On the kernels of the pro-p outer Galois representations associated to once-punctured CM elliptic curves

Shun Ishii
ishii.shun@keio.jp

Department of Mathematics, Keio University, 3-14-1 Hiyoshi, Kouhoku-ku, Yokohama 223-8522, Japan.

Abstract

In this paper, we compare a certain field naturally arising from the kernel of the pro-p outer Galois representation associated to a once-punctured CM elliptic curve over an imaginary quadratic field K with the maximal pro-p Galois extension of the mod-p ray class field $K(p)$ of K unramified outside p. We prove that two fields coincide with each other for every prime p satisfying certain conditions, assuming an analogue of the Deligne-Ihara conjecture. This result is an analogue of Sharifi's result on the kernel of the kernel of the pro-p outer Galois representation associated to the thrice-punctured projective line.

Contents

1 Introduction

In this paper, we study the kernel of the pro-p outer Galois representations associated to once-punctured CM elliptic curves.

Let us recall the definition of the pro-p outer Galois representations: Suppose that X is a geometrically connected algebraic variety defined over a number field F. We denote the étale fundamental group of X by $\pi_1(X, \bar{x})$ where $\bar{x}$ is a (possibly tangential) basepoint. In the following, we write $\bar{X} \coloneqq X \times_F \bar{\mathbb{Q}}$. There is an exact sequence determined by the structure morphism $X \to \mathrm{Spec}(F)$:

$$1 \to \pi_1(\bar{X}, \bar{x}) \to \pi_1(X, \bar{x}) \to G_F \coloneqq \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to 1.$$

Hence this homotopy exact sequence, together with the conjugation action of $\pi_1(X, \bar{x})$ on $\pi_1(\bar{X}, \bar{x})$, determines the outer Galois representation

$$\rho_X : G_F \to \mathrm{Out}(\pi_1(\bar{X}, \bar{x})) \coloneqq \mathrm{Aut}(\pi_1(\bar{X}, \bar{x}))/\mathrm{Inn}(\pi_1(\bar{X}, \bar{x}))$$

which does not depend on the choice of basepoints. For a rational prime p, since the maximal pro-p quotient $\pi_1(\bar{X}, \bar{x})^{(p)}$ of $\pi_1(\bar{X}, \bar{x})$ is characteristic, ρ_X induces a homomorphism

$$\rho_{X,p} : G_F \to \mathrm{Out}(\pi_1(\bar{X}, \bar{x})^{(p)}),$$

which we call *the pro-p outer Galois representation associated to X*.

If X is a hyperbolic curve, such an outer representation is mainly studied in the context of anabelian geometry. In particular, it is known that ρ_X is injective if X is a hyperbolic curve, cf. Matsumoto [Mat96] when X is affine and Hoshi-Mochizuki [HM11] when X is proper.

As for the pro-p outer Galois representation associated to a hyperbolic curve X, it is far from being injective since the group $\mathrm{Out}(\pi_1(\bar{X}, \bar{x})^{(p)})$ contains an open subgroup which is pro-p. In particular, the fixed field of the kernel of $\rho_{X,p}$ is an almost pro-p extension over F, and, it seems to be interesting to study arithmetic properties of this extension.

In the case of the thrice-punctured projective line $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ over $\mathbb{Q}$ (see Appendix A for a brief summary of previous results), Anderson and Ihara [AI88, Theorem 2 (IV)] proved that the fixed field $\bar{\mathbb{Q}}^{\rho_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\},p}}$ is a nonabelian infinite pro-p extension over the field $\mathbb{Q}(\mu_{p^\infty})$ unramified outside p which is generated by all higher circular p-units. Moreover, They asked whether $\bar{\mathbb{Q}}^{\rho_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\},p}}$ is equal to the maximal pro-p extension of the p-th cyclotomic field $\mathbb{Q}(\mu_p)$ unramified outside p or not [AI88, page 272, (a)].

Regarding this question, Sharifi obtained the following answer for odd regular primes, assuming the Deligne-Ihara conjecture (Conjecture A.3) on the structure of a graded Lie algebra over $\mathbb{Q}_p$ associated to a certain filtration on the Galois group $G_{\mathbb{Q}}$:

Theorem (Sharifi [Sha02, Theorem 1.1], see also Theorem A.4)**.** *Assume that $p > 2$ is regular and the Deligne-Ihara conjecture holds for p. Then the fixed field $\bar{\mathbb{Q}}^{\rho_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\},p}}$ is the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p.*

Note that Hain-Matsumoto [HM03] and Brown [Bro12] proved the Deligne-Ihara conjecture for every prime p. Hence Anderson-Ihara's question is affirmative if p is odd and regular.

To the author's knowledge, Sharifi's theorem is the only case that a purely field-theoretic characterization of the fixed field $\bar{\mathbb{Q}}^{\rho_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\},p}}$ has been found among the pro-p outer Galois representations associated to hyperbolic curves over number fields.

In this paper, we prove an analogue of Sharifi's result in the case of once-punctured CM elliptic curves. For the precise statement of the following theorem and our strategy for the proof, see 2.2.

Theorem (Theorem 2.13)**.** *Let K be an imaginary quadratic field of class number one and $X := E \setminus O$ an once-punctured CM elliptic curve over K. Let $p \geq 5$ be a rational prime satisfying the following assumptions:*

1. *E has potentially good ordinary reduction at the primes above p,*
2. *the class number of the mod-p ray class field $K(p)$ is not divisible by p,*
3. *there are exactly two primes of the mod-p^∞ ray class field $K(p^\infty)$ above p, and*
4. *an analogue of the Deligne-Ihara conjecture (Conjecture 2.10) holds.*

Then the fixed field $\bar{\mathbb{Q}}^{\ker(\rho_{X,p})}$ is equal to the compositum of the field $K(E[p])$ and the maximal pro-p extension of $K(p)$ unramified outside p.

This paper proceeds as follows: In Section 2, we explain previous studies on the pro-p outer Galois representations associated to once-punctured elliptic curves, especially the construction of a certain series and Nakamura's explicit formula for this power series. Then we explain properties of certain Kummer characters associated to the power series, propose an analogue of the Deligne-Ihara conjecture and state the main result. In Section 3, we define a certain two-variable version of the descending central series for various profinite groups and establish their fundamental properties, which are essential to prove the main result. Section 4 is devoted to the proof of the main theorem. Finally, in App.A, we explain previous studies on the pro-p outer Galois representations associated to the thrice-punctured projective line which motivates our study.

Acknowledgements. This paper is essentially a part of the author's doctoral thesis submitted to Kyoto university. The author sincerely thanks for his advisor *Akio Tamagawa* for helpful comments. He also would like to express his gratitude to *Benjamin Collas* who read a draft of the thesis and gave him a lot of advice. This research is supported by JSPS KAKENHI Grand number 23KJ1882.

Notation

We will use the following notations throughout this paper:

Indexes. For a pair $\boldsymbol{m} = (m_1, m_2)$ in $\mathbb{Z}^2$, we write $|\boldsymbol{m}| \coloneqq m_1 + m_2$. Moreover, for an integer w, we write $\boldsymbol{m} \equiv 0 \bmod w$ if $\boldsymbol{m} \in (w\mathbb{Z})^2$. For any two pairs $\boldsymbol{m} = (m_1, m_2)$ and $\boldsymbol{n} = (n_1, n_2)$, we write $\boldsymbol{m} \geq \boldsymbol{n}$ if $m_i \geq n_i$ holds for every $i = 1, 2$. Moreover, we write $\boldsymbol{m} > \boldsymbol{n}$ if $\boldsymbol{m} \geq \boldsymbol{n}$ and $|\boldsymbol{m}| > |\boldsymbol{n}|$. Finally, we often denote $(1, 1)$ by $\mathbf{1}$.

Profinite Groups. For a profinite group G and a subset $S \subset G$, let $\langle S \rangle$ denote the closed subgroup of G topologically generated by S. We say that S generates G if $G = \langle S \rangle$. Moreover, we say that S *strongly* generates G if S generates G and S converges to 1, i.e. every open subgroup of G contains all but a finite number of elements of S.

Let $\langle S \rangle_{\mathrm{normal}}$ denote the minimal normal closed subgroup of G containing S. We call $\langle S \rangle_{\mathrm{normal}}$ the normal closure of S. If $G = \langle S \rangle_{\mathrm{normal}}$, then we say S *normally* generates G.

The descending central series $\{G(m)\}_{m \geq 1}$ of G is defined by

$$G(1) \coloneqq G \quad \text{and} \quad G(m) \coloneqq \langle [G(m'), G(m'')] \mid m' + m'' = m \rangle \quad (m \geq 2).$$

where, for every pair of subgroups $H, K \subset G$, $[H, K]$ denotes the topological closure of the commutator subgroup of H and K.

We denote the maximal abelian quotient of G by $G^{\mathrm{ab}} = G/G(2)$ and the maximal pro-p quotient of G by $G^{(p)}$ for a prime p.

We denote the (continuous) automorphism group of G by $\mathrm{Aut}(G)$, the inner automorphism group by $\mathrm{Inn}(G)$ and the outer automorphism group of G by $\mathrm{Out}(G) \coloneqq \mathrm{Aut}(G)/\mathrm{Inn}(G)$. For $g \in G$, the corresponding inner automorphism is denoted by $\mathrm{inn}(g)$.

In this paper, every free pro-p group is assumed to be a free pro-p group on a set converging to 1 (see Ribes-Zalesskii [RZ10, Lemma 3.3.4] for its characterization).

Number Fields. Throughout this paper, we fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and an embedding from $\bar{\mathbb{Q}}$ into $\mathbb{C}$. Every number field is considered to be a subfield of $\bar{\mathbb{Q}}$.

For a subfield F of $\bar{\mathbb{Q}}$, we denote the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ of F by G_F and the ring of integers in F by O_F. We denote the set of m-th roots of unity in $\bar{\mathbb{Q}}$ by μ_m.

For a prime p, we denote the set of primes of F above p by $\Sigma_p(F)$. Moreover, for a place v of F, we denote the v-adic completion of F by F_v.

Imaginary Quadratic Fields. Let K be an imaginary quadratic field.

For a nonzero integral ideal $\mathfrak{m}$ of K, we denote the ray class field of K modulo $\mathfrak{m}$ by $K(\mathfrak{m})$ and write $K(\mathfrak{m}^\infty) := \cup_{n\geq 1} K(\mathfrak{m}^n)$. If $\alpha \in O_K$ generates $\mathfrak{m}$, we sometimes denote $K(\mathfrak{m})$ and $K(\mathfrak{m}^\infty)$ by $K(\alpha)$ and $K(\alpha^\infty)$, respectively.

Elliptic Curves with Complex Multiplication. Let K be an imaginary quadratic field and (E, O) an elliptic curve over K with its origin $O \in E(K)$ which has complex multiplication by O_K.

For an ideal $\mathfrak{m}$ of O_K, we denote the $\mathfrak{m}$-torsion subgroup scheme of E by $E[\mathfrak{m}]$. The G_K-action on $E[\mathfrak{m}](\bar{\mathbb{Q}})$ determines an injective homomorphism

$$\mathrm{Gal}(K(E[\mathfrak{m}])/K) \hookrightarrow \mathrm{Aut}(E[\mathfrak{m}](\bar{\mathbb{Q}})) \cong (O_K/\mathfrak{m})^\times.$$

Moreover, this homomorphism induces an isomorphism

$$\mathrm{Gal}(K(\mathfrak{m})/K) \xrightarrow{\sim} (O_K/\mathfrak{m})^\times/\mathrm{im}(O_K^\times)$$

which does not depend on the choice of E.

For a prime p, we denote the p-adic Tate module of E by $T_p(E)$. If p splits into two distinct primes in O_K as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, let $T_{\mathfrak{p}}(E)$ (resp. $T_{\bar{\mathfrak{p}}}(E)$) denote the inverse limit $\varprojlim_n E[\mathfrak{p}^n](\bar{\mathbb{Q}})$ (resp. $\varprojlim_n E[\bar{\mathfrak{p}}^n](\bar{\mathbb{Q}})$) whose transition maps are taken to be multiplication by p. They determine two characters

$$\chi_1 \colon G_K \to \mathrm{Aut}(T_{\mathfrak{p}}(E)) \cong \mathbb{Z}_p^\times \quad \text{and} \quad \chi_2 \colon G_K \to \mathrm{Aut}(T_{\bar{\mathfrak{p}}}(E)) \cong \mathbb{Z}_p^\times.$$

Note that $\chi_1\chi_2 = \chi_{\mathrm{cyc}}$, the p-adic cyclotomic character.

