}(G) \to \mathrm{Aut}(G^{\mathrm{ab}}) \cong \mathrm{GL}_2(\mathbb{Z}/3)$ lies in $\mathrm{SL}_2(\mathbb{Z}/3)$. Nonetheless, one can compute that $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ consists of two connected components which are isomorphic to each other over $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$.

Proof of Theorem 6.4. The geometric fiber of $\mathcal{M}(G)_{\mathbb{Q}} \to \mathcal{M}(1)_{\mathbb{Q}}$ over $E_{\overline{K}}$ is given by $\mathrm{Epi}^{\mathrm{ext}}(M, G)$, which admits an action of $\mathrm{Out}(G)$ on the target, commuting with the monodromy action of $\pi_1(\mathcal{M}(1)_{\mathbb{Q}}, E)$ on the source. By Theorem 6.1, the action of $\pi_1(\mathcal{M}(1)_{\mathbb{Q}}, E)$ factors through $\mathrm{Out}(M, \mathcal{I})$. Thus part (a) is the Galois-theoretic translation of Corollary 3.23.

Let $\varphi : M \to G$ be a surjection. For (b), we must show that $\widehat{G\Gamma}_\varphi \supset \widehat{G\Gamma}(nm)$. Indeed, φ factors as $M \to M_{nm,m} \to M_{n,m} \to G$. If ψ denotes the composition $M \to M_{nm,m} \to M_{n,m}$, then we have $\widehat{G\Gamma}_\varphi \supset \widehat{G\Gamma}_\psi$. We will show that $\widehat{G\Gamma}_\psi \supset \widehat{G\Gamma}(nm)$. Let $\gamma \in \widehat{G\Gamma}(nm)$, then we want to show that $\psi \circ \gamma$ is conjugate to ψ by an inner automorphism of $M_{n,m}$, or equivalently the generating pair $((\psi \circ \gamma)(x_1), (\psi \circ \gamma)(x_2))$ of $M_{n,m}$ is conjugate to the

[16] This is a finite group – indeed M_e', M_e^{ab} are both finite since they are finitely generated and abelian of bounded exponent.

[17] This group can be accessed in GAP as `SmallGroup(243,7)`.

pair $(\psi(x_1), \psi(x_2))$. For this it suffices to check that the criteria of Corollary 4.20 are satisfied, but this is clear - (a) is satisfied since $\gamma \in \widehat{G\Gamma}(nm)$. For (b), note $[(\psi \circ \gamma)(x_1), (\psi \circ \gamma)(x_2)] = [\psi(x_1), \psi(x_2)]^{\det(\gamma)}$; since $M'_{nm,m}$ has exponent m and γ preserves $\mathcal{I}$ with $\det(\gamma) \equiv 1 \mod nm$, these commutators are the same, so (b) is satisfied.

For (c), we must show that $\Gamma_\varphi \supset \Gamma(e)$, but this follows immediately from Corollary 7.2 in the appendix. □

6.2.2 Bounding $\mathcal{M}(G)$ from below

Theorem 6.4 implies that if G is a quotient of $M_{n,m}$, then for $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(M, G)$, $\widehat{G\Gamma}_\varphi \supset \widehat{G\Gamma}(nm)$ and $\Gamma_\varphi \supset \Gamma(e)$. Let $\mathrm{ab} : G \to G^{\mathrm{ab}}$ be the abelianization; then we have

$$\widehat{G\Gamma}_{\mathrm{ab}\circ\varphi} \supset \widehat{G\Gamma}_\varphi \supset \widehat{G\Gamma}(nm) \qquad \text{and} \qquad \Gamma_{\mathrm{ab}\circ\varphi} \supset \Gamma_\varphi \supset \Gamma(e) \tag{27}$$

In the remainder of this section we study the first containments. The key observation is that by Corollary 4.8, φ induces a map $\varphi_* : \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi} \longrightarrow \mathrm{IOut}(G)$ with kernel $\widehat{G\Gamma}_\varphi$. Let e' be the exponent of G', and let $\widehat{G\Gamma}_{ab\circ\varphi,\det\equiv 1(e')} \le \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi}$ be the subgroup consisting of elements with determinant $\equiv 1 \mod e'$. Then on this subgroup φ_* takes values in $\mathrm{IOut}_1(G)$. To summarize,

Proposition 6.7. *Let $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(M, G)$. Then with notation as above, we have a diagram with exact rows:*

$$\begin{tikzcd}
1 \arrow[r] & \widehat{G\Gamma}_\varphi \arrow[r] & \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi} \arrow[r, "\varphi_*"] & \mathrm{IOut}(G) \\
1 \arrow[r] & \widehat{G\Gamma}_\varphi \cap \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi,\det\equiv 1(e')} \arrow[r] \arrow[u, hook] & \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi,\det\equiv 1(e')} \arrow[r, "\varphi_*"] \arrow[u, hook] & \mathrm{IOut}_1(G) \arrow[u, hook]
\end{tikzcd} \tag{28}$$

Restricting to Γ_φ, we also have an exact sequence

$$1 \longrightarrow \Gamma_\varphi \longrightarrow \Gamma_{\mathrm{ab}\circ\varphi} \xrightarrow{\varphi_*} \mathrm{IOut}_1(G)$$

Proof. Follows from the above discussion. □

This allows us to control the field of definition of connected components of $\mathcal{M}(G)$ in terms of $\mathrm{IOut}_1(G)$.

Theorem 6.8. *Let n be the order of the cyclic group $G^{\mathrm{ab}} \wedge G^{\mathrm{ab}}$, and let $m := \mathrm{lcm}(n, e')$. Then there is a number field L containing $\mathbb{Q}(\zeta_m)$ with $\mathrm{Gal}(L/\mathbb{Q}(\zeta_m)) \le \mathrm{IOut}_1(G)$ such that the connected components of $\mathcal{M}(G)_L$ are geometrically connected over L. In fact L is contained in a cyclotomic field, and hence abelian over $\mathbb{Q}$.*

Proof. Let $\varphi : M \longrightarrow G$ be a surjection. Let $\overline{\Gamma_\varphi}$ denote the closure of the image of Γ_φ inside $\mathrm{Out}^+(M, \mathcal{I}) \cong \mathrm{SL}_2(\widehat{\mathbb{Z}})$. For a number field L, let $\mathrm{Mon}_{\overline{\mathbb{Q}}}, \mathrm{Mon}_L$ denote the monodromy images of $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E_{\overline{\mathbb{Q}}}), \pi_1(\mathcal{M}(1)_L, E_{\overline{\mathbb{Q}}})$ inside $\mathrm{Out}(M, \mathcal{I})$ respectively. Then we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Mon}_{\overline{\mathbb{Q}}} \arrow[r] & \mathrm{Mon}_L \arrow[r, "\det"] & \det(\mathrm{Mon}_L) \arrow[r] & 1 \\
1 \arrow[r] & \overline{\Gamma_\varphi} \cap \mathrm{Mon}_{\overline{\mathbb{Q}}} \arrow[r] \arrow[u, hook] & \widehat{G\Gamma}_\varphi \cap \mathrm{Mon}_L \arrow[r, "\det"] \arrow[u, hook] & \det(\widehat{G\Gamma}_\varphi \cap \mathrm{Mon}_L) \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