For $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2$, we define

$$\chi^{\boldsymbol{m}} := \chi_1^{m_1}\chi_2^{m_2} \colon G_K \to \mathbb{Z}_p^\times.$$

The character $\chi^{\boldsymbol{m}}$ factors through $\mathrm{Gal}(K(p^\infty)/K)$ if $m_1 \equiv m_2 \bmod |O_K^\times|$.

For a $\mathbb{Z}_p$-module M on which G_K acts continuously, we denote the $\chi^{\boldsymbol{m}}$-twist of M by $M(\boldsymbol{m})$. Using this notation, we have $T_{\mathfrak{p}}(E) \cong \mathbb{Z}_p(1,0)$, $T_{\bar{\mathfrak{p}}}(E) \cong \mathbb{Z}_p(0,1)$ and $\mathbb{Z}_p(m,m)$ is simply the m-th Tate twist $\mathbb{Z}_p(m)$.

2 Preliminaries

In this section, we prepare backgrounds which are necessary to explain the main result of this paper (Theorem 2.13). In the following we explain:

- construction of a certain basis $\{x_1, x_2\}$ of the pro-p geometric fundamental group of once-punctured CM elliptic curve X, cf. Lemma 2.1,
- construction of an elliptic analogue of Ihara's universal power series for Jacobi sums and Nakamura's explicit formula of that power series, cf. Section 2.1,
- conditional nonvanishing and surjectivity of certain Kummer characters associated to that power series, cf. Theorem 2.7 and Theorem 2.8,

- formulation of an analogue of the Deligne-Ihara conjecture and state the main result, cf. Section 2.2.

In the following of this paper, let K be an imaginary quadratic field of class number one and $p \geq 5$ a prime which splits into two prime ideals in O_K as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$.

Let (E, O) be an elliptic curve which has complex multiplication by O_K. We denote the associated *once-punctured CM elliptic curve* by $X \coloneqq E \setminus O$ and its pro-p geometric fundamental group $\pi_1(\bar{X})^{(p)}$ with respect to a possibly tangential basepoint by $\Pi_{1,1}$. Since $\Pi_{1,1}$ is isomorphic to the pro-p completion of the topological fundamental group of $X(\mathbb{C})$, we can identify $\Pi_{1,1}$ with a free pro-p group of rank two with basis $\{x, y\}$ in such a way that $[y, x]$ generates an inertia subgroup at O.

Note that the pro-p geometric fundamental group $\Pi_{1,0}$ of E is isomorphic to $\Pi_{1,1}^{\mathrm{ab}}$ through a homomorphism $\Pi_{1,1}^{\mathrm{ab}} \to \Pi_{1,0}$ induced by the inclusion $X \hookrightarrow E$. Moreover, we have a natural isomorphism $T_p(E) \xrightarrow{\sim} \Pi_{1,0}$.

Throughout this paper, we fix the following particular basis $\{x_1, x_2\}$ of $\Pi_{1,1}$.

Lemma 2.1. *We can choose a basis $\{x_1, x_2\}$ of $\Pi_{1,1}$ in such a way that*

1. *Let $(\omega_{1,n})_{n\geq 1}$ (resp. $(\omega_{2,n})_{n\geq 1}$) denote the image of x_1 (resp. x_2) in $\Pi_{1,1}^{\mathrm{ab}} \cong T_p(E) = T_{\mathfrak{p}}(E) \oplus T_{\bar{\mathfrak{p}}}(E)$. Then $(\omega_{1,n})_{n\geq 1}$ (resp. $(\omega_{2,n})_{n\geq 1}$) generates $T_{\mathfrak{p}}(E)$ (resp. $T_{\bar{\mathfrak{p}}}(E)$).*
2. *$z \coloneqq [x_2, x_1]$ generates the inertia subgroup $\langle [y, x] \rangle$ at O.*

Proof. The assertion immediately follows from the fact that the natural map $\tilde{\Gamma}_{1,1} \to \mathrm{Aut}(\Pi_{1,1}^{\mathrm{ab}})$ is surjective (for the definition of $\tilde{\Gamma}_{1,1}$, see the next subsection) by a result of Kaneko [Kan89, Proposition 2] and every inner automorphism of $\Pi_{1,1}$ acts trivially on the maximal abelian quotient. □

2.1 An analogue of Ihara's power series and Soulé characters

In this subsection, we introduce a certain power series which expresses the action of the Galois group $G_{K(E[p^\infty])}$ on the maximal meta-abelian quotient of $\Pi_{1,1}$. This power series can be regarded as an analogue of Ihara's power series, cf. App A for a brief account, and was firstly considered in a letter of Bloch to Deligne, according to Nakamura [Nak95] and Tsunogai [Tsu95].

Then we explain Nakamura's explicit formula of that power series. Certain Kummer character, which we call *elliptic Soulé characters* in this paper, appear as coefficients of that power series. In [Ish23], we proved elliptic Soulé characters are nontrivial or even surjective under certain assumptions.

First, we define

$$\tilde{\Gamma}_{1,1} \coloneqq \{f \in \mathrm{Aut}(\Pi_{1,1}) \mid f \text{ preserves the conjugacy class of inertia subgroups at } O\},$$

its subgroup

$$\Gamma_{1,1}^{\dagger} \coloneqq \{f \in \mathrm{Aut}(\Pi_{1,1}) \mid f \text{ preserves } \langle z \rangle\}^{1},$$

and a quotient $\Gamma_{1,1} \coloneqq \tilde{\Gamma}_{1,1}/\mathrm{Inn}(\Pi_{1,1})$ which is called *the pro-p mapping class group of type* $(1,1)$. This group comes equipped with a descending central filtration $\{F^m\tilde{\Gamma}_{1,1}\}_{m\geq 1}$ defined by

$$F^m\tilde{\Gamma}_{1,1} \coloneqq \ker\left(\tilde{\Gamma}_{1,1} \to \mathrm{Aut}(\Pi_{1,1}/\Pi_{1,1}(m+1))\right)$$

for every $m \geq 1$. This filtration naturally induces filtrations on $\Gamma_{1,1}^{\dagger}$ and $\Gamma_{1,1}$ by

$$F^m\Gamma_{1,1}^{\dagger} \coloneqq \Gamma_{1,1}^{\dagger} \cap F^m\tilde{\Gamma}_{1,1} \quad \text{and} \quad F^m\Gamma_{1,1} \coloneqq F^m\tilde{\Gamma}_{1,1}\mathrm{Inn}(\Pi_{1,1})/\mathrm{Inn}(\Pi_{1,1}),$$

respectively.

Since $\cap_{m\geq 1}\Pi_{1,1}(m+1) = \{1\}$, it holds that the intersection $\cap_{m\geq 1}F^m\tilde{\Gamma}_{1,1}$ is trivial. Moreover, the intersection $\cap_{m\geq 1}F^m\Gamma_{1,1}$ is also known to be trivial, see Asada [Asa95, Theorem 2], for example.

Since the normalizer subgroup of $\langle z \rangle$ in $\Pi_{1,1}$ is equal to $\langle z \rangle$ itself and $z \in \Pi_{1,1}(2) \setminus \Pi_{1,1}(3)$, it follows that the intersection $F^m\Gamma_{1,1}^{\dagger} \cap \mathrm{Inn}(\Pi_{1,1})$ is trivial for every $m \geq 3$ and is equal to $\langle \mathrm{inn}(z) \rangle$ for $m = 1, 2$. Hence the natural projection $F^m\Gamma_{1,1}^{\dagger} \to F^m\Gamma_{1,1}$ is an isomorphism for every $m \geq 3$ and is surjective with $\langle \mathrm{inn}(z) \rangle$ as its kernel for $m = 1, 2$ [Nak95, (4.4)].

We define subgroups $\Psi_1^{\dagger} \subset \Psi^{\dagger} \subset \mathrm{Aut}\left(\Pi_{1,1}/[\Pi_{1,1}(2), \Pi_{1,1}(2)]\right)$ by

$$\Psi^{\dagger} \coloneqq \{f \in \mathrm{Aut}\left(\Pi_{1,1}/[\Pi_{1,1}(2), \Pi_{1,1}(2)]\right) \mid f \text{ preserves } \langle \bar{z} \rangle\}$$

and

$$\Psi_1^{\dagger} \coloneqq \ker\left(\Psi^{\dagger} \to \mathrm{Aut}(\Pi^{\mathrm{ab}})\right),$$

where $\bar{z} \in \Pi_{1,1}(2)/[\Pi_{1,1}(2), \Pi_{1,1}(2)]$ is the image of z under the natural projection. We shall identify $\mathbb{Z}_p[[\Pi_{1,1}^{\mathrm{ab}}]]$ with $\mathbb{Z}_p[[T_1, T_2]]$ via $T_i \coloneqq x_i - 1$ for $i = 1, 2$. The action of $\mathrm{Aut}(\Pi_{1,1}^{\mathrm{ab}}) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ on $\Pi_{1,1}^{\mathrm{ab}}$ extends to that of $\mathbb{Z}_p[[\Pi_{1,1}^{\mathrm{ab}}]] \cong \mathbb{Z}_p[[T_1, T_2]]$ in a natural way.

Apparently, every element $f \in \Psi_1^{\dagger}$ is determined by a pair $f(x_i)x_i^{-1} \in \Pi_{1,1}(2)/[\Pi_{1,1}(2), \Pi_{1,1}(2)]$ for $i = 1, 2$. Since $\Pi_{1,1}(2)/[\Pi_{1,1}(2), \Pi_{1,1}(2)]$ is a free $\mathbb{Z}_p[[T_1, T_2]]$-module generated by $\bar{z}$ by [Iha86b, Theorem 2], there exists a unique element $G_i(f) \in \mathbb{Z}_p[[T_1, T_2]]$ such that $f(x_i)x_i^{-1} = G_i(f)z$ for $i = 1, 2$.

Lemma 2.2 (Nakamura [Nak95, (4.7)], Tsunogai [Tsu95, Proposition 1.9]). *For every* $f \in \Psi_1^{\dagger}$, $G_1(f)$ *and* $G_2(f)$ *satisfies*

$$T_1G_2(f) - G_1(f)T_2 = 0.$$

[1] In [Nak95], this subgroup is denoted by $\Gamma_{1,1}^{*}$. Since we use the symbol $*$ to refer to different kinds of objects in this paper, we use the symbol $\dagger$ instead.

If we write $H(f) \coloneqq \frac{G_2(f)}{T_2} = \frac{G_1(f)}{T_1}$, then $H\colon \Psi_1^\dagger \to \mathbb{Z}_p[[T_1, T_2]]$ is an isomorphism. Moreover, $\mathrm{GL}_2(\mathbb{Z}_p)$-action on $\Psi_1^\dagger$ induced by the exact sequence

$$1 \to \Psi_1^\dagger \to \Psi \to \mathrm{GL}_2(\mathbb{Z}_p) \to 1$$

makes $H\colon \Psi_1^\dagger \xrightarrow{\sim} \mathbb{Z}_p[[T_1, T_2]](1)$ equivariant. Here (1) means the twist by the determinant character.

In the following, we shall exploit the following section

$$s\colon G_{K(E[p^\infty])} \to F^3\Gamma_{1,1}^\dagger$$

whose construction is as follows: it holds that $F^1\Gamma_{1,1} = F^2\Gamma_{1,1} = F^3\Gamma_{1,1}$ [Nak95, (4.4)]. Hence the image of $G_{K(E[p^\infty])}$ under $\rho_{X,p}$ is contained in $F^3\Gamma_{1,1}$. By composing the inverse of the natural projection $F^3\Gamma_{1,1}^\dagger \xrightarrow{\sim} F^3\Gamma_{1,1}$, we obtain a homomorphism $s\colon G_{K(E[p^\infty])} \to F^3\Gamma_{1,1}^\dagger$ which lifts $\rho_{X,p}\mid_{G_{K(E[p^\infty])}}$.

Definition 2.1. We define a $\mathrm{Gal}(K(E[p^\infty])/K)$-equivariant homomorphism

$$\alpha_{1,1}\colon G_{K(E[p^\infty])} \to \mathbb{Z}_p[[T_1, T_2]](1)$$

as a compositum of the following three homomorphisms:

1. the section $s\colon G_{K(E[p^\infty])} \to F^3\Gamma_{1,1}^\dagger$ constructed above,
2. the natural projection $F^3\Gamma_{1,1}^\dagger \to \Psi_1^\dagger$, and
3. the isomorphism $H\colon \Psi_1^\dagger \xrightarrow{\sim} \mathbb{Z}_p[[T_1, T_2]](1)$ in Lemma 2.2.

In [Nak95], Nakamura obtained an explicit description of $\alpha_{1,1}$ in terms of special values of the fundamental theta functions. We fix a Weierstrass form of $E\colon y^2 = 4x^3 - g_2x - g_3$ with $g_2, g_3 \in K$ and a corresponding lattice $\mathcal{L} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ of $E(\mathbb{C})$ with $\frac{\omega_1}{\omega_2}$ belonging to the upper half plane. Then the fundamental theta function $\theta(z, \mathcal{L})$, which is a certain nonholomorphic function on $\mathbb{C}$, is defined as in [Nak95, (2.1)], see also de Shalit [dS87, Chapter II, 2.1]).

In the following formula, we use the convention $0^0 \coloneqq 1$ and regard $\mathbb{Z}_p[[T_1, T_2]]$ as a subring of $\mathbb{Q}_p[[U_1, U_2]]$ where $U_i \coloneqq \log(1 + T_i)$.

Theorem 2.3 (Nakamura [Nak95, Theorem (A) and (3.11.5)])**.**

$$\alpha_{1,1}(\sigma) = \sum_{m \geq 2\colon\ even}^{\infty} \frac{1}{1 - p^m} \sum_{\substack{\boldsymbol{m}=(m_1,m_2)\geq(0,0)\\ |\boldsymbol{m}|=m}} \kappa_{\boldsymbol{m}+\boldsymbol{1}}(\sigma) \frac{U_1^{m_1}U_2^{m_2}}{m_1!m_2!}$$

holds for every $\sigma \in G_{K(E[p^\infty])}$. Here, $\kappa_{\boldsymbol{m}}\colon G^{\mathrm{ab}}_{K(E[p^\infty])} \to \mathbb{Z}_p$ is a Kummer character whose reduction modulo p^n corresponds to the p^n-th root of

$$\prod_{\substack{0\leq a,b<p^n\\ p\nmid \gcd(a,b)}} \theta(a\omega_{1,n} + b\omega_{2,n}, \mathcal{L})^{a^{m_1-1}b^{m_2-1}}$$

for every $n \geq 1$.

Remark 2.4. *Nakamura originally proved Theorem 2.3 for once-punctured elliptic curves defined over arbitrary number fields, not only for once-punctured CM elliptic curves.*

Definition 2.2 (The elliptic Soulé character)**.** For every $\boldsymbol{m} = (m_1, m_2) > \mathbf{1}$ such that $|\boldsymbol{m}|$ is even, we call the character $\kappa_{\boldsymbol{m}}$ appearing in Theorem 2.3 *the* $\boldsymbol{m}$*-th elliptic Soulé character* associated to X.

Remark 2.5. *More precisely, we should call $\kappa_{\boldsymbol{m}}$ the $\boldsymbol{m}$-th elliptic Soulé character with respect to $\{x_1, x_2\}$ since it depends on the choice of the basis. However, it can be shown that $\kappa_{\boldsymbol{m}}$ depends only on the image of $\{x_1, x_2\}$ in $\Pi_{1,1}^{\mathrm{ab}}$ and the degree m-part of the power series $\alpha_{1,1}$ gives a well-defined element of $\mathrm{Hom}_{\mathrm{Gal}(K(E[p^\infty])/K)}(G_{K(E[p^\infty])}^{\mathrm{ab}}, \mathrm{Sym}^m T_p(E)(1))$ which does not depend on the choice of the basis.*

Nakamura observed that some linear combinations of elliptic Soulé characters are nontrivial [Nak95, (3.12)]. In [Ish23], we further studied the elliptic Soulé characters arising from once-punctured CM elliptic curves. We summarize the results obtained in [Ish23].

First, with respect to our basis $\{x_1, x_2\}$, the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}}$ is a $\mathrm{Gal}(K(E[p^\infty])/K)$-equivariant homomorphism

$$\kappa_{\boldsymbol{m}} \colon G_{K(E[p^\infty])} \to \mathbb{Z}_p(\boldsymbol{m})$$

for every $\boldsymbol{m} = (m_1, m_2) > \mathbf{1}$ such that $|\boldsymbol{m}|$ is even. Let

$$I \coloneqq \{\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}_{\geq 1}^2 \setminus \{\mathbf{1}\} \mid m_1 \equiv m_2 \bmod |O_K^\times|\}.$$

Since the outer action of the automorphism group $\mathrm{Aut}_K(X)$ on the fundamental group commutes with the Galois action, one can observe the following lemma.

Lemma 2.6 ([Ish23, Lemma 3.1])**.** *The character $\kappa_{\boldsymbol{m}}$ is trivial unless $\boldsymbol{m} \in I$.*

For $\boldsymbol{m} \in I$, we proved the following conditional nonvanishing of the $\boldsymbol{m}$-th elliptic Soulé character. The proof relies on the Iwasawa main conjecture for imaginary quadratic fields proved by Rubin [Rub91].

Theorem 2.7 ([Ish23, Theorem 1.4 (1)])**.** *Let $\boldsymbol{m} \in I$ and assume that $H_{\text{ét}}^2(O_K[\frac{1}{p}], \mathbb{Z}_p(\boldsymbol{m}))$ is finite. Then the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}} \colon G_{K(E[p^\infty])} \to \mathbb{Z}_p(\boldsymbol{m})$ is nontrivial.*

Here, $H_{\text{ét}}^2(O_K[\frac{1}{p}], \mathbb{Z}_p(\boldsymbol{m}))$ is the second étale cohomology group of the spectrum of the ring of p-integers of K whose finiteness is a special case of [Jan89, Conjecture 1]. For example, such a cohomology group is known to be finite for every $\boldsymbol{m} \in (p-1)\mathbb{Z}_{\geq 1}^2$.

Moreover, a similar finiteness on the second étale cohomology group with coefficient in $\mathbb{Z}_p(m)$ for odd $m \geq 3$ is used to establish the nontriviality of the m-th Soulé character κ_m, cf. the proof of Ichimura-Sakaguchi [IS87, Theorem

B]. Such a finiteness holds unconditionally by a result of Soulé [Sou79, page 287, Corollaire].

We also observed the surjectivity of the elliptic Soulé characters under certain assumptions on p by using *elliptic units*.

Theorem 2.8 ([Ish23, Theorem 1.4 (2) and (3)])**.** *The elliptic Soulé characters have the following properties:*

1. *$\kappa_{\boldsymbol{m}}$ is not surjective for every $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv \mathbf{1} \mod p-1$.*
2. *If the class number of $K(p)$ is not divisible by p and there exists a unique prime of $K(p)$ above $\mathfrak{p}$, then $\kappa_{\boldsymbol{m}}$ is surjective for every $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \not\equiv \mathbf{1} \mod p-1$.*

We remark that, although $\kappa_{\boldsymbol{m}}$ is not surjective for every $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv \mathbf{1} \mod p-1$, it is nontrivial by Theorem 2.7 since $H^2_{\text{ét}}(O_K[\frac{1}{p}], \mathbb{Z}_p(m))$ is finite by a result of Soulé [Sou79, page 287, Corollaire].

2.2 Analogue of the Deligne-Ihara conjecture and its consequence

In this subsection, we formulate an analogue of the Deligne-Ihara conjecture. Then we study some fundamental properties of the fixed field of $\ker(\rho_{X,p})$ and state the main result in a precise manner.

The absolute Galois group G_K inherits a descending central filtration $\{F^m G_K\}_{m\geq 1}$ by $F^m G_K := \rho_{X,p}^{-1}(F^m\Gamma_{1,1})$. For example, $F^1 G_K = G_{K(E[p^\infty])}$. We can form graded quotients and their directed sum

$$\mathfrak{g}_m := F^m G_K / F^{m+1} G_K \text{ for } m \geq 1 \text{ and } \mathfrak{g} := \bigoplus_{m\geq 1} \mathfrak{g}_m.$$

It is known that:

- Each $\mathfrak{g}_m$ is naturally embedded into $F^m\Gamma_{1,1}/F^{m+1}\Gamma_{1,1}$, which is known to be a free $\mathbb{Z}_p$-module of finite rank [NT93, Corollary (1.16), (ii)].
- Each $\mathfrak{g}_m \otimes \mathbb{Q}_p$ is isomorphic to a finite direct sum of (a finite direct sum of) $\mathbb{Q}_p(\boldsymbol{m})$'s, where $\boldsymbol{m} \in \mathbb{Z}^2_{\geq 1}$ is an index satisfying $|\boldsymbol{m}| = m$. The assertion follows from the $\mathrm{GL}_2(\mathbb{Z}_p)$-equivariance of the commutative diagram given in Nakamura-Tsunogai [NT93, Theorem (1.14)].

Recall the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}} \colon F^1 G_K \to \mathbb{Z}_p(\boldsymbol{m})$ in the previous subsection. We have the following two lemma.

Lemma 2.9. *For $\boldsymbol{m} \in I$, the following assertions hold.*

1. *If $\kappa_{\boldsymbol{m}} \colon F^1 G_K \to \mathbb{Z}_p(\boldsymbol{m})$ is nontrivial, then the restricted character $\kappa_{\boldsymbol{m}} |_{F^{|\boldsymbol{m}|} G_K}$ is also nontrivial.*

2. *The restricted character $\kappa_{\boldsymbol{m}} \mid_{F^{|\boldsymbol{m}|}G_K}$ factors through $\mathfrak{g}_{|\boldsymbol{m}|}$.*

Proof. In the following proof, we denote $|\boldsymbol{m}|$ by m. (1) Suppose that the restricted character $\kappa_{\boldsymbol{m}} \mid_{F^m G_K}$ vanishes. Then there exists an integer $1 \leq n < m$ such that $\kappa_{\boldsymbol{m}} \mid_{F^{n+1}G_K} = 0$ but $\kappa_{\boldsymbol{m}} \mid_{F^n G_K} \neq 0$. This implies that $\mathfrak{g}_n \otimes \mathbb{Q}_p$ has a nontrivial $\chi^{\boldsymbol{m}}$-isotypic component, which is absurd since $n < m = |\boldsymbol{m}|$.

(2) It suffices to prove that $\kappa_{\boldsymbol{m}}$ vanishes on $F^{m+2}G_K$ since we have $F^{m+1}G_K = F^{m+2}G_K$ by [Nak95, (4.2) Proposition]. By the construction of the power series $\alpha_{1,1}(\sigma) \in \mathbb{Z}_p[[T_1, T_2]]$, it follows that, for $\sigma \in F^{m+2}G_K$,

$$T_1 \alpha_{1,1}(\sigma) z \in \Pi_{1,1}(m+3)\Pi_{1,1}(2)/[\Pi_{1,1}(2), \Pi_{1,1}(2)] \subset \mathbb{Z}_p[[T_1, T_2]]z.$$

Note that $\Pi_{1,1}(m+3)\Pi_{1,1}(2)/[\Pi_{1,1}(2), \Pi_{1,1}(2)]$ is isomorphic to J^{m+1} where J is the augmentation ideal of $\mathbb{Z}_p[[T_1, T_2]]$, cf. [Iha86b, (19) on page 67]). It follows that $T_1\alpha_{1,1}(\sigma) \in J^{m+1}$, hence $\alpha_{1,1}(\sigma) \in J^m$. This is equivalent to saying that every coefficient of $\alpha_{1,1}(\sigma)$ of a monomial with total degree less than m vanishes. By observing Theorem 2.3, it follows that $\kappa_{\boldsymbol{n}}(\sigma)$ vanishes for every $\boldsymbol{n} \in I$ such that $|\boldsymbol{n}| \leq m - 2$. □

Now we propose an analogue of the Deligne-Ihara conjecture:

Conjecture 2.10. *For every $\boldsymbol{m} \in I$, let $\sigma_{\boldsymbol{m}}$ be an element of $\mathfrak{g}$ such that*

1. *$\sigma_{\boldsymbol{m}}$ is contained in the $\chi^{\boldsymbol{m}}$-isotypic component of $\mathfrak{g}_{|\boldsymbol{m}|}$, and*
2. *$\kappa_{\boldsymbol{m}}(\sigma_{\boldsymbol{m}})$ generates $\kappa_{\boldsymbol{m}}(F^{|\boldsymbol{m}|}G_K) \subset \mathbb{Z}_p(\boldsymbol{m})$.*

Then the graded Lie algebra $\mathfrak{g} \otimes \mathbb{Q}_p$ is freely generated by $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$.

We now turn our attention to field-theoretic properties of the fixed field of $\ker(\rho_{X,p})$. First, we have the following lemma:

Lemma 2.11. *The field $\bar{K}^{\ker(\rho_{X,p})}$ is a pro-p extension of $K(E[p])$ unramified outside p.*

Proof. By the theory of specialization homomorphisms of étale fundamental groups, it suffices to prove that X has good reduction outside p over $K(E[p])$. To prove this claim, it suffices to prove that every inertia subgroup I over an arbitrary prime of $K(p)$ outside p acts trivially on $T_p(E)$ by the Néron-Ogg-Shafarevich criterion.