where det is the restriction of the "canonical" determinant $\mathrm{Out}(M, \mathcal{I}) \to \widehat{\mathbb{Z}}^\times$, the rows are exact, and each vertical arrow is the inclusion of a finite index subgroup. By Theorem 6.4(a), the components of $\mathcal{M}(G)_L$ are all geometrically connected over L if and only if the component corresponding to φ is geometrically connected. By Galois theory this happens if and only if $[\mathrm{Mon}_{\overline{\mathbb{Q}}} : \overline{\Gamma_\varphi} \cap \mathrm{Mon}_{\overline{\mathbb{Q}}}] = [\mathrm{Mon}_L : \widehat{G\Gamma}_\varphi \cap \mathrm{Mon}_L]$, or equivalently, if and only if $\det(\mathrm{Mon}_L) = \det(\widehat{G\Gamma}_\varphi \cap \mathrm{Mon}_L)$ as subgroups of $\widehat{\mathbb{Z}}^\times$. Since Mon_L contains the kernel of $\det : \mathrm{Out}(M, \mathcal{I}) \to \widehat{\mathbb{Z}}^\times$, $\det(\widehat{G\Gamma}_\varphi \cap \mathrm{Mon}_L) = \det(\widehat{G\Gamma}_\varphi) \cap \det(\mathrm{Mon}_L)$. From the diagram (26), $\det(\mathrm{Mon}_L) = \chi(\mathrm{Gal}(\overline{\mathbb{Q}}/L))$, so our task is to choose an appropriate L such that $\chi(\mathrm{Gal}(\overline{\mathbb{Q}}/L)) \subset \det(\widehat{G\Gamma}_\varphi)$.

By Remark 3.21 we know $\det \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi} = 1 + n\widehat{\mathbb{Z}}$, so $\det(\widehat{G\Gamma}_{\mathrm{ab}\circ\varphi,\det\equiv 1(e')}) = 1 + m\widehat{\mathbb{Z}}$. The bottom row of (28) then implies that $D := \det(\widehat{G\Gamma}_{\varphi} \cap \widehat{G\Gamma}_{\mathrm{ab}\circ\varphi,\det\equiv 1(e')})$ is a normal subgroup of $1 + m\widehat{\mathbb{Z}}$ with quotient a subgroup of $\mathrm{IOut}_1(G)$. Taking L to be the fixed field of $\chi^{-1}(D)$, we find that L is contained in a cyclotomic field and is Galois over $\mathbb{Q}(\zeta_m)$ with Galois group a subgroup of $\mathrm{IOut}_1(G)$, as desired. □

Since abelian quotients of congruence subgroups by congruence subgroups are relatively small (Proposition 7.3), the fact that $\Gamma_\varphi/\Gamma_{\mathrm{ab}\circ\varphi}$ is abelian implies additional restrictions on the congruence level of Γ_φ. In the simplest case, suppose $G^{\mathrm{ab}} = \mathbb{Z}/n \times \mathbb{Z}/n$ where n is odd, then $\Gamma_{\mathrm{ab}\circ\varphi} = \Gamma(n)$ and Γ_φ is a (linear) congruence subgroup normal inside $\Gamma(n)$ with abelian quotient isomorphic to a subgroup of $\mathrm{IOut}_1(G)$. If m is the exponent of $\mathrm{IOut}_1(G)$, then the structure of "coabelian" linear congruence subgroups of $\Gamma(n)$ described in §7.1 implies that Γ_φ has linear congruence level dividing nm.

To give a precise statement, for integers n, m, let $\varphi_{n,m} : \Pi \to \mathbb{Z}/n \times \mathbb{Z}/m$ be a surjection sending x_1, x_2 to elements of order n, m respectively. Define

$$\Gamma(n,m) := \mathrm{Stab}_{\mathrm{Out}^+(\Pi)}(\varphi_{n,m}) \qquad \Gamma^1(n) := \Gamma(n,1)$$

Let $h : \mathrm{Out}^+(\Pi) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})$ be the isomorphism defined by x_1, x_2. Then via h, $\Gamma(n,m)$ is mapped onto the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ given by matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with $a - 1 \equiv b \equiv 0 \mod n$ and $c \equiv d - 1 \equiv 0 \mod m$.

Theorem 6.9. *Let G be a 2-generated finite metabelian group, and suppose $G^{\mathrm{ab}} \cong \mathbb{Z}/nd \times \mathbb{Z}/n$ for integers $d, n \geq 1$. Let $\varphi : \Pi \to G$ be a surjection. For a subgroup $\Gamma \leq \mathrm{Out}^+(\Pi)$, write $\overline{\Gamma}$ for its closure inside $\mathrm{SL}_2(\mathbb{Z}_p)$ via h. Let p^{ω_p} denote the exponent of the Sylow-p subgroup of $\mathrm{IOut}_1(G)$. Let $r := \mathrm{ord}_p(n), s := \mathrm{ord}_p(d)$. Then*

- *(a) $0 \leq \omega_p \leq r$,*
- *(b) if $r = 0$, then $\overline{\Gamma_\varphi} = \overline{\Gamma_{\mathrm{ab}\circ\varphi}}$ is conjugate to $\overline{\Gamma^1(p^s)}$ in $\mathrm{GL}_2(\mathbb{Z}_p)$, and*
- *(c) if $r \geq 1$, then $\overline{\Gamma_\varphi}$ contains a $\mathrm{GL}_2(\mathbb{Z}_p)$-conjugate of $\overline{\Gamma(p^{r+s+\omega_p}, p^{r+\omega_p})}$.*

In particular, if $\epsilon = \prod_p p^{\omega_p}$ denotes the exponent of $\mathrm{IOut}_1(G)$, then $\epsilon \mid n$ and the linear congruence level of Γ_φ divides $nd\epsilon$. If $\mathrm{IOut}_1(G) = 0$ (i.e. G is rigid), then the map $\mathcal{M}(G)_{\overline{\mathbb{Q}}} \to \mathcal{M}(G^{\mathrm{ab}})_{\overline{\mathbb{Q}}}$ restricts to an isomorphism on any connected component, and there exist precisely $|R^\times_{G,\epsilon=1}/\rho_G(G^{\mathrm{ab}})|$ components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ lying over any component of $\mathcal{M}(G^{\mathrm{ab}})_{\overline{\mathbb{Q}}}$ (see (13)).

Proof. Part (a) from Proposition 4.26(b),(c); this also implies $\epsilon \mid n$. The statements appearing below (c) follows from (b) and (c).

We now prove parts (b) and (c). We will first prove them assuming that $\mathrm{ab} \circ \varphi$ sends x_1, x_2 to elements of order nd, n respectively. From Proposition 6.7, we know that for any prime p, $\overline{\Gamma_{\mathrm{ab}\circ\varphi}}' \trianglelefteq \overline{\Gamma_\varphi} \trianglelefteq \overline{\Gamma_{ab\circ\varphi}}$ with $\overline{\Gamma_{ab\circ\varphi}}/\overline{\Gamma_\varphi}$ isomorphic to a subgroup of $\mathrm{IOut}_1(G)$.