Since E has complex multiplication, E has everywhere potentially good reduction. This implies that the image of I in $\mathrm{Aut}(T_p(E))$ is finite. Moreover, the image of I is contained in $\ker(\mathrm{Aut}(T_p(E)) \to \mathrm{Aut}(E[p]))$, which is a torsion-free pro-p group for every $p \geq 5$. This concludes the proof. □

Lemma 2.12. *The field $\bar{K}^{\ker(\rho_{X,p})}$ is a compositum of $K(E[p])$ and a subfield $\Omega^* \subset \bar{K}^{\ker(\rho_{X,p})}$ which is unramified outside p. Moreover, the Galois group $\mathrm{Gal}(\bar{K}^{\ker(\rho_{X,p})}/K(p))$ naturally splits into the direct product of the finite abelian prime-to-p group $\mathrm{Gal}(K(E[p])/K(p))$ and the pro-p group $\mathrm{Gal}(\Omega^*/K(p))$.*

Proof. Consider the exact sequence

$$1 \to \rho_{X,p}(G_{K(E[p])}) \to \rho_{X,p}(G_{K(p)}) \to \mathrm{Gal}(K(E[p])/K(p)) \to 1.$$

Since $\rho_{X,p}(G_{K(E[p])})$ is pro-p and $\mathrm{Gal}(K(E[p])/K(p))$ is prime-to-p (here we use $p \geq 5$), this sequence splits. Let $t\colon \mathrm{Gal}(K(E[p])/K(p)) \to \rho_{X,p}(G_{K(p)})$ be an arbitrary section.

By functoriality of étale fundamental groups, there exists a natural homomorphism $\mathrm{Aut}_K(X) \to \mathrm{Out}(\Pi_{1,1})$ which does not depend on the choice of basepoints and the image of $\mathrm{Aut}_K(X)$ centralizes $\rho_p(G_K)$.

Observe that $\mathrm{Gal}(K(E[p])/K(p))$ is isomorphic to a subgroup of $\mathrm{Aut}_K(X)$ in $\mathrm{Aut}_{O_K}(E[p])$ under the Galois representation. Note that $\mathrm{Aut}_K(X) = O_K^\times$ injects into $\mathrm{Aut}_{O_K}(E[p]) = (O_K/p)^\times$ since p is prime to the order of $O_K^\times$ by assumption.

Hence for every $g \in \mathrm{Gal}(K(E[p])/K(p))$, we can find a unique element $\tilde{g} \in \mathrm{Aut}_K(X)$ such that $t(g)$ and $\tilde{g}$ coincide in $\mathrm{Out}(\Pi_{1,1}^{\mathrm{ab}}/p) = \mathrm{Aut}(E[p])$. Since the element $t(g)\tilde{g}^{-1}$ has a prime-to-p order and is contained in the pro-p group $\ker\left(\mathrm{Out}(\Pi_{1,1}) \to \mathrm{Out}(\Pi_{1,1}^{\mathrm{ab}}/p)\right)$, it follows that $t(g) = \tilde{g}$.

This argument shows that $t(\mathrm{Gal}(K(E[p])/K(p)))$ coincides with the image of a subgroup of $\mathrm{Aut}_K(X)$ in $\mathrm{Out}(\Pi_{1,1})$, hence is contained in the center of $\rho_{X,p}(G_K)$. In particular, the section t induces the decomposition

$$\rho_{X,p}(G_{K(p)}) = \rho_{X,p}(G_{K(E[p])}) \times t(\mathrm{Gal}(K(E[p])/K(p))).$$

Now let Ω^* be the field corresponding to the kernel of the projection $\rho_{X,p}(G_{K(p)}) \to \rho_{X,p}(G_{K(E[p])})$. Then it is clear that Ω^* is a pro-p extension of $K(p)$ unramified outside p and the Galois group $\rho_{X,p}(G_{K(p)}) = \mathrm{Gal}(\bar{K}^{\ker(\rho_{X,p})}/K(p))$ has the required decomposition. $\square$

Let Ω be the maximal pro-p extension of $K(p)$ which is unramified outside p. Our analogue of Anderson-Ihara's question [AI88, page 272, (a)] is :

Is the field Ω^* is equal to the field Ω?

Recalling Sharifi's result (Theorem A.4) characterizing the kernel of the pro-p outer Galois representation associated to the thrice-punctured elliptic curve for odd regular primes under the Deligne-Ihara conjecture, one may wonder if this question is also affirmative if Conjecture 2.10 and a certain condition on p are satisfied. This is the main result of this paper:

Theorem 2.13. *Assume that the following conditions hold:*

1. *the class number of $K(p)$ is not divisible by p,*
2. *there are exactly two primes of $K(p^\infty)$ above p, and*
3. *Conjecture 2.10 holds.*

Then we have the equality $\Omega^* = \Omega$.

Our strategy to prove Theorem 2.13 is to generalize Sharifi's technique developed in [Sha02] to a certain two-variable situation. To accomplish this, we introduce a two-variable filtration on the pro-p geometric fundamental group $\Pi_{1,1}$, on the pro-p mapping class group $\Gamma_{1,1}$ and on the absolute Galois group G_K and establish their fundamental properties in the next section.

Moreover, the Galois group $\mathrm{Gal}(\Omega/K(p))$ has a nontrivial relation for every split prime $p \geq 5$ unlike in the case of the Galois group of the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p for odd regular p, which is one of the main objects in [Sha02]. Hence we need to take such a nontrivial relation into consideration when following Sharifi's approach.

3 Two-variable filtrations on profinite groups

In this section, we define two-variable filtrations on various groups related to our study, e.g. the pro-p geometric fundamental groups of once-punctured elliptic curves, the pro-p mapping class group of type $(1,1)$ and Galois groups, and prove some fundamental properties required in this paper.

Throughout this section, Let Π denote a free pro-p group of rank two Π and we fix a free basis $\{x, y\}$ of Π. Moreover, we set $z := [y, x]$.

3.1 Two-variable filtration on free pro-p group of rank two

First, we define a two-variable variant of the descending central series on Π.

Definition 3.1. We inductively define a normal subgroup $\Pi(\boldsymbol{m})$ of Π for $\boldsymbol{m} \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$ as follows:

1. Let $\Pi(1,0)$ (resp. $\Pi(0,1)$) be the normal closure of x (resp. y) in Π.
2. For $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 0}$ with $|\boldsymbol{m}| \geq 2$, we define $\Pi(\boldsymbol{m}) \subset \Pi$ to be

$$\langle [\Pi(\boldsymbol{m}'), \Pi(\boldsymbol{m}'')] \mid \boldsymbol{m}' + \boldsymbol{m}'' = \boldsymbol{m} \text{ where } \boldsymbol{m}', \boldsymbol{m}'' \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\} \rangle_{\mathrm{normal}}.$$

Note that the definition does depend on the choice of the basis $\{x, y\}$ of Π. More precisely, the definition depends on the choice of the basis $\{\bar{x}, \bar{y}\}$ of Π^{ab} where $\bar{x}$ and $\bar{y}$ are the images of x and y in Π^{ab}, respectively.

Example 3.1. $\Pi(\mathbf{1}) = \Pi(2)$ holds since both are the normal closure of z.

We have the following inclusions and equalities:

Lemma 3.1. *Let* $\boldsymbol{m} = (m_1, m_2), \boldsymbol{n} = (n_1, n_2) \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$ *and* $m \geq 2$.
(1) $\Pi(\boldsymbol{m}) \subset \Pi(|\boldsymbol{m}|)$ *holds.*
(2) $\Pi(m, 0) = \Pi(m, 1)$ *holds. Similarly,* $\Pi(0, m) = \Pi(1, m)$ *holds.*
(3) If $\boldsymbol{m} \geq \boldsymbol{n}$*, then* $\Pi(\boldsymbol{m}) \subset \Pi(\boldsymbol{n})$ *holds.*

Proof. (1) The assertion immediately follows by induction on $|\boldsymbol{m}|$.

(2) The inclusion $\Pi(m,1) \subset \Pi(m,0)$ immediately follows by induction on m. To prove the opposite inclusion, by induction on m, it suffices to prove the assertion for $m=2$. Note that $\Pi(2,0)/\Pi(2,1)$ is normally generated by the image of the commutator map

$$\Pi(1,0)/\Pi(\mathbf{1}) \times \Pi(1,0)/\Pi(\mathbf{1}) \to \Pi(2,0)/\Pi(2,1).$$

However, since $\Pi(1,0)/\Pi(\mathbf{1})$ is generated by the image of x, the image is trivial. Hence $\Pi(2,0)=\Pi(2,1)$, as desired.

(3) We prove the assertion by induction on $|\boldsymbol{m}|+|\boldsymbol{n}|$. If $|\boldsymbol{m}|+|\boldsymbol{n}|=2$, the assertion holds. Let us assume $|\boldsymbol{m}|+|\boldsymbol{n}|>2$. Since $\Pi(\boldsymbol{m})$ is normally generated by $[\Pi(\boldsymbol{m}'),\Pi(\boldsymbol{m}'')]$ with $\boldsymbol{m}'+\boldsymbol{m}''=\boldsymbol{m}$, the assertion follows if there exist $\boldsymbol{n}'$ and $\boldsymbol{n}''$ such that $\boldsymbol{m}' \geq \boldsymbol{n}'$, $\boldsymbol{m}'' \geq \boldsymbol{n}''$ and $\boldsymbol{n}'+\boldsymbol{n}''=\boldsymbol{n}$. Such a pair $(\boldsymbol{n}',\boldsymbol{n}'')$ clearly exists unless (m_1,n_1) or (m_2,n_2) is equal to $(1,0)$. However, the assertion in this exceptional case also follows by using (2). □

Definition 3.2. For $\mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$, we define graded quotients $\mathrm{gr}_1^{\boldsymbol{m}}\Pi$ and $\mathrm{gr}_2^{\boldsymbol{m}}\Pi$ of Π as

$$\mathrm{gr}_1^{\boldsymbol{m}}\Pi \coloneqq \Pi(\boldsymbol{m})/\Pi(\boldsymbol{m}+(1,0)) \quad \text{and} \quad \mathrm{gr}_2^{\boldsymbol{m}}\Pi \coloneqq \Pi(\boldsymbol{m})/\Pi(\boldsymbol{m}+(0,1)).$$

Note that $\mathrm{gr}_1^{\boldsymbol{m}}\Pi$ (resp. $\mathrm{gr}_2^{\boldsymbol{m}}\Pi$) is a $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$ (resp. $\mathbb{Z}_p[[\Pi/\Pi(0,1)]]$)-module where the group $\Pi/\Pi(1,0)$ (resp. $\Pi/\Pi(0,1)$) acts by conjugation.

Example 3.2. (1) $\mathrm{gr}_1^{(1,0)}\Pi = \Pi(1,0)/\Pi(2,0)$ is a free $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-module of rank one generated by x, cf. [Iha86a, Theorem 2.2]. Similarly, $\mathrm{gr}_2^{(0,1)}\Pi$ is a free $\mathbb{Z}_p[[\Pi/\Pi(0,1)]]$-module of rank one generated by y.

(2) $\mathrm{gr}_2^{(1,0)}\Pi = \Pi(1,0)/\Pi(\mathbf{1})$ generated by the image of x on which $\Pi/\Pi(1,0)$ acts trivially. Similarly, $\mathrm{gr}_1^{(0,1)}\Pi$ is generated by y on which $\Pi/\Pi(0,1)$ acts trivially. Moreover, by Lemma 3.1(2), $\mathrm{gr}_2^{(m,0)}\Pi = \mathrm{gr}_1^{(0,m)}\Pi = 0$ for every $m \geq 2$.

3.2 Two-variable filtration on pro-p mapping class group

We define a subgroup $\tilde{\Gamma}$ and $\Gamma^\dagger$ of $\mathrm{Aut}(\Pi)$ as

$$\tilde{\Gamma} \coloneqq \left\{ f \in \mathrm{Aut}(\Pi) \;\middle|\; \begin{array}{l} \bar{f} \text{ preserves } \langle \bar{x} \rangle \text{ and } \langle \bar{y} \rangle \text{ respectively, and} \\ f \text{ preserves the conjugacy class of } \langle z \rangle \end{array} \right\},$$

$\Gamma \coloneqq \tilde{\Gamma}/\mathrm{Inn}(\Pi)$ and

$$\Gamma^\dagger \coloneqq \{ f \in \tilde{\Gamma} \mid f \text{ preserves } \langle z \rangle \},$$

where $\bar{f}$ is the image of f in $\mathrm{Aut}(\Pi^{\mathrm{ab}})$. One can easily observe that the subgroup $\Pi(\boldsymbol{m})$ introduced in Section 3.1 is preserved under the action of $\tilde{\Gamma}$.

By definition, there are two natural homomorphisms[2]

$$\chi_1\colon \tilde{\Gamma} \to \mathrm{Aut}(\langle \bar{x} \rangle) = \mathbb{Z}_p^\times \quad \text{and} \quad \chi_2\colon \tilde{\Gamma} \to \mathrm{Aut}(\langle \bar{y} \rangle) = \mathbb{Z}_p^\times.$$

There is a similar homomorphism $\Gamma^\dagger \to \mathrm{Aut}(\langle z \rangle) = \mathbb{Z}_p^\times$, by the definition of $\Gamma^\dagger$. This character coincides with $\chi_1\chi_2$ since the commutator map $\Pi/\Pi(2) \times \Pi/\Pi(2) \to \Pi(2)/\Pi(3)$ is bilinear.

The usual weight filtration $\{F^m\tilde{\Gamma}(m)\}_{m\geq 1}$ on $\tilde{\Gamma}$ is defined as

$$F^m\tilde{\Gamma} \coloneqq \ker\left(\tilde{\Gamma} \to \mathrm{Aut}(\Pi/\Pi(m+1))\right)$$

for $m \geq 1$. By using the two-variable filtration $\{\Pi(\boldsymbol{m})\}_{\boldsymbol{m}}$, we define a two-variable filtration on $\tilde{\Gamma}$ as follows.

Definition 3.3. For every $\boldsymbol{m} \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$, we define a subgroup $F^{\boldsymbol{m}}\tilde{\Gamma}$ to be

$$F^{\boldsymbol{m}}\tilde{\Gamma} \coloneqq \ker\left(\tilde{\Gamma} \to \prod_{\boldsymbol{k}\in\{(0,1),(1,0)\}} \mathrm{Aut}(\Pi(\boldsymbol{k})/\Pi(\boldsymbol{m}+\boldsymbol{k}))\right).$$

Note that the filtration $\{F^{\boldsymbol{m}}\tilde{\Gamma}\}_{\boldsymbol{m}}$ induces a two-variable filtration $\{F^{\boldsymbol{m}}\Gamma^\dagger\}_{\boldsymbol{m}}$ on $\Gamma^\dagger$ by taking the intersection. By Lemma 3.1 (1), it follows that $F^{\boldsymbol{m}}\tilde{\Gamma} \subset F^{|\boldsymbol{m}|}\tilde{\Gamma}$ for every $\boldsymbol{m} \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$.

Moreover, since $[\Pi(\boldsymbol{m}), \Pi(\boldsymbol{k})] \subset \Pi(\boldsymbol{m}+\boldsymbol{k})$ for $\boldsymbol{k} \in \{(1,0),(0,1)\}$, the inner automorphism group $\mathrm{Inn}_{\Pi(\boldsymbol{m})}(\Pi)$ of Π induced by elements of $\Pi(\boldsymbol{m})$ is contained in $F^{\boldsymbol{m}}\tilde{\Gamma}$.

The following lemma characterizes elements of $F^{\boldsymbol{m}}\tilde{\Gamma}$.

Lemma 3.2. *Let $\boldsymbol{m} \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$. Then, for every $f \in \tilde{\Gamma}$, f is contained in $F^{\boldsymbol{m}}\tilde{\Gamma}$ if and only if $f(x)x^{-1} \in \Pi(\boldsymbol{m}+(1,0))$ and $f(y)y^{-1} \in \Pi(\boldsymbol{m}+(0,1))$.*

Proof. We only have to prove the "if" part of the assertion. Note that $\Pi(1,0)$ is generated by y^nxy^{-n} for all $n \geq 0$. Hence, to prove the assertion, it suffices to prove that $f(y^nxy^{-n})y^nx^{-1}y^{-n} \in \Pi(\boldsymbol{m}+(1,0))$ for every $n \geq 0$. We compute this term as follows.

$$\begin{aligned} f(y^nxy^{-n})y^nx^{-1}y^{-n} &= f(y)^nf(x)f(y)^{-n}y^nx^{-1}y^{-n} \\ &\equiv f(y)^nf(y)^{-n}y^nf(x)x^{-1}y^{-n} \bmod \Pi(\boldsymbol{m}+(1,0)) \\ &= y^nf(x)x^{-1}y^{-n} \equiv 1. \end{aligned}$$

Here, we use $[f(y)^{-n}y^n, f(x)] \in [\Pi(\boldsymbol{m}+(0,1)), \Pi(1,0)] \subset \Pi(\boldsymbol{m}+\boldsymbol{1}) \subset \Pi(\boldsymbol{m}+(1,0))$ to establish the first congruence. A similar computation shows that f also acts trivially on $\Pi(0,1)/\Pi(\boldsymbol{m}+(0,1))$. ☐

[2] This notation is ambiguous since we already use the characters χ_1 and χ_2 to indicate the Galois characters $G_K \to \mathbb{Z}_p^\times$. However, if we take $x \coloneqq x_1$ and $y \coloneqq x_2$, then the image of $\rho_{X,p}$ is contained in Γ and this notation becomes compatible.

Moreover, we have the following lemma:

Lemma 3.3. *Let $\boldsymbol{m} \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$. Then, the group $F^{\boldsymbol{m}}\tilde{\Gamma}$ acts trivially on $\Pi(\boldsymbol{n})/\Pi(\boldsymbol{n}+\boldsymbol{m})$ for every $\boldsymbol{n} \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$.*

Proof. The assertion follows by induction on $|\boldsymbol{n}|$ $\square$

Let us consider the two natural homomorphisms:

$$i_{\boldsymbol{m},1}\colon \mathrm{gr}_1^{\boldsymbol{m}}\tilde{\Gamma} \to \mathrm{gr}_1^{\boldsymbol{m}+(1,0)}\Pi \oplus \mathrm{gr}_1^{\boldsymbol{m}+(0,1)}\Pi\colon f \mapsto (f(x)x^{-1}, f(y)y^{-1})$$

and

$$i_{\boldsymbol{m},2}\colon \mathrm{gr}_2^{\boldsymbol{m}}\tilde{\Gamma} \to \mathrm{gr}_2^{\boldsymbol{m}+(1,0)}\Pi \oplus \mathrm{gr}_2^{\boldsymbol{m}+(0,1)}\Pi\colon f \mapsto (f(x)x^{-1}, f(y)y^{-1})$$

where $\mathrm{gr}_1^{\boldsymbol{m}}\tilde{\Gamma} := F^{\boldsymbol{m}}\tilde{\Gamma}/F^{\boldsymbol{m}+(1,0)}\tilde{\Gamma}$ and $\mathrm{gr}_2^{\boldsymbol{m}}\tilde{\Gamma} := F^{\boldsymbol{m}}\tilde{\Gamma}/F^{\boldsymbol{m}+(0,1)}\tilde{\Gamma}$. Then the above lemma implies that $i_{\boldsymbol{m},1}$ and $i_{\boldsymbol{m},2}$ are injective for every $\boldsymbol{m} \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$.

Write

$$\tilde{\Gamma}_1 := \{\gamma \in \tilde{\Gamma} \mid \gamma(y)y^{-1} \in \Pi(2)\} \quad \text{and} \quad \tilde{\Gamma}_2 := \{\gamma \in \tilde{\Gamma} \mid \gamma(x)x^{-1} \in \Pi(2)\}$$

and set $\Gamma_1^\dagger := \tilde{\Gamma}_1 \cap \Gamma^\dagger$ and $\Gamma_2^\dagger := \tilde{\Gamma}_2 \cap \Gamma^\dagger$. Then, the action of $\tilde{\Gamma}_1/\tilde{\Gamma}(1,0)$ (resp. $\tilde{\Gamma}_2/\tilde{\Gamma}(0,1)$) on $\mathrm{gr}_1^{\boldsymbol{m}}\Pi$ (resp. $\mathrm{gr}_2^{\boldsymbol{m}}\Pi$) commutes with the action of $\Pi/\Pi(1,0)$ (resp. $\Pi/\Pi(0,1)$).

In the following, we study the action of $\Gamma_1^\dagger/\Gamma^\dagger(1,0)$ (resp. $\Gamma_2^\dagger/\Gamma^\dagger(0,1)$) on $\mathrm{gr}_1^{\boldsymbol{m}}$ (resp. $\mathrm{gr}_2^{\boldsymbol{m}}$) of Π and $\tilde{\Gamma}$.

Lemma 3.4. *$\gamma(x)x^{-\chi_1(\gamma)} \in \Pi(2,0)$ for every $\gamma \in \Gamma_1^\dagger$. Similarly, $\gamma(y)y^{-\chi_2(\gamma)} \in \Pi(0,2)$ for every $\gamma \in \Gamma_2^\dagger$.*

Proof. We prove the first assertion since the proof of the second one is similar. Since $\gamma \in \Gamma_1^\dagger$ acts $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-linearly on $\Pi(1,0)/\Pi(2,0)$, which is a free $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-module generated by x, this action is a scalar multiplication by an element of $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]^\times$. However, since $z = [y,x] = (y-1)x \neq 0$ in $\Pi(1,0)/\Pi(2,0)$ and $\gamma(z) = z^{\chi_1(\gamma)}$, such a scalar is necessary to be equal to $\chi_1(\gamma)$. In particular, $\gamma(x) = x^{\chi_1(\gamma)} \bmod \Pi(2,0)$ holds. $\square$

Lemma 3.5. *Let $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$. Then, $\Gamma_1^\dagger/\Gamma^\dagger(1,0)$ acts on $\mathrm{gr}_1^{\boldsymbol{m}}\Pi$ as multiplication by $\chi_1^{m_1}$. Similarly, $\Gamma_2^\dagger/\Gamma^\dagger(0,1)$ acts on $\mathrm{gr}_2^{\boldsymbol{m}}\Pi$ as multiplication by $\chi_2^{m_2}$.*

Proof. Let $\gamma \in \Gamma_1^\dagger$. We prove the former assertion by induction on $|\boldsymbol{m}|$. If $|\boldsymbol{m}| = 1$, the assertion follows from (the proof of) Lemma 3.4. In general, we know that $\mathrm{gr}_1^{\boldsymbol{m}}\Pi$ is generated (as a $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-module) by the image of commutator maps

$$[\,\cdot\,,\,\cdot\,]\colon \mathrm{gr}_1^{\boldsymbol{m}'}\Pi \times \mathrm{gr}_1^{\boldsymbol{m}''}\Pi \to \mathrm{gr}_1^{\boldsymbol{m}}\Pi$$

with $\boldsymbol{m}' + \boldsymbol{m}'' = \boldsymbol{m}$. Since this pairing is bilinear, for every $(\tau', \tau'') \in \mathrm{gr}_1^{\boldsymbol{m}'}\Pi \times \mathrm{gr}_1^{\boldsymbol{m}''}\Pi$,

$$\gamma([\tau', \tau'']) = [\gamma(\tau'), \gamma(\tau'')] = [\chi_1^{m_1'}(f)\tau', \chi_1^{m_1''}(\gamma)\tau''] = \chi_1^{m_1}(\gamma)[\tau', \tau'']$$

holds by induction hypothesis. This concludes the proof. □

Lemma 3.6. *Let* $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$. *Then,*

$$i_{\boldsymbol{m},1} \colon \mathrm{gr}_1^{\boldsymbol{m}}\tilde{\Gamma} \to (\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}\Pi)(-1,0) \oplus \mathrm{gr}_1^{\boldsymbol{m}+(0,1)}\Pi$$

is compatible with the action of $\Gamma_1^\dagger/\Gamma^\dagger(1,0)$ *on both sides. Here,* $(\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}\Pi)(-1,0)$ *is the* χ_1^{-1}*-twist of* $\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}\Pi$. *Similarly,*

$$i_{\boldsymbol{m},2} \colon \mathrm{gr}_2^{\boldsymbol{m}}\tilde{\Gamma} \to \mathrm{gr}_2^{\boldsymbol{m}+(1,0)}\Pi \oplus (\mathrm{gr}_2^{\boldsymbol{m}+(0,1)}\Pi)(0,-1)$$

is compatible with the action of $\Gamma_2^\dagger/\Gamma^\dagger(0,1)$ *on both sides.*

Proof. We prove the former assertion by computing the action of $\gamma \in \Gamma_1^\dagger$ on $f(x)x^{-1} \in \mathrm{gr}_1^{\boldsymbol{m}+(1,0)}\Pi$ and $f(y)y^{-1} \in \mathrm{gr}_1^{\boldsymbol{m}+(0,1)}\Pi$ for an arbitrary $f \in F^{\boldsymbol{m}}\tilde{\Gamma}$.