In case (b), first assume $s = 0$. Then $\overline{\Gamma_{\mathrm{ab}\circ\varphi}}$ contains the matrices $\left[\begin{smallmatrix} 1 & nd \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right]$. Since $n, nd \in \mathbb{Z}_p^\times$,

$$\begin{bmatrix} 1 & nd \\ 0 & 1 \end{bmatrix}^{(nd)^{-1}} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}^{n^{-1}} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

where $(nd)^{-1}, n^{-1}$ denote inverses in $\mathbb{Z}_p$ (see the proof of Proposition 7.1). Thus $\overline{\Gamma_{\mathrm{ab}\circ\varphi}}$ contains $\mathrm{SL}_2(\mathbb{Z})$, and hence is equal to $\mathrm{SL}_2(\mathbb{Z}_p)$, and $\overline{\Gamma_{\mathrm{ab}\circ\varphi}}' = \mathrm{SL}_2(\mathbb{Z}_p)'$. For $p \geq 5$, this commutator subgroup is the entirety of $\mathrm{SL}_2(\mathbb{Z}_p)$, and for $p = 2, 3$, this is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ of index 4,3 respectively (Proposition 7.4). Since $r = 0$, we must also have $\omega_p = 0$, so $[\overline{\Gamma_{\mathrm{ab}\circ\varphi}} : \overline{\Gamma_\varphi}]$ is prime to p. Thus, for any p, we must have $\overline{\Gamma_\varphi} = \mathrm{SL}_2(\mathbb{Z}_p)$ as desired. If $s \geq 1$, then a similar argument using Proposition 7.1 shows that $\overline{\Gamma_{ab\circ\varphi}} = \overline{\Gamma^1(p^s)}$, and again since $\omega_p = 0$, $\overline{\Gamma_\varphi} = \overline{\Gamma_{\mathrm{ab}\circ\varphi}} = \overline{\Gamma^1(p^s)}$ as desired.

In case (c), we will use more results from §7.1, where $\overline{\Gamma(p^{r+s}, p^r)}$ is denoted $\Gamma_{r+s,r+s,r}$. Note that in this case, $\overline{\Gamma_{\mathrm{ab}\circ\varphi}} = \overline{\Gamma(p^{r+s}, p^r)}$. By (34), $\overline{\Gamma(p^{r+s}, p^r)}' \subset \overline{\Gamma(p^{2r+s}, p^{2r})}$, and $\overline{\Gamma(p^{r+s}, p^r)}/\overline{\Gamma(p^{2r+s}, p^{2r})} \cong (\mathbb{Z}/p^r)^3$. In addition, Proposition 7.3(a1)-(a2) implies that the Frattini quotient of $\overline{\Gamma(p^{r+s}, p^r)}$ is $\mathbb{F}_p^3$. Applying (34) again, all of this implies that for any $0 \leq k \leq r$, the maximal abelian p^k-torsion quotient of $\overline{\Gamma(p^{r+s}, p^r)}$ is $(\mathbb{Z}/p^k)^3$, with kernel $\overline{\Gamma(p^{r+s+k}, p^{r+k})}$. Setting $k = \omega_p$ gives the desired result.

Finally we consider the case where $\mathrm{ab} \circ \varphi$ does not send x_1, x_2 to elements of order nd, n respectively. By Gaschütz' lemma, there exists a φ' such that $\mathrm{ab} \circ \varphi$ does, and which is mapped to φ in $\mathrm{Epi}^{\mathrm{ext}}(\Pi, G) = \mathrm{Epi}^{\mathrm{ext}}(M, G)$ by the action of an element of $\mathrm{Out}(M)$. By Corollary 3.23, one can take φ' to lie in the same $\mathrm{Out}(M, \mathcal{I}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$-orbit as φ. It follows that the corresponding $\mathrm{SL}_2(\widehat{\mathbb{Z}})$-stabilizers are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and using the decomposition $\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$, the $\mathrm{SL}_2(\mathbb{Z}_p)$-stabilizers are conjugate in $\mathrm{GL}_2(\mathbb{Z}_p)$, as desired. □

Theorems 6.9 and 6.4 imply the following corollary.

Corollary 6.10. *Let G be a finite 2-generated metabelian group with exponent e. Suppose $G^{\mathrm{ab}} \cong \mathbb{Z}/nd \times \mathbb{Z}/n$, and let ϵ be the exponent of $\mathrm{IOut}_1(G)$. Then $\epsilon \mid n$, and every component of $\mathcal{M}(G)_{\mathbb{C}}$ has congruence level dividing $\gcd(e, nd\epsilon)$.*

7 Appendix

7.1 Congruence subgroups

In this section we establish some results regarding generators and abelianizations of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Since most congruence subgroups are free, this question is more interesting if we consider it in the category of congruence subgroups. For example, we will show that for any $n \geq 1$, the principal congruence subgroup $\Gamma(n) := \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n))$ can be generated by three elements *as a congruence subgroup* (see 7.1). We will also show that the maximal abelian quotient of $\Gamma(n)$ with congruence kernel is an extension of $(\mathbb{Z}/n)^3$ by $(\mathbb{Z}/4)^2$ (see 7.3).

The group $\mathrm{SL}_2(\mathbb{Z})$ embeds as a dense subgroup of its pro-congruence completion $\mathrm{SL}_2(\widehat{\mathbb{Z}}) = \prod_p \mathrm{SL}_2(\mathbb{Z}_p)$. There is a bijection between congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, the forward direction being given by taking closures, and the inverse by taking intersections with $\mathrm{SL}_2(\mathbb{Z})$. If $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a general finite index subgroup, then the topological closure of Γ inside $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ is an open subgroup whose intersection with $\mathrm{SL}_2(\mathbb{Z})$ is the minimum congruence subgroup containing Γ, called the *congruence closure*. The results stated in the previous paragraph can thus be translated into questions about open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}}) = \prod_p \mathrm{SL}_2(\mathbb{Z}_p)$, which can be studied profitably via the theory of formal groups [Ser06, §IV.6-9]. We briefly recall some of the results here.

Let p be a prime, and $\underline{r} = (r_1, r_2, r_3) \in (\mathbb{Z}_{\geq 1})^3$. If $k \in \mathbb{Z}$, we write $\underline{r} + k := (r_1 + k, r_2 + k, r_3 + k)$. In the following we work in $\mathrm{SL}_2(\mathbb{Z}_p)$, and let $\mathfrak{m} := p\mathbb{Z}_p$. We write $\Gamma_{\underline{r}} = \Gamma_{r_1, r_2, r_3}$ for the subset of $\mathrm{SL}_2(\mathbb{Z}_p)$

$$\Gamma_{\underline{r}} = \Gamma_{r_1,r_2,r_3} := \left\{ \begin{bmatrix} 1+a & b \\ c & 1+d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p) \;\middle|\; a \in \mathfrak{m}^{r_1}, b \in \mathfrak{m}^{r_2}, c \in \mathfrak{m}^{r_3} \right\}$$

If $k \in \mathbb{Z}_{\geq 1}$, write $\Gamma_k := \Gamma_{k,k,k}$ for the closure $\overline{\Gamma(p^k)}$ of the principal congruence subgroup $\Gamma(p^k)$ inside $\mathrm{SL}_2(\mathbb{Z}_p)$. Since the determinant is 1, d is uniquely determined by a, b, c:

$$d = (1+a)^{-1}(1+bc) - 1 = -a + a^2 + bc - a^3 - abc + a^4 + a^2bc + O(d_0 \geq 5) \tag{29}$$

where $O(d_0 \geq 5)$ denotes a power series in $\mathbb{Z}_p[\![a, b, c]\!]$ with all terms having total degree ≥ 5. The group multiplication in $\mathrm{SL}_2(\mathbb{Z}_p)$ then defines a 3-dimensional formal group law $\mathfrak{F} = (\mathfrak{F}_1, \mathfrak{F}_2, \mathfrak{F}_3)$, where each $\mathfrak{F}_i$ is a power series in (the coordinates a, b, c of) pairs of matrices X, Y in $\Gamma_{\underline{r}}$. Explicitly, if $X = \left[\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right]$ and