First,

$$\begin{aligned}(\gamma \cdot f)(y)y^{-1} &= (\gamma f \gamma^{-1})(y)y^{-1} \\ &= \gamma(f(\gamma^{-1}(y))\gamma^{-1}(y^{-1})).\end{aligned}$$

Writing $\gamma^{-1}(y) = y\alpha$ with some $\alpha \in \Pi(2) = \Pi(\mathbf{1})$ yields

$$\gamma(f(\gamma^{-1}(y))\gamma^{-1}(y^{-1})) = \gamma(f(y\alpha)\alpha^{-1}y^{-1}) \equiv \gamma(f(y)y^{-1}) \bmod \Pi(\boldsymbol{m}+\mathbf{1}).$$

Here, we use the fact $f(\alpha)\alpha^{-1} \in \Pi(\boldsymbol{m}+\mathbf{1})$ to deduce the last congruence. By Lemma 3.5, we see that the last term is equal to $\chi_1^{m_1}(\gamma)(f(y)y^{-1})$.

Secondly,

$$\begin{aligned}(\gamma \cdot f)(x)x^{-1} &= (\gamma f \gamma^{-1})(x)x^{-1} \\ &= \gamma(f(\gamma^{-1}(x))\gamma^{-1}(x^{-1})).\end{aligned}$$

By Lemma 3.4, we can set $\gamma^{-1}(x) = x^{\chi_1(\gamma^{-1})}\beta$ with some $\beta \in \Pi(2,0)$. Since $f(\beta)\beta^{-1} \in \Pi(\boldsymbol{m}+(2,0))$,

$$\begin{aligned}\gamma(f(\gamma^{-1}(x))\gamma^{-1}(x^{-1})) &= \gamma(f(x^{\chi_1(\gamma^{-1})}\beta)\beta^{-1}x^{-\chi_1(\gamma^{-1})}) \\ &\equiv \gamma(f(x^{\chi_1(\gamma^{-1})})x^{-\chi_1(\gamma^{-1})}) \bmod \Pi(\boldsymbol{m}+(2,0)) \\ &= \chi_1^{m_1+1}(\gamma)(f(x^{\chi_1(\gamma^{-1})})x^{-\chi_1(\gamma^{-1})})\end{aligned}$$

So the only thing we have to prove is that $f(x^n)x^{-n} \equiv (f(x)x^{-1})^n \bmod \Pi(\boldsymbol{m}+(2,0))$ for every $n \in \mathbb{Z}_p$. By continuity, it suffices to prove the assertion for every

$n \in \mathbb{Z}_{\geq 1}$. By induction on n,

$$\begin{aligned} f(x^n)x^{-n} &= f(x)f(x^{n-1})x^{-(n-1)}x^{-1} \\ &\equiv f(x)(f(x)x^{-1})^{n-1}x^{-1} \bmod \Pi(\boldsymbol{m}+(2,0)) \\ &= f(x)(f(x)x^{-1})^{n-1}f(x)^{-1}(f(x)x^{-1}) = [f(x),(f(x)x^{-1})^{n-1}](f(x)x^{-1})^n \\ &\equiv (f(x)x^{-1})^n \bmod \Pi(\boldsymbol{m}+(2,0)) \end{aligned}$$

holds. Here, the induction hypothesis is used to deduce the second congruence and we used $[f(x),(f(x)x^{-1})^{n-1}] \in \Pi(\boldsymbol{m}+(2,0))$ to establish the last congruence. $\square$

Finally, we define $F^{\boldsymbol{m}}\Gamma \subset \Gamma$ (resp. Γ_1 and Γ_2) to be the image of $F^{\boldsymbol{m}}\tilde{\Gamma}$ (resp. $\tilde{\Gamma}_1$ and $\tilde{\Gamma}_2$) under the natural projection. By definition, there is a natural surjection $\mathrm{gr}_1^{\boldsymbol{m}}\tilde{\Gamma} \to \mathrm{gr}_1^{\boldsymbol{m}}\Gamma := F^{\boldsymbol{m}}\Gamma/F^{\boldsymbol{m}+(1,0)}\Gamma$ for every $\mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$. The action of $\Gamma_1^\dagger/\Gamma^\dagger(1,0)$ on the right hand side and $\Gamma_1/\Gamma(1,0)$ on the left hand side is compatible. The similar statement holds for $\mathrm{gr}_2^{\boldsymbol{m}}$.

The following two lemmas are used in the next section:

Lemma 3.7. *The kernel of* $\Gamma_1^\dagger \xrightarrow{\chi_1} \mathbb{Z}_p^\times$ *is equal to* $\Gamma^\dagger(1,0)$. *Similarly, the kernel of* $\Gamma_2^\dagger \xrightarrow{\chi_2} \mathbb{Z}_p^\times$ *is equal to* $\Gamma^\dagger(0,1)$

Proof. We prove the former assertion. For $\gamma \in \ker(\Gamma_1^\dagger \xrightarrow{\chi_1} \mathbb{Z}_p^\times)$, we have $\gamma(z) = z$. Moreover, since $\Gamma_1^\dagger$ acts $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-linearly on $\Pi(1,0)/\Pi(2,0)$, which is a free $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-module generated by x and $z \in \Pi(1,0)/\Pi(2,0)$ is nonzero, $\gamma(x) = x \bmod \Pi(2,0)$. $\square$

Lemma 3.8. *The natural homomorphism*

$$\Gamma_1^\dagger/\Gamma^\dagger(1,0) \to \Gamma_1/\Gamma(1,0)$$

is an isomorphism. Similarly we have $\Gamma_2^\dagger/\Gamma^\dagger(0,1) \xrightarrow{\sim} \Gamma_2/\Gamma(0,1)$.

Proof. Since $\ker(\Gamma_1^\dagger \to \Gamma_1) = \ker(\Gamma^\dagger(1,0) \to \Gamma(1,0)) = \langle \mathrm{inn}(z) \rangle$, it suffices to prove that $\Gamma_1^\dagger \to \Gamma_1$ and $\Gamma^\dagger(1,0) \to \Gamma(1,0)$ are both surjective, by virtue of the snake lemma. For $\Gamma_1^\dagger \to \Gamma_1$, let $\bar{\gamma} \in \Gamma_1$ and $\gamma \in \tilde{\Gamma}_1$ an arbitrary lift of $\bar{\gamma}$. If we write $\gamma(z) = gz^\alpha g^{-1}$ for some $g \in \Pi$ and $\alpha \in \mathbb{Z}_p^\times$, $g^{-1}\gamma g = \mathrm{inn}(g^{-1}) \circ \gamma$ preserves $\langle z \rangle$. Moreover,

$$(g^{-1}\gamma g)(y)y^{-1} = g^{-1}\gamma(y)gy^{-1} = [g^{-1},\gamma(y)]\gamma(y)y^{-1} \in \Pi(2).$$

This shows $g^{-1}\gamma g \in \Gamma_1^\dagger$, hence the surjectivity of $\Gamma_1^\dagger \to \Gamma_1$.

For $\Gamma^\dagger(1,0) \to \Gamma(1,0)$, let $\bar{\gamma} \in \Gamma(1,0)$ and $\gamma \in \tilde{\Gamma}(1,0)$ an arbitrary lift of $\bar{\gamma}$. If we write $\gamma(z) = gz^\alpha g^{-1}$ for some $g \in \Pi$ and $\alpha \in \mathbb{Z}_p^\times$, then $g^{-1}\gamma g \in \Gamma_1^\dagger$ by the above argument. Observe that

$$\gamma(z)z^{-1} = [g, z^\alpha]z^{\alpha-1} \in \Pi(3) \Rightarrow z^{\alpha-1} \in \Pi(3) \Rightarrow \alpha = 1.$$

To prove $(g^{-1}\gamma g)(x)x^{-1} = [g^{-1}, \gamma(x)]\gamma(x)x^{-1} \in \Pi(2,0)$, it is enough to prove that $g \in \Pi(1,0)$.

Note that $\Pi(\mathbf{1})/\Pi(2,1) = \Pi(\mathbf{1})/\Pi(2,0) \subset \Pi(1,0)/\Pi(2,0)$ is a free $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$-submodule generated by $z = (y-1)x$. Hence $\gamma(z)z^{-1} = [g,z] = (g-1)z \in \Pi(2,0)$ implies $g = 1$ in $\mathbb{Z}_p[[\Pi/\Pi(1,0)]]$ i.e. $g \in \Pi(1,0)$. □

3.3 Two-variable filtration on Galois group

In the following, we apply results obtained in this section to $\Pi = \Pi_{1,1}$. We use our fixed basis $x = x_1$ and $y = x_2$ of $\Pi_{1,1}$. Recall that we have the pro-p outer Galois representation

$$\rho_{X,p} \colon G_K \to \mathrm{Out}(\Pi_{1,1}).$$

Note that the image of $\rho_{X,p}$ is naturally contained in Γ, which is a subgroup of $\Gamma_{1,1}$ introduced in 2.1. For $\boldsymbol{m} \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$, let $F^{\boldsymbol{m}}G_K \subset F^{|\boldsymbol{m}|}G_K$ denote the inverse image of $F^{\boldsymbol{m}}\Gamma$ under $\rho_{X,p}$. Moreover, let F_1G_K (resp. F_2G_K) denote the inverse image of Γ_1 (resp. Γ_2).

Lemma 3.9. *The following equality holds:*

1. $F_1G_K = G_{K(E[\bar{\mathfrak{p}}^\infty])}$ *and* $F_2G_K = G_{K(E[\mathfrak{p}^\infty])}$.
2. $F^{(1,0)}G_K = F^{(0,1)}G_K = F^{(1,1)}G_K = G_{K(E[p^\infty])}$.

Proof. (1) is clear, so we only prove (2). By Lemma 3.7 and Lemma 3.8, it follows that $F^{(1,0)}G_K$ is equal to the kernel of $F_1G_K \xrightarrow{\chi_1} \mathbb{Z}_p^\times$, hence equal to $G_{K(E[p^\infty])}$. The same argument proves that $F^{(0,1)}G_K$ coincides with $G_{K(E[p^\infty])}$. Since $F^{(1,0)}G_K \cap F^{(0,1)}G_K = F^{(1,1)}G_K$, the last assertion follows. □

Corollary 3.10. $\mathrm{Gal}(K(E[p^\infty])/K(E[\bar{\mathfrak{p}}^\infty]))$ *acts on* $\mathrm{gr}_1^{\boldsymbol{m}}G_K \coloneqq F^{\boldsymbol{m}}G_K/F^{\boldsymbol{m}+(1,0)}G_K$ *as multiplication by* $\chi_1^{m_1}$*. Similarly,* $\mathrm{Gal}(K(E[p^\infty])/K(E[\mathfrak{p}^\infty]))$ *acts on* $\mathrm{gr}_2^{\boldsymbol{m}}G_K \coloneqq F^{\boldsymbol{m}}G_K/F^{\boldsymbol{m}+(0,1)}G_K$ *as multiplication by* $\chi_2^{m_2}$*.*

Proof. Both assertions follow from Lemma 3.5, Lemma 3.6 and Lemma 3.9. □

4 Proof of main theorem

In this section, we assume that p satisfies the first two assumptions of Theorem 2.13, i.e. the class number of $K(p)$ is not divisible by p and there are exactly two primes of $K(p^\infty)$ above p.

In the following, We abbreviate the groups $\mathrm{Gal}(\Omega/K(p))$ and $\mathrm{Gal}(\Omega^*/K(p))$ as G and G^*, respectively. Let us recall the definition of the index set

$$I = \{\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{\mathbf{1}\} \mid m_1 \equiv m_2 \bmod |O_K^\times|\}.$$

In this section, we also use the following subset of I:

$$I_0 \coloneqq \{\boldsymbol{m} \in I \mid (p-1, p-1) \geq \boldsymbol{m}\} \cup \{(p,1), (1,p)\}.$$

First, we give two filtrations on G^* (and on G, by taking inverse images through the natural projection $G \to G^*$). Note that, by Lemma 2.12, it holds that

$$\rho_{X,p}(G_{K(p)}) = \mathrm{Gal}(\Omega^* K(E[p])/K(p)) = G^* \times \mathrm{Gal}(K(E[p])/K(p)) \subset \Gamma_{1,1}.$$

The group $\rho_{X,p}(G_{K(p)})$ has a descending central filtration and its two-variable variant which are induced from these on $\Gamma_{1,1}$. By taking the images under the natural projection $\rho_{X,p}(G_{K(p)}) \to G^*$, the group G^* also comes equipped with a descending central filtration $\{F^m G^*\}_{m \geq 1}$ and its two-variable variant $\{F^{\boldsymbol{m}} G^*\}_{\boldsymbol{m}}$.