$Y = \left[\begin{smallmatrix} 1+a' & b' \\ c' & 1+d' \end{smallmatrix}\right]$, we have

$$\begin{array}{lcl} (XY)_1 = \mathfrak{F}_1(X,Y) = \mathfrak{F}_1\left(\left[\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right], \begin{bmatrix} 1+a' & b' \\ c' & 1+d' \end{bmatrix}\right) & = & a + a' + aa' + bc' \\ (XY)_2 = \mathfrak{F}_2(X,Y) = \mathfrak{F}_2\left(\left[\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right], \begin{bmatrix} 1+a' & b' \\ c' & 1+d' \end{bmatrix}\right) & = & b + b' + ab' - ba' + ba'^2 + bb'c' - ba'b'c' - ba'^3 + O(d_0 \geq 5) \\ (XY)_3 = \mathfrak{F}_3(X,Y) = \mathfrak{F}_3\left(\left[\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right], \begin{bmatrix} 1+a' & b' \\ c' & 1+d' \end{bmatrix}\right) & = & c + c' + ca' - ac' + a^2c' + bcc' - abcc' - a^3c' + O(d_0 \geq 5) \end{array} \tag{30}$$

where for $\mathfrak{F}_2, \mathfrak{F}_3$ we have used the relation (29).[18] It will be useful to note that in $(XY)_2$, every term of degree ≥ 3 is divisible by b, and in $(XY)_3$, every term of degree ≥ 3 is divisible by c'. The inverse X^{-1} is given by

$$\begin{array}{lcl} (X^{-1})_1 & = & -a + a^2 + bc - abc - a^3 + a^2bc + a^4 + O(d_0 \geq 5) \\ (X^{-1})_2 & = & -b \\ (X^{-1})_3 & = & -c \end{array} \tag{31}$$

where every term of degree ≥ 2 is divisible either by a^2 or bc. It follows from these formulas that for $\underline{r} = (r_1, r_2, r_3) \in \mathbb{Z}_{\geq 1}$, $\Gamma_{\underline{r}}$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ if and only if $r_2 + r_3 \geq r_1$. A triple $\underline{r}$ satisfying this condition will be called *admissible.* In this case, $\mathfrak{F}$ defines a group structure on the set $\mathfrak{m}^{\underline{r}} := \mathfrak{m}^{r_1} \times \mathfrak{m}^{r_2} \times \mathfrak{m}^{r_3}$. Let $G(\mathfrak{m}^{\underline{r}})$ be the group with underlying set $\mathfrak{m}^{\underline{r}}$ and group operation given by $\mathfrak{F}$. We will henceforth pass freely between $\Gamma_{\underline{r}}$ and $G(\mathfrak{m}^{\underline{r}})$ via the isomorphism $\left[\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right] \mapsto (a, b, c)$.

Using (30) and (31), the conjugate XYX^{-1} is given by

$$\begin{array}{lcl} (XYX^{-1})_1 & = & a' + bc' - cb' + 2bca' - acb' - abc' - bcb'c' + b^2cc' - a'^2bc + a^2bc' + O(d_0 \geq 5) \\ (XYX^{-1})_2 & = & b' - 2ba' + 2ab' + bb'c' + ba'^2 - b^2c' - 2aba' + a^2b' - ba'b'c' - ba'^3 + abb'c' + aba'^2 + O(d_0 \geq 5) \\ (XYX^{-1})_3 & = & c' + 2a'c - 2ac' - cb'c' + 2bcc' - ca'^2 - c^2b' - 2aca' + 3a^2c' + ca'b'c' + ca'^3 + 2bc^2a' \\ & & \quad + acb'c' - 4abcc' + aca'^2 + O(d_0 \geq 5) \end{array} \tag{32}$$

Similarly, the commutator is then given by

$$\begin{array}{lcl} [X,Y]_1 & = & bc' - cb' + ca'b' + ba'c' + 2bca' - 2ab'c' - acb' - abc' - cb'^2c' - bcb'c' + b^2c'^2 + b^2cc' - ca'^2b' \\ & & - 3bca'^2 + aca'b' + 3aba'c' - a^2b'c' + a^2bc' + O(d_0 \geq 5) \\ [X,Y]_2 & = & 2ab' - 2ba' + cb'^2 - ba'^2 - b^2c' + 2aa'b' - 2aba' + a^2b' - 2bca'b' - b^2a'c' + acb'^2 + 2abb'c' \\ & & - aba'^2 + a^2a'b' + O(d_0 \geq 5) \\ [X,Y]_3 & = & 2ca' - 2ac' + bc'^2 - 2cb'c' + 2bcc' - 3ca'^2 - c^2b' + 2aa'c' - 2aca' + 3a^2c' + 4ca'b'c' + 4ca'^3 \\ & & + c^2a'b' + 2bc^2a' - 2ab'c'^2 - abc'^2 - 2aa'^2c' - 4abcc' + 3aca'^2 - 3a^2a'c' + 2a^2ca' - 4a^3c' + O(d_0 \geq 5) \end{array} \tag{33}$$

The isomorphisms $\Gamma_{\underline{r}} \cong G(\mathfrak{m}^{\underline{r}})$ carries the filtration $\Gamma_{\underline{r}} \supset \Gamma_{\underline{r}+1} \supset \cdots$ to the filtration $G(\mathfrak{m}^{\underline{r}}) \supset G(\mathfrak{m}^{\underline{r}+1}) \supset \cdots$ given by the canonical containments $\mathfrak{m}^k \supset \mathfrak{m}^{k+1} \supset \cdots$. From the multiplication formulas (30), we find that if $m := \min\{r_1, r_2, r_3\}$, then

$$\Gamma_{\underline{r}}/\Gamma_{\underline{r}+m} \cong G(\mathfrak{m}^{\underline{r}})/G(\mathfrak{m}^{\underline{r}+m}) \cong (\mathbb{Z}/p^m)^3 \tag{34}$$

Proposition 7.1. *Let $e \in \mathbb{Z}_{\geq 1}$, and $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup which contains $I + eX_i$ for $i = 1, 2, 3$, where*

$$X_1 := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad X_2 := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad X_3 := \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}.$$

Then Γ contains the principal congruence subgroup $\Gamma(e)$. In other words, the group $\langle I + eX_i \rangle_{i=1,2,3} \leq \mathrm{SL}_2(\mathbb{Z})$ is dense inside the closure of $\Gamma(e)$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Proof. Let $\overline{\Gamma}$ be the closure of Γ inside $\mathrm{SL}_2(\mathbb{Z}_p)$. We wish to show that for every $p \nmid e$, we have $\overline{\Gamma} = \mathrm{SL}_2(\mathbb{Z}_p)$, and for every $p \mid e$ with $\mathrm{ord}_p(e) = r$, we have $\overline{\Gamma} \supset \overline{\Gamma(p^r)}$. First we note that for any $i = 1, 2, 3$ and $n \in \mathbb{Z}$, we have $I + nX_i = (I + X_i)^n \in \mathrm{SL}_2(\mathbb{Z})$. More generally, for any prime p, the closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ generated

[18] The equations (30),(31),(32),(33) were computed with the aid of Wolfram Mathematica.

by $I + X_i$ is isomorphic to the additive group of $\mathbb{Z}_p$ as topological groups, and hence for any $a, b \in \mathbb{Z}_p$, we have $(I + aX_i)^b = I + abX_i$ in $\mathrm{SL}_2(\mathbb{Z}_p)$.

Suppose $p \nmid e$. Let e^{-1} denote the inverse in $\mathbb{Z}_p$. Since $I + eX_i \in \overline{\Gamma_p}$, we have $(I + eX_i)^{e^{-1}} = I + X_i \in \overline{\Gamma}$. Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by the $I + X_i$'s and is dense in $\mathrm{SL}_2(\mathbb{Z}_p)$, this shows that $\overline{\Gamma} = \mathrm{SL}_2(\mathbb{Z}_p)$ for $p \nmid e$.

Now suppose $e = up^r$ where $p \nmid u$. Since $\overline{\Gamma} \leq \mathrm{SL}_2(\mathbb{Z}_p)$ is an open subgroup, $\overline{\Gamma} \supset \overline{\Gamma(p^s)}$ for some s, where we may assume $s - 1 \geq r$. Then, $\overline{\Gamma(p^{s-1})}/\overline{\Gamma(p^s)}$ is isomorphic to $G(p^{s-1})/G(p^s)$ which from (34) is isomorphic to the additive group $\mathbb{F}_p^3$. Thus, we have an injective homomorphism of $\mathbb{F}_p$-vector spaces

$$\frac{\overline{\Gamma} \cap \overline{\Gamma(p^{s-1})}}{\overline{\Gamma(p^s)}} \subset \frac{\overline{\Gamma(p^{s-1})}}{\overline{\Gamma(p^s)}} \ \Big(\cong \frac{G(p^{s-1})}{G(p^s)} \cong \mathbb{F}_p^3 \Big). \tag{35}$$

Since $I + up^r X_i \in \overline{\Gamma}$, as above we have $(I + up^r X_i)^{u^{-1}p^{s-1-r}} = I + p^{s-1}X_i \in \overline{\Gamma}$. We clearly also have $I + p^{s-1}X_i \in \overline{\Gamma} \cap \overline{\Gamma(p^{s-1})}$ (for $i = 1, 2, 3$). Since their images in $G(p^{s-1})/G(p^s) \cong \mathbb{F}_p^3$ are $(0, 1, 0), (0, 0, 1), (1, -1, 1)$, the inclusion (35) is an equality, so $\Gamma \supset \Gamma(p^{s-1})$. By induction, we find that $\Gamma \supset \Gamma(p^r)$, as desired. □

Corollary 7.2. *Let G be a finite 2-generated group of exponent e. Let $\mathbf{F}$ be a free group of rank 2. Choose an isomorphism $\mathbf{F}^{\mathrm{ab}} \cong \mathbb{Z}^2$, which induces an isomorphism $f : \mathrm{Out}^+(\mathbf{F}) \cong \mathrm{SL}_2(\mathbb{Z})$, and yields an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathrm{Epi}^{\mathrm{ext}}(\mathbf{F}, G)$. Let $\varphi \in \mathrm{Epi}^{\mathrm{ext}}(\mathbf{F}, G)$. If $\Gamma_\varphi := \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\varphi)$ is congruence, then $\Gamma_\varphi \supset \Gamma(e)$.*

Proof. Let x_1, x_2 be generators of F. In the notation of 7.1, the matrix $I + eX_1 = [\begin{smallmatrix} 1 & e \\ 0 & 1 \end{smallmatrix}]$ is represented by the automorphism of F sending $(x_1, x_2) \mapsto (x_1, x_1^e x_2)$. Since G has exponent e, this automorphism clearly fixes φ, and hence $I + eX_1 \in \Gamma_\varphi$. Since this does not depend on the choice of generators x_1, x_2, it follows that Γ_φ must also contain all conjugates of $I + eX_1$. In particular, it must contain $I + eX_2, I + eX_3$. Proposition 7.1 then implies that $\Gamma_\varphi \supset \Gamma(e)$ as desired. □

Proposition 7.3. *Let p be a prime, and $\underline{r} = (r_1, r_2, r_3)$ an admissible triple. The Frattini subgroup $\Phi(\Gamma_{\underline{r}})$ of $\Gamma_{\underline{r}}$ is as follows:*

(a1) If p is odd, then $\Phi(\Gamma_{\underline{r}}) = \Gamma_{\underline{r}+1}$ and $\Gamma_{\underline{r}}/\Phi(\Gamma_{\underline{r}}) \cong \mathbb{F}_p^3$.

(a2) If $p = 2$ and either $r_1 \geq 2$ or $\underline{r} = (1, 1, 1)$, then $\Phi(\Gamma_{\underline{r}}) = \Gamma_{\underline{r}+1}$ and $\Gamma_{\underline{r}}/\Phi(\Gamma_{\underline{r}}) \cong \mathbb{F}_2^3$.

(a3) If $p = 2$, $r_1 = 1$, and $\underline{r} \neq (1, 1, 1)$, then $\Phi(\Gamma_{\underline{r}}) = \Gamma_{3, r_2+1, r_3+1}$, and $\Gamma_{\underline{r}}/\Phi(\Gamma_{\underline{r}}) \cong \mathbb{F}_2^4$.

Let $n \geq 1$ be an integer. Recall that $\Gamma_n := \Gamma_{n,n,n} \leq \mathrm{SL}_2(\mathbb{Z}_p)$ is the closure of the principal congruence subgroup $\Gamma(p^n)$. Then the derived subgroup Γ_n' and abelianization Γ_n^{ab} are as follows:

(b1) If p is odd, then $\Gamma_n' = \Gamma_{2n}$, and $\Gamma_n^{\mathrm{ab}} \cong (\mathbb{Z}/p^n)^3$.

(b2) If $p = 2$ and $n \geq 2$, then $\Gamma_n' = \Gamma_{2n, 2n+1, 2n+1}$, and $\Gamma_n^{\mathrm{ab}} \cong \mathbb{Z}/2^n \times \mathbb{Z}/2^{n+1} \times \mathbb{Z}/2^{n+1}$.

(b3) If $p = 2$, and $n = 1$, then $\Gamma_{3,4,4} \subset \Gamma_1' \subset \Gamma_{2,3,3}$ and $\Gamma_1'/\Gamma_{3,4,4} \cong \mathbb{F}_2$ generated by the image of $[\begin{smallmatrix} 5 & 8 \\ 8 & 13 \end{smallmatrix}]$, and the abelianization is $\Gamma_1^{\mathrm{ab}} \cong \mathbb{Z}/2 \times \mathbb{Z}/8 \times \mathbb{Z}/8$.

Proof. Inside a pro-p group G, the Frattini subgroup is $\Phi(G) = G^p G'$ and the Frattini quotient $G/\Phi(G)$ is the maximal p-elementary abelian quotient with rank equal to the minimum size $d(G)$ amongst generating sets of G. We also refer to $d(G)$ as the rank of G. It follows that $\Phi(G)$ can be characterized as the unique normal subgroup satisfying $G/\Phi(G) \cong \mathbb{F}_p^{d(G)}$.