Moreover, the natural surjection $G \to G^*$ induces filtrations $\{F^m G\}_{m \geq 1}$ and $\{F^{\boldsymbol{m}} G\}_{\boldsymbol{m}}$. By construction, the graded Lie algebras associated to $\{F^m G^*\}_{m \geq 1}$ and $\{F^m G\}_{m \geq 1}$ are both naturally isomorphic to $\mathfrak{g}$. A similar statement also holds for two-variable graded quotients.

In the following, we give a proof of Theorem 2.13. Roughly, the proof goes as follows. First, to prove the theorem, it suffices to prove that the intersection $\cap_{m \geq 1} F^m G = \mathrm{Gal}(\Omega/\Omega^*)$ is trivial.

1. In Section 4.1, we construct an element $\sigma_{\boldsymbol{m}} \in F^{\boldsymbol{m}} G$ whose image in $\mathfrak{g}_m$ satisfies the assumption of Conjecture 2.10. Moreover, from its construction, it is proved in Section 4.2 that $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$ strongly generates $F^1 G$. Here, results obtained in the previous section are essential.

2. Conjecture 2.10 implies that the filtration $\{F^m G\}_{m \geq 1}$ coincides with the "fastest" descending central filtration $\{\tilde{F}^m G\}_{m \geq 1}$ such that $\sigma_{\boldsymbol{m}} \in$ for every $\boldsymbol{m} \in I$. Since the intersection of the latter filtration is proved to be trivial by Lemma 4.10 (3), we obtain the desired result.

This strategy essentially follows Sharifi's approach [Sha02, Theorem 1.2].

4.1 Construction of elements

In this subsection, we construct elements $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$ of G in a certain way which can be regarded as a two-variable variant of Sharifi's construction in [Sha02, 2].

First, we lift generators of $\mathrm{Gal}(K(p^\infty)/K) \cong \Delta \times \mathbb{Z}_p^2$ as follows: Let us denote the maximal pro-p subextension of $K(p^\infty)/K$ by K_∞/K. The upper exact sequence in the following commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(\Omega/K(p^\infty)) & \longrightarrow & \mathrm{Gal}(\Omega/K_\infty) & \longrightarrow & \mathrm{Gal}(K(p^\infty)/K_\infty) & \longrightarrow & 1 \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow \wr & & \\
1 & \longrightarrow & G & \longrightarrow & \mathrm{Gal}(\Omega/K) & \longrightarrow & \Delta = \mathrm{Gal}(K(p)/K) & \longrightarrow & 1
\end{array}$$

splits since $\mathrm{Gal}(\Omega/K(p^\infty))$ is a pro-p group and Δ is a prime-to-p group. We choose a section $r\colon \mathrm{Gal}(K(p)/K) \to \mathrm{Gal}(\Omega/K_\infty)$ and identify $\mathrm{Gal}(\Omega/K)$ with the semi-direct product $G \rtimes \Delta$. Then Δ acts on $\mathrm{Gal}(\Omega/K(p^\infty))$ through this section. Hence

$$1 \to \mathrm{Gal}(\Omega/K(p^\infty)) \to G \to \mathrm{Gal}(K(p^\infty)/K(p)) \to 1$$

is an exact sequence of pro-p groups with Δ-action, noting that Δ acts trivially on $\mathrm{Gal}(K(p^\infty)/K(p))$. Taking the Δ-invariant of the above diagram yields an exact sequence

$$1 \to \mathrm{Gal}(\Omega/K(p^\infty))^\Delta \to G^\Delta \to \mathrm{Gal}(K(p^\infty)/K(p)) \to 1$$

since the orders of Δ and $\mathrm{Gal}(\Omega/K(p^\infty))$ are prime to each other.

Let γ_1 (resp. γ_2) be an element of G^Δ which restricts to a generator of $\mathrm{Gal}(K(p^\infty)/K(\mathfrak{p}^\infty\bar{\mathfrak{p}})) \cong \mathbb{Z}_p$ (resp. $\mathrm{Gal}(K(p^\infty)/K(\mathfrak{p}\bar{\mathfrak{p}}^\infty)) \cong \mathbb{Z}_p$). Moreover, fix a generator $\delta \in \mathbb{F}_p^\times$ and let δ_1 (resp. δ_2) be the image of $(\delta, 1) \in \mathrm{Gal}(K(p)/K) \cong (\mathbb{F}_p^\times)^2/\mathrm{im}(O_K^\times)$ (resp. $(1,\delta) \in \mathrm{Gal}(K(p)/K)$) under the section r.

By construction, the following relations hold:

$$[\delta_1,\delta_2]=1, \quad [\delta_1,\gamma_1]=1, \quad [\delta_1,\gamma_2]=1, \quad [\delta_2,\gamma_1]=1, \quad \text{and} \quad [\delta_2,\gamma_2]=1.$$

For $m \in \mathbb{Z}_{\geq 0}$ and $i = 1, 2$, we define $\epsilon_{i,m} \in \mathbb{Z}_p[\mathrm{Gal}(\Omega/K)]$ to be

$$\epsilon_{i,m} \coloneqq \frac{1}{p-1}\sum_{j=0}^{p-2} \chi_i^{-m}(\delta_i^j)\delta_i^j.$$

Moreover, for $g \in G$, we define

$$g^{\epsilon_{i,m}} \coloneqq (g \cdot \delta_i g^{\chi_i^{-m}(\delta_i)}\delta_i^{-1}\cdots \delta_i^{p-2} g^{\chi_i^{-m}(\delta_i^{p-2})}\delta_i^{-(p-2)})^{\frac{1}{p-1}}$$

and let $g^{\epsilon_{i,m}^j} = (\cdots(g^{\epsilon_{i,m}})\cdots)^{\epsilon_{1,m}}$ denote its j-th iterate for every $j \geq 1$. Since G is nonabelian, we do not necessarily have $g^{\epsilon_{i,m}^j} = g^{\epsilon_{i,m}}$. However, we have the following result, whose proof is the same as [Sha02, Lemma 2.1]:

Lemma 4.1. *For every $g \in G$, $m \in \mathbb{Z}_{\geq 0}$ and $i = 1, 2$, the limit*

$$g^{(i,m)} \coloneqq \lim_{j\to\infty} g^{\epsilon_{i,m}^j}$$

exists and satisfies $\delta_i g^{(i,m)}\delta_i^{-1} \coloneqq (g^{(i,m)})^{\chi_i^m(\delta)}$.

Before we construct elements $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$ of G, we need to study the structure of $A \coloneqq \mathrm{Gal}(\Omega/K(p^\infty))^{\mathrm{ab}}$ as a $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K)]]$-module:

Lemma 4.2. *Let $\boldsymbol{m} \in I_0$ and $A^{\boldsymbol{m}} \coloneqq \epsilon_{1,m_1}(\epsilon_{2,m_2}A)$.*

1. *If $\boldsymbol{m} \neq (1,p)$ or $(p,1)$, then $A^{\boldsymbol{m}}$ is a cyclic $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]$-module.*

2. $A^{(p,1)} = A^{(1,p)}$ *is isomorphic to a quotient of the annihilator of* $\mathbb{Z}_p(1)$ *i.e. a quotient of the* $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]$*-module* M *generated by two elements* v_1, v_2 *satisfying* $(\gamma_1 - \chi_1(\gamma_1))v_2 = (\gamma_2 - \chi_2(\gamma_2))v_1$.

Proof. There is the five-term exact sequence of $\mathbb{F}_p[\Delta]$-modules

$$0 \to H^1(\mathrm{Gal}(K(p^\infty)/K(p)), \mathbb{F}_p) \to H^1(G, \mathbb{F}_p) \to \mathrm{Hom}_{\mathrm{Gal}(K(p^\infty)/K(p))}(A, \mathbb{F}_p) \to H^2(\mathrm{Gal}(K(p^\infty)/K(p)), \mathbb{F}_p) \to H^2(G, \mathbb{F}_p).$$

Note that $H^1(\mathrm{Gal}(\Omega/K(p^\infty)), \mathbb{F}_p)^{\mathrm{Gal}(K(p^\infty)/K(p))} = \mathrm{Hom}_{\mathrm{Gal}(K(p^\infty)/K(p))}(A, \mathbb{F}_p) = \oplus_{\boldsymbol{m} \in I_0 \setminus \{(p,1)\}} \mathrm{Hom}_{\mathrm{Gal}(K(p^\infty)/K(p))}(A^{\boldsymbol{m}}, \mathbb{F}_p)$. Hence to prove (1), it suffices to compute the dimension of each eigenspace.

First, we compute the dimension of each eigenspace of $H^1(G, \mathbb{F}_p)$. By Kummer theory, there exists an isomorphism

$$O_{K(p)}[\frac{1}{p}]^\times / \left(O_{K(p)}[\frac{1}{p}]^\times\right)^p \cong H^1(G, \mu_p)$$

since the class number of $K(p)$ does not divide p. Hence the dimension of the right hand side is $r_2 + 2$ by Dirichlet's unit theorem. Moreover, [NSW08, (8.7.2) Proposition] shows that there is an isomorphism of $\mathbb{Q}[\Delta]$-modules

$$O_{K(p)}[\frac{1}{p}]^\times \otimes \mathbb{Q} \cong \mathbb{Q}[\Delta] \oplus \mathbb{Q}.$$

By decomposing the p-unit group $O_{K(p)}[\frac{1}{p}]^\times$ into the product of the torsion-part and the free-part, it follows that the dimension of $\chi^{\boldsymbol{m}}$-component of $H^1(G, \mathbb{F}_p)$ is at most 1 if $\boldsymbol{m} \in I_0 \setminus \{(1,p), (p,1), (p-1, p-1)\}$ and otherwise at most 2. By counting argument, all these inequalities are equalities. Since the action of Δ on $H^i(\mathrm{Gal}(K(p^\infty)/K(p)), \mathbb{F}_p)$ $(i = 1, 2)$ is trivial, the assertion of (1) follows from the above five-term exact sequence.

By our assumption, there exists a unique prime of $K(p^\infty)$ above $\mathfrak{p}$ which we also denote by the same letter $\mathfrak{p}$. By a theorem of Wintenberger [Win81, THÉORÈME], it holds that the decomposition group of $A^{(1,p)}$ at $\mathfrak{p}$ is a quotient of $\mathrm{ann}_{\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)_\mathfrak{p}/K(p)_\mathfrak{p})]]}(\mathbb{Z}_p(1)) = \mathrm{ann}_{\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]}(\mathbb{Z}_p(1))$. Hence to prove (2), it suffices to prove that the decomposition group of $A^{(1,p)}$ at $\mathfrak{p}$ is equal to the whole $A^{(1,p)}$.

Recall that $\mathrm{Hom}_\Delta(A^{(1,p)}, \mathbb{F}_p(1)) \cong \mathrm{Hom}_\Delta(\mathrm{Gal}(\Omega/K(p)), \mathbb{F}_p(1)) \cong O_K[\frac{1}{p}]^\times/(O_K[\frac{1}{p}]^\times)^p$ is generated by Kummer characters corresponding to π and $\bar{\pi}$. Hence the assertion is equivalent to the assertion that the images of π and $\bar{\pi}$ in $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p$ is still two-dimensional. To prove the latter assertion, it suffices to show that the projection of $\bar{\pi} \in O_{K_\mathfrak{p}}^\times$ to the principal group of units $1 + \pi O_{K_\mathfrak{p}} \cong \mathbb{Z}_p$ is a generator. This follows since $\mathrm{Frob}_{\bar{\mathfrak{p}}} \in \mathrm{Gal}(K(\mathfrak{p}^\infty)/K) \cong O_{K_\mathfrak{p}}^\times / O_K^\times$ is a generator, which is implied by our assumption that there exists a unique prime of $K(p^\infty)$ above $\bar{\mathfrak{p}}$. $\square$

Now we define elements $\sigma_{\boldsymbol{m}} \in F^{\boldsymbol{m}} G_K$ for $\boldsymbol{m} \in I_0$ as follows:

Construction.

For $\boldsymbol{m} \in I_0$, we choose an element $t_{\boldsymbol{m}} \in \mathrm{Gal}(\Omega/K(p^\infty))$, as follows:

- If $\boldsymbol{m} \in I_0 \backslash \{(p,1),(1,p),(p-1,p-1)\}$, we choose a lift $t_{\boldsymbol{m}} \in \mathrm{Gal}(\Omega/K(p^\infty))$ of a generator of $A^{\boldsymbol{m}}$ as $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]$-module.
- For $\boldsymbol{m} = (p,1)$ and $(1,p)$, fix a surjection from M given above to $A^{(p,1)}$ and let $t_{(p,1)}$ and $t_{(1,p)}$ be arbitrary lifts of the images of v_1 and v_2, respectively.
- For $\boldsymbol{m} = (p-1,p-1)$, set $t_{(p-1,p-1)} = [\gamma_1, \gamma_2]$.