We first consider the cases (a1) and (a2). We claim that $\Gamma_{\underline{r}}$ has rank ≤ 3. If $\underline{r} = (k, k, k)$ for some integer $k \geq 1$, then this follows from 7.1. In the general case, for integers $k \geq 1$, let

$$Y_{1,k} := \begin{bmatrix} 1 + p^k & 0 \\ 0 & (1 + p^k)^{-1} \end{bmatrix}, \qquad Y_{2,k} := \begin{bmatrix} 1 & p^k \\ 0 & 1 \end{bmatrix}, \qquad Y_{3,k} := \begin{bmatrix} 1 & 0 \\ p^k & 1 \end{bmatrix}$$

and let $H \leq \Gamma_{\underline{r}}$ be the (closed) subgroup generated by $Y_{1,r_1}, Y_{2,r_2}, Y_{3,r_3}$. As long as $(p, r_1) \neq (2, 1)$, the multiplicative group $1 + \mathfrak{m}^{r_1}$ is pro-cyclic, generated by $1 + p^{r_1}$, so for any $s_1 \geq r_1$, H contains Y_{1,s_1}. Similarly, since

Y_{2,r_2}, Y_{3,r_3} generate additive groups, for any $s_2 \geq r_2, s_3 \geq r_3$, H also contains Y_{2,s_2}, Y_{3,s_3}. Thus, for any $k \geq 0$, the map

$$f_k : H \cap \Gamma_{\underline{r}+k} \hookrightarrow \Gamma_{\underline{r}+k} \twoheadrightarrow \Gamma_{\underline{r}+k}/\Gamma_{\underline{r}+k+1} \cong G(\mathfrak{m}^{\underline{r}+k})/G(\mathfrak{m}^{\underline{r}+k+1}) \cong \mathbb{F}_p^3$$

sends $\{Y_{i,r_i+k}\}_{i=1,2,3}$ to the canonical basis, and hence f_k is surjective. This shows that for any open subgroup $U \leq \Gamma_{\underline{r}}$, $\langle H, U\rangle = \Gamma_{\underline{r}}$; in particular, the only open subgroup containing H is $\Gamma_{\underline{r}}$. Since closed subgroups are intersections of open subgroups [RZ10, Prop 2.1.4(d)], it follows that $H = \Gamma_{\underline{r}}$.

Thus we have shown that in cases (a1),(a2), $\Gamma_{\underline{r}}$ has rank ≤ 3, and since $\Gamma_{\underline{r}}/\Gamma_{\underline{r}+1} \cong \mathbb{F}_p^3$, its rank is 3, so its Frattini quotient is $\mathbb{F}_p^3$. Since $\Gamma_{\underline{r}}/\Gamma_{\underline{r}+1} \cong \mathbb{F}_p^3$ we must have $\Phi(\Gamma_{\underline{r}}) = \Gamma_{\underline{r}+1}$; this establishes (a1),(a2).

For case (a3), we have $r_1 = 1$ and $r_2 + r_3 \geq 3$. We know from (a2) that $\Gamma_{2,r_2,r_3} \leq \mathrm{SL}_2(\mathbb{Z}_2)$ has rank ≤ 3. Since $\Gamma_{1,r_2,r_3}/\Gamma_{2,r_2,r_3}$ is cyclic, Γ_{1,r_2,r_3} has rank ≤ 4. It follows from the commutator formulas (33) that $\Gamma'_{1,r_2,r_3} \subset \Gamma_{3,r_2+1,r_3+1}$, so that the quotient $A := \Gamma_{1,r_2,r_3}/\Gamma_{3,r_2+1,r_3+1}$ is abelian of order 16 and contains the subgroup $B := \Gamma_{2,r_2,r_3}/\Gamma_{3,r_2+1,r_3+1} \cong \mathbb{F}_2^3$. On the other hand, since $r_2 + r_3 \geq 3$, one checks using the multiplication formulas (30) that $\left[\begin{smallmatrix} 1+2 & 2^{r_2} \\ 2^{r_3} & (1+2)^{-1}(1+2^{r_2+r_3}) \end{smallmatrix}\right] \in A - B$ has order 2 in A, and hence $A \cong \mathbb{F}_2^4$ and Γ_{1,r_2,r_3} has rank 4. It follows that the Frattini quotient of $\Gamma_{\underline{r}} = \Gamma_{1,r_2,r_3}$ is $\mathbb{F}_2^4$, and hence we must have $\Phi(\Gamma_{\underline{r}}) = \Gamma_{3,r_2+1,r_3+1}$.

Next we address (b1),(b2),(b3). Writing (a, b, c) for the matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}_p)$, the formulas for the commutator (33) show that $\Gamma'_{n,n,n} \subset \Gamma_{2n,2n,2n}$, and moreover

$$\begin{array}{rcll} Z_1 := [(p^n,0,0),(0,p^n,0)] & \equiv & (0, 2p^{2n} + p^{3n}, 0) & \bmod \mathfrak{m}^{5n} \\ Z_2 := [(p^n,0,0),(0,0,p^n)] & \equiv & (0, 0, -2p^{2n} + 3p^{3n} - 4p^{4n}) & \bmod \mathfrak{m}^{5n} \\ Z_3 := [(0,p^n,0),(0,0,p^n)] & \equiv & (p^{2n} + p^{4n}, -p^{3n}, p^{3n}) & \bmod \mathfrak{m}^{5n} \end{array} \tag{36}$$

If p is odd, by (a1) these commutators generates the Frattini quotient of Γ_{2n} and hence they generate Γ_{2n}, so $\Gamma'_n = \Gamma_{2n}$, with quotient $\Gamma_n^{\mathrm{ab}} \cong (\mathbb{Z}/p^n)^3$ by (34); this proves (b1). If $p = 2$, then the commutator formulas show that $\Gamma'_n \subset \Gamma_{2n,2n+1,2n+1}$. If $n \geq 2$, then by (a2) the commutators Z_1, Z_2, Z_3 again generates the Frattini quotient of $\Gamma_{2n,2n+1,2n+1}$, and hence $\Gamma'_n = \Gamma_{2n,2n+1,2n+1}$. By (a2), the abelianization Γ_n^{ab} is an abelian 2-group of rank 3, which by (34) is an extension of $\Gamma_n/\Gamma_{n,n+1,n+1} \cong (\mathbb{Z}/2)^2$ by $\Gamma_{n,n+1,n+1}/\Gamma_{2n,2n+1,2n+1} \cong (\mathbb{Z}/2^n)^3$, so it must be $\mathbb{Z}/2^n \times \mathbb{Z}/2^{n+1} \times \mathbb{Z}/2^{n+1}$. This proves (b2). Now suppose $n = 1$. The commutator $[\cdot,\cdot]$ induces an alternating bilinear map of $\mathbb{F}_2$-vector spaces

$$\Gamma_1/\Gamma_2 \times \Gamma_1/\Gamma_2 \longrightarrow \Gamma_{2,3,3}/\Gamma_{3,4,4} \cong \mathbb{F}_2^3$$

whose image, by (36), is the span of $(1, -1, 1) \in \mathbb{F}_2^3$. This shows that $\Gamma'_1/\Gamma_{3,4,4}$ has order 2, generated by the image of $\left[\begin{smallmatrix} 5 & 8 \\ 8 & 13 \end{smallmatrix}\right]$. It remains to show that $\Gamma'_1 \supset \Gamma_{3,4,4}$. The commutators Z_1, Z_2 map to $(0,1,0), (0,0,1)$ in $\Gamma_{3,4,4}/\Gamma_{4,5,5} \cong \mathbb{F}_2^3$, and $Z_3^2 \equiv (2^3, 0, 0) \bmod \Gamma_{4,5,5}$ lies in $\Gamma_{3,4,4}$ and maps to $(1,0,0)$ in $\Gamma_{3,4,4}/\Gamma_{4,5,5} \cong \mathbb{F}_2^3$. It follows that Z_1, Z_2, Z_3^2 generate the Frattini quotient of $\Gamma_{3,4,4}$, and hence they generate $\Gamma_{3,4,4}$. The abelianization Γ_1^{ab} is by (a3) a rank 3 abelian 2-group of order 2^7, so there are two possibilities: $\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/8$ or $\mathbb{Z}/2 \times \mathbb{Z}/8 \times \mathbb{Z}/8$. Note that working modulo 2^5, by (30), $(0,2,0)^n \equiv (0,2n,0)$ and $(0,0,2)^n \equiv (0,0,2n)$. Since $(0,2,0)^4 \equiv (0,8,0) \notin \Gamma'_1$ and $(0,0,2)^4 \equiv (0,0,8) \notin \Gamma'_1$, the images of $(0,2,0), (0,0,2)$ in Γ^{ab} generate subgroups of order 8. Since $(0,8,0) - (0,0,8) \equiv (0,8,-8) \notin \Gamma'_1$, we find that $(0,2,0), (0,0,2)$ generate order 8 subgroups with trivial intersection. Thus the first possibility is ruled out, so $\Gamma_1^{\mathrm{ab}} \cong \mathbb{Z}/2 \times \mathbb{Z}/8 \times \mathbb{Z}/8$; this proves (b3). □

Proposition 7.4. *For $p \geq 5$, $\mathrm{SL}_2(\mathbb{Z}_p)' = \mathrm{SL}_2(\mathbb{Z}_p)$. For $p = 2, 3$, we have $\mathrm{SL}_2(\mathbb{Z}_2)^{\mathrm{ab}} \cong \mathbb{Z}/4$, and $\mathrm{SL}_2(\mathbb{Z}_3)^{\mathrm{ab}} \cong \mathbb{Z}/3$. Finally, $\mathrm{SL}_2(\widehat{\mathbb{Z}})' = \prod_p \mathrm{SL}_2(\mathbb{Z}_p)'$.*

Proof. One can algorithmically check that $\mathrm{SL}_2(\mathbb{Z})'$ is a normal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of index 12 and level 12, so $\mathrm{SL}_2(\mathbb{Z})' \supset \Gamma(12)$. For $p > 3$, as in the proof of Proposition 7.1, the images of $\left[\begin{smallmatrix} 1 & 12 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 12 & 1 \end{smallmatrix}\right] \in \Gamma(12)$ generate $\mathrm{SL}_2(\mathbb{Z}_p)$, so $\mathrm{SL}_2(\mathbb{Z})'$ is dense in $\mathrm{SL}_2(\mathbb{Z}_p)$. It follows that $\mathrm{SL}_2(\mathbb{Z}_p)' = \mathrm{SL}_2(\mathbb{Z}_p)$ for $p > 3$. For $p = 3$, from Proposition 7.3 we know $\mathrm{SL}_2(\mathbb{Z}_3)' \supset \overline{\Gamma(3)}' = \overline{\Gamma(9)}$, so $\mathrm{SL}_2(\mathbb{Z}_3)^{\mathrm{ab}} = \mathrm{SL}_2(\mathbb{Z}/9)^{\mathrm{ab}}$ which by an explicit computation is $\cong \mathbb{Z}/3$. For $p = 2$, we similarly know $\mathrm{SL}_2(\mathbb{Z}_2)' \supset \overline{\Gamma(2)}' \supset \overline{\Gamma(16)}$, so $\mathrm{SL}_2(\mathbb{Z}_2)^{\mathrm{ab}} = \mathrm{SL}_2(\mathbb{Z}/16)^{\mathrm{ab}}$ which by an explicit computation is $\cong \mathbb{Z}/4$.

Finally, we have $\mathrm{SL}_2(\widehat{\mathbb{Z}})' \leq \prod_p \mathrm{SL}_2(\mathbb{Z}_p)'$, where $\mathrm{SL}_2(\widehat{\mathbb{Z}})'$ can be identified with the closure of $\mathrm{SL}_2(\mathbb{Z})'$ inside $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since both subgroups have index 12 in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, the inequality must be an equality. □

7.2 Remarks on profinite homology and cohomology

♠♠♠ NOTE: [Should either check the final theorem, or remove this section]

Let G be a profinite group. Let $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ denote the category of profinite $\widehat{\mathbb{Z}}[\![G]\!]$-modules, and let $\underline{\mathbf{DMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ denote the category of discrete $\widehat{\mathbb{Z}}[\![G]\!]$-modules (see [RZ10, §5.1]). The completed tensor product $-\widehat{\otimes}_{\widehat{\mathbb{Z}}[\![G]\!]}\widehat{\mathbb{Z}}$ defines a right-exact functor from $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ to itself. This category has enough projectives, and so we define $\mathrm{Tor}_n^{\widehat{\mathbb{Z}}[\![G]\!]}(-,\widehat{\mathbb{Z}})$ to be the left derived functors of $-\widehat{\otimes}_{\widehat{\mathbb{Z}}[\![G]\!]}\widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}}$ is given the trivial G-action. For a profinite $\widehat{\mathbb{Z}}[\![G]\!]$-module M, the nth homology group of G with coefficients in M is the profinite group

$$H_n(G,M) := \mathrm{Tor}_n^{\widehat{\mathbb{Z}}[\![G]\!]}(M,\widehat{\mathbb{Z}}) \qquad \text{[RZ10, §6.3].}$$

In particular, we have $H_0(G,M) = M_G$, where $M_G := M/I_GM$ is the module of coinvariants.

If M is a discrete $\widehat{\mathbb{Z}}[\![G]\!]$-module, then $\mathrm{Hom}_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}},-)$ is a left-exact functor from $\underline{\mathbf{DMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ to itself. This category has enough injectives, and hence we may define $\mathrm{Ext}^n_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}},-)$ to be the right derived functors of $\mathrm{Hom}_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}},-)$. For a discrete G-module M, its nth cohomology group of G with coefficients in M is

$$H^n(G,M) := \mathrm{Ext}^n_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}},M) \qquad \text{[RZ10, §6.2].}$$

Cohomology with profinite coefficients is more subtle; one difficulty is that the category $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ may not have enough injectives. If M is profinite, one approach is to consider Tate's continuous cohomology $H^n_{\mathrm{cont}}(G,M)$ [Tat76, §2], defined as the cohomology of the complex of continuous cochains. Viewed as a functor from $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$ to $\underline{\mathbf{Ab}}$, the groups $H^n_{\mathrm{cont}}(G,M)$ define a cohomological δ-functor[19], but it is unclear if it is universal in general.

A more sophiscated approach is taken in [BCC16]. Let $\underline{\mathbf{IP}}(\widehat{\mathbb{Z}}[\![G]\!])$ (resp. $\underline{\mathbf{PD}}(\widehat{\mathbb{Z}}[\![G]\!])$) denote the categories of *ind-profinite* (resp. *pro-discrete*) $\widehat{\mathbb{Z}}[\![G]\!]$-modules[20]. These categories are Pontryagin-dual, and enough projectives (resp. injectives). However these categories are not abelian - they are only quasi-abelian, and hence derived functors on them take values in the heart of an appropriate t-structure on the derived category. For an arbitrary profinite group G, deriving $\mathrm{Hom}_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}},-)$ (see [BCC16, §6]) yields cohomology functors

$$H^n(G,-) : \mathcal{RH}(\underline{\mathbf{PD}}(\widehat{\mathbb{Z}}[\![G]\!])) \longrightarrow \mathcal{RH}(\underline{\mathbf{PD}}(\widehat{\mathbb{Z}})) \qquad \text{[BCC16, §7].}$$

Here, for a quasi-abelian category $\mathcal{E}$, $\mathcal{RH}(\mathcal{E})$ denotes the "right heart" of the derived category $\mathcal{D}(\mathcal{E})$. This is an abelian full subcategory which contains $\mathcal{E}$ as a coreflexive full subcategory. In particular we may compute, for any profinite $\widehat{\mathbb{Z}}[\![G]\!]$-module M, the cohomology object $H^n(G,M) \in \mathcal{RH}(\underline{\mathbf{PD}}(\widehat{\mathbb{Z}}))$ such that if

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

is an exact sequence in $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$, then we have the usual long exact sequence in cohomology. However, it is not clear if $H^0(G,M) = M^G$ (See [BCC16, Remarks 6.2, 6.11]), or if $H^0(G,M)$ lands in the subcategory $\underline{\mathbf{PD}}(\widehat{\mathbb{Z}})$. It turns out that a sufficient condition for this is that G is of type FP_∞:

Definition 7.5. A profinite group G is of type FP_n $(n \geq 0)$ if there exists an exact sequence of profinite $\widehat{\mathbb{Z}}[\![G]\!]$-modules

$$P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0$$

where $\widehat{\mathbb{Z}}$ has trivial G-action, and each P_i is finitely generated and projective in $\underline{\mathbf{PMod}}(\widehat{\mathbb{Z}}[\![G]\!])$. The group G is of type FP_∞ if it is of type FP_n for every $n \geq 0$.

[19] This follows from [Tat76, §2] upon noting that surjections of profinite groups admit a continuous set-theoretic section [RZ10, Proposition 2.2.2]

[20] By definition not all colimits/limits are allowed - the indexing poset must be a subset of $\mathbb{N}$. In particular any profinite $\widehat{\mathbb{Z}}[\![G]\!]$-module is ind-profinite, and any second-countable profinite $\widehat{\mathbb{Z}}[\![G]\!]$-module is pro-discrete. See [BCC16, §1-2].

Theorem 7.6 (Cook, [CC16])**.** *Any virtually poly pro-cyclic group is of type* FP_∞*. In particular this includes all profinite abelian groups.*

Theorem 7.7 ([BCC16])**.** *If* G *is a profinite group of type* FP_∞*, then* $H^0(G,M) = M^G$*,* $H^n(G,M)$ *agrees with Tate's continuous cohomology* $H^n_{cont}(G,M)$ *for all* n *and all* $M \in \underline{\boldsymbol{PD}}(\widehat{\mathbb{Z}}[\![G]\!])$*. Moreover* $H^n(G,-)$ *is a universal* δ*-functor.*

Proof. That $H^0(G,M) = M^G$ and agrees with Tate's continuous cohomology follows from [BCC16, Proposition 8.2, Corollary 8.3, 8.4]. The fact that $H^n(G,-)$ is a universal δ-functor is a bit more difficult. It follows from private communication with the second author of the paper, which I have not fully checked. □

8 References

[Asa01] Mamoru Asada, *The faithfulness of the monodromy representations associated with certain families of algebraic curves*, J. Pure Appl. Algebra **159** (2001), no. 2-3, 123–147. MR1828935

[Bac65] Seymour Bachmuth, *Automorphisms of free metabelian groups*, Transactions of the American Mathematical Society **118** (1965), 93–104.

[BBCL22] Renee Bell, Jeremy Booher, William Y. Chen, and Yuan Liu, *Tamely ramified covers of the projective line with alternating and symmetric monodromy*, Algebra Number Theory **16** (2022), no. 2, 393–446. MR4412578

[BCC16] Marco Boggi and Ged Corob Cook, *Continuous cohomology and homology of profinite groups*, Doc. Math. **21** (2016), 1269–1312. MR3578207

[BEL17] David El-Chai Ben-Ezra and Alexander Lubotzky, *The congruence subgroup problem for low rank free and free metabelian groups*, Journal of Algebra (2017).

[BER11] Kai-Uwe Bux, Mikhail V. Ershov, and Andrei S. Rapinchuk, *The congruence subgroup property for* $\operatorname{Aut} F_2$*: a group-theoretic proof of Asada's theorem*, Groups Geom. Dyn. **5** (2011), no. 2, 327–353. MR2782176

[CC16] Ged Corob Cook, *Bieri-Eckmann criteria for profinite groups*, Israel J. Math. **212** (2016), no. 2, 857–893. MR3505405

[Che17] Dawei Chen, *Teichmüller dynamics in the eyes of an algebraic geometer*, Surveys on recent developments in algebraic geometry, 2017, pp. 171–197. MR3727500

[Che18] William Yun Chen, *Moduli interpretations for noncongruence modular curves*, Math. Ann. **371** (2018), no. 1-2, 41–126. MR3788845

[Che21] William Chen, *Nonabelian level structures, nielsen equivalence, and markoff triples*, to appear in Annals of Math (2021), available at `2011.12940`.

[CLP16] Fabrizio Catanese, Michael Lönne, and Fabio Perroni, *Genus stabilization for the components of moduli spaces of curves with symmetries*, Algebr. Geom. **3** (2016), no. 1, 23–49. MR3455419

[Dav13] Rachel Davis, *Images of metabelian galois representations associated to elliptic curves*, Women in Numbers 2: Research Directions in Number Theory **606** (2013), 29.

[Del89] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), 1989, pp. 79–297. MR1012168

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109. MR262240

[DT06] Nathan M. Dunfield and William P. Thurston, *Finite covers of random 3-manifolds*, Invent. Math. **166** (2006), no. 3, 457–521. MR2257389

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786. MR3488737

[FV91] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800. MR1119950

[Lön20] Michael Lönne, *Branch stabilisation for the components of Hurwitz moduli spaces of Galois covers*, Galois covers, Grothendieck-Teichmüller Theory and Dessins d'Enfants, 2020, pp. 181–204. MR4166931

[LWZB19] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown, *A predicted distribution for galois groups of maximal unramified extensions*, arXiv preprint arXiv:1907.05002 (2019).

[Mat89] Hideyuki Matsumura, *Commutative ring theory*, Second, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989. Translated from the Japanese by M. Reid. MR1011461

[McD98] Aidan McDermott, *The nonabelian tensor product of groups: Computations and structural results*, Department of Mathematics facuality of arts national university of ireland galway (1998).

[Mel76] OV Mel'nikov, *The congruence kernel of the group* $SL_2(\mathbb{Z})$, Dokl. akad. nauk sssr, 1976, pp. 1034–1036.

[MKS04] Wilhelm Magnus, Abraham Karrass, and Donald Solitar, *Combinatorial group theory*, second, Dover Publications, Inc., Mineola, NY, 2004. Presentations of groups in terms of generators and relations. MR2109550

[PdJ95] M. Pikaart and A. J. de Jong, *Moduli of curves with non-abelian level structure*, The moduli space of curves (Texel Island, 1994), 1995, pp. 483–509. MR1363068

[RZ10] Luis Ribes and Pavel Zalesskii, *Profinite groups*, Second, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 40, Springer-Verlag, Berlin, 2010. MR2599132

[Ser06] Jean-Pierre Serre, *Lie algebras and Lie groups*, Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition. MR2179691

[Ser89] ______, *Abelian l-adic representations and elliptic curves*, Second, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute. MR1043865

[Sza09] Tamás Szamuely, *Galois groups and fundamental groups*, Vol. 117, Cambridge university press, 2009.

[Tam97] Akio Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), no. 2, 135–194. MR1478817

[Tat76] John Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR429837

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324

[Wil98] John S Wilson, *Profinite groups*, Vol. 19, Clarendon Press, 1998.

[Zoo01] V Zoonekynd, *The fundamental group of an algebraic stack*, arXiv preprint math (2001).