For every $\boldsymbol{m} \in I_0$, let

$$\sigma_{\boldsymbol{m}} \coloneqq \left(t_{\boldsymbol{m}}^{(1,m_1)}\right)^{(2,m_2)} \quad \text{and} \quad g_{\boldsymbol{m}} \coloneqq \sigma_{\boldsymbol{m}}.$$

Note that $\sigma_{(p-1,p-1)} = g_{(p-1,p-1)} = [\gamma_1, \gamma_2]$ since γ_1 and γ_2 commute with δ_1 and δ_2. These elements $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0}$ satisfy the following properties:

Lemma 4.3. *For $\boldsymbol{m} \in I_0$, the following two assertions hold.*

1. *$\sigma_{\boldsymbol{m}} \in F^{\boldsymbol{m}} G$ and the image of $\sigma_{\boldsymbol{m}}$ in $\mathfrak{g}_{|\boldsymbol{m}|}$ is contained in the $\chi^{\boldsymbol{m}}$-isotypic component.*
2. *$\kappa_{\boldsymbol{m}}(\sigma_{\boldsymbol{m}})$ generates $\kappa_{\boldsymbol{m}}(F^1 G)$.*

Before proving the lemma, we firstly prove the following two lemmas concerning the case where $m_1 = 1$ or $m_2 = 1$.

Lemma 4.4. *We have $\kappa_{(1,p)}(\sigma_{(p,1)}) = 0$ and $\kappa_{(p,1)}(\sigma_{(1,p)}) = 0$.*

Proof. The following computation shows that $\kappa_{(p,1)}(\sigma_{(1,p)}) = 0$:

$$\begin{aligned} \kappa_{(p,1)}((\gamma_1 - \chi_1(\gamma_1))v_2) &= (\chi_1^p(\gamma_1) - \chi_1(\gamma_1))\kappa_{(p,1)}(v_2) \\ &= \kappa_{(p,1)}((\gamma_2 - \chi_2(\gamma_2))v_1) \\ &= (\chi_2(\gamma_2) - \chi_2(\gamma_2))\kappa_{p,1}(v_1) = 0. \end{aligned}$$

The same argument shows that $\kappa_{(1,p)}(\sigma_{(p,1)}) = 0$ as desired. ∎

Lemma 4.5. *We have $t_{(p,1)} \in F^{(2,1)} G$. Similarly, $t_{(1,p)} \in F^{(1,2)} G$.*

Proof. Let $s\colon F^1 G_K \to F^3 \Gamma^\dagger_{1,1}$ be the lift of $\rho_{X,p}$ constructed in 2.1. Then s factors through $F^1 G_K \to F^1 G$ and we denote the resulting homomorphism $F^1 G \to F^3 \Gamma^\dagger_{1,1}$ by the same letter.

The power series $\alpha_{1,1}(t_{(p,1)}) \in \mathbb{Z}_p[[T_1, T_2]]$ is contained in the ideal generated by T_1^{p-1} since $\kappa_{\boldsymbol{n}}(t_{(p,1)}) = 0$ unless $\boldsymbol{n} = (n_1, n_2) \in I$ satisfies $n_1 \equiv 1 \bmod p-1$ and $n_2 = 1$ (we used Lemma 4.4 here). This implies that

$$\begin{aligned} s(t_{(p,1)})(x_2)x_2^{-1} &= \alpha_{1,1}(t_{(p,1)})[x_2, z] \\ &= \frac{\alpha_{1,1}(t_{(p,1)})}{T_1}[x_1, [x_2, z]] \in \Pi(2)/[\Pi(2), \Pi(2)]. \end{aligned}$$

Since $[\Pi(2),\Pi(2)] = [\Pi(1,1),\Pi(1,1)] \subset \Pi(2,2)$ and $[x_1,[x_2,z]] \in \Pi(2,2)$, it follows that $s(t_{(p,1)})(x_2)x_2^{-1} \in \Pi(2,2)$. Moreover, from the equality $s(t_{(p,1)})(z) = z$, it follows that the element $[s(t_{(p,1)})(x_1)x_1^{-1}, x_2]$ is contained in $\Pi(3,2)$. Hence the assertion of the lemma is reduced to showing the following claim:

Claim. The identity is the only element of $\Pi(2,0)/\Pi(3,0)$ which is invariant under the conjugation of y.

In fact, this implies $s(t_{(p,1)})(x_1)x_1^{-1} \in \Pi(3,0) = \Pi(3,1)$, hence $t_{(p,1)} \in F^{(2,1)}G$ as desired. To prove the above claim, first note that, for every $m \geq 1$, the group $\Pi(m,0)$ is the m-th component of the descending central series of $\Pi(1,0)$, which is a free pro-p group on the set $\{w_n\}_{n\geq 1}$ where $w_0 \coloneqq x$ and $w_n \coloneqq [y, w_{n-1}]$ for every $n \geq 1$.

For $n \geq 1$, let F_n be the quotient of $\Pi(1,0)$ by the normal closure of $\{w_i\}_{i\geq n}$, which is a free pro-p group on the set $\{w_i\}_{0\leq i<n}$. Then $\Pi(1,0)$ is naturally isomorphic to the projective limit $\varprojlim_n F_n$. Then it holds that the commutator map gives a natural isomorphism

$$F_n/F_n(2) \wedge F_n/F_n(2) \xrightarrow{\sim} F_n(2)/F_n(3)$$

for every $n \geq 1$, since the Lie algebra associated to the descending central series of F_n is freely generated by the image of $\{w_i\}_{0\leq i<n}$ in $F_n/F_n(2)$. In other words, $F_n(2)/F_n(3)$ is a free $\mathbb{Z}_p$-module with basis $\{[w_i,w_j]\}_{0\leq i<j<n}$. Therefore, the group $\Pi(2,0)/\Pi(3,0) = \varprojlim_n F_n(2)/F_n(3)$ can be written as

$$\Pi(2,0)/\Pi(3,0) = \prod_{0\leq i<j} \mathbb{Z}_p[w_i,w_j].$$

Observe that the action of y sends $[w_i,w_j] \in \Pi(2,0)/\Pi(3,0)$ to $[w_{i+1}w_i, w_{j+1}w_j] = [w_{i+1},w_{j+1}] + [w_{i+1},w_j] + [w_i,w_{j+1}] + [w_i,w_j]$. If an element $v = (v_{i,j}) \in \prod_{0\leq i<j} \mathbb{Z}_p[w_i,w_j] = \Pi(2,0)/\Pi(3,0)$ is fixed by the conjugation of y, then one can show that $v_{0,j} = 0$ for every $j > 0$ by induction on j. By repeating induction for every $i > 0$, it follows that $v_{i,j} = 0$ for every $0 \leq i < j$, hence $v = 0$ as desired. □

Proof of Lemma 4.3. First, note that $\sigma_{\boldsymbol{m}} \in F^1G = F^{\mathbf{1}}G$ by Lemma 3.9. Hence (1) immediately follows from Corollary 3.10, except when $\boldsymbol{m} = (1,p)$ or $(p,1)$. If $\boldsymbol{m} = (p,1)$, we know $t_{(p,1)} \in F^{(2,1)}G$ by Lemma 4.5. Then the claim $\sigma_{(p,1)} \in F^{(p,1)}G$ follows from Corollary 3.10. The case $\boldsymbol{m} = (1,p)$ is similar. The second assertion of (1) also follows from Corollary 3.10.

Next we prove (2). For $\boldsymbol{m} \in I_0 \setminus \{(1,p),(p,1),(p-1,p-1)\}$, the assertion immediately follows since $\kappa_{\boldsymbol{m}}(t_{\boldsymbol{m}}) = \kappa_{\boldsymbol{m}}(\sigma_{\boldsymbol{m}})$ and $t_{\boldsymbol{m}}$ generates $A^{\boldsymbol{m}}$ as a $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]$-module.

Assume that $\boldsymbol{m} = (p-1,p-1)$. Since $A^{(p-1,p-1)} = A^{\Delta}$, it follows that $A^{(p-1,p-1)}$ is isomorphic to $\mathrm{Gal}(L/K_\infty)^{\mathrm{ab}}$, where L is the maximal pro-p extension of K unramified outside p. By [NSW08, (10.7.13) Theorem], $\mathrm{Gal}(L/K)$ is a free pro-p group of rank two on the set $\{\gamma_1, \gamma_2\}$.[3] In particular, $\mathrm{Gal}(L/K_\infty)^{\mathrm{ab}}$ is a free $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-module of rank one generated by $[\gamma_1, \gamma_2]$ by [Iha86b, Theorem 2]. Therefore, the image of $\kappa_{(p-1,p-1)}(\sigma_{(p-1,p-1)})$ generates the image of $\kappa_{(p-1,p-1)}(A)$. Finally, the case where $\boldsymbol{m} = (p,1)$ or $(1,p)$ follows from Lemma 4.4. $\square$

We inductively define $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ for general $\boldsymbol{m} \in I$ as follows:

Construction.

- For $\boldsymbol{m} = (m_1, m_2) \in I$ such that $\boldsymbol{m} \not\equiv \mathbf{1} \bmod p-1$, $p \leq m_1$ and $m_2 \leq p-1$, we define $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ as

$$\sigma_{\boldsymbol{m}} \coloneqq \left(\gamma_1 \sigma_{\boldsymbol{m}-(p-1,0)} \gamma_1^{-1} \sigma_{\boldsymbol{m}-(p-1,0)}^{-\chi_1^{m_1}(\gamma_1)}\right)^{(1,m_1)}$$

  and

$$g_{\boldsymbol{m}} \coloneqq \gamma_1 g_{\boldsymbol{m}-(p-1,0)} \gamma_1^{-1} g_{\boldsymbol{m}-(p-1,0)}^{-\chi_1^{m_1}(\gamma_1)}.$$

- For every $\boldsymbol{m} \in I$ such that $p \leq m_2$ and $\boldsymbol{m} \not\equiv \mathbf{1} \bmod p-1$, we define $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ as

$$\sigma_{\boldsymbol{m}} \coloneqq \left(\gamma_2 \sigma_{\boldsymbol{m}-(0,p-1)} \gamma_2^{-1} \sigma_{\boldsymbol{m}-(0,p-1)}^{-\chi_2^{m_2}(\gamma_2)}\right)^{(2,m_2)}$$

  and

$$g_{\boldsymbol{m}} \coloneqq \gamma_2 g_{\boldsymbol{m}-(0,p-1)} \gamma_2^{-1} g_{\boldsymbol{m}-(0,p-1)}^{-\chi_2^{m_2}(\gamma_2)}.$$

If we apply the above construction for $\boldsymbol{m} = (p,1)$ and $(1,p)$, then we obtain two candidates for $\sigma_{\boldsymbol{m}}$ for every $\boldsymbol{m}$ which satisfies $\boldsymbol{m} \equiv \mathbf{1} \bmod p-1$ and $\boldsymbol{m} \geq (2,2)$. However, we claim that these candidates define the same element on the level of the abelianization.

In fact, let $\boldsymbol{m} = (1 + n_1(p-1), 1 + n_2(p-1))$ for some $\boldsymbol{n} = (n_1, n_2) \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$. If we start from $\sigma_{(p,1)}$ to obtain $\sigma_{\boldsymbol{m}}$ through the above construction, we have

$$\sigma_{\boldsymbol{m}} = \prod_{i=1}^{n_1-1} (\gamma_1 - \chi_1(\gamma_1)^{1+i(p-1)}) \prod_{j=0}^{n_2-1} (\gamma_2 - \chi_2(\gamma_2)^{1+j(p-1)}) \sigma_{(p,1)}.$$

as an element of A. On the other hand, if we start from $\sigma_{(p,1)}$ we have

$$\sigma_{\boldsymbol{m}} = \prod_{i=0}^{n_1-1} (\gamma_1 - \chi_1(\gamma_1)^{1+i(p-1)}) \prod_{j=1}^{n_2-1} (\gamma_2 - \chi_2(\gamma_2)^{1+j(p-1)}) \sigma_{(1,p)}.$$

Hence two constructions yield the same element on A for every $\boldsymbol{n} \geq \mathbf{1}$ by Lemma 4.2(2) . Therefore, we construct elements as follows:

[3] The group $Б_{\{\mathfrak{p},\bar{\mathfrak{p}}\}}(K)$ appearing in the computation of [NSW08, (10.7.13) Theorem] is easily seen to be trivial.

- For $\boldsymbol{m} = (m, 1)$ such that $m \geq 2$ and $m \equiv 1 \bmod p-1$, we define $\sigma_{(m,1)}$ and $g_{(m,1)}$ by applying the above construction starting from $\sigma_{(p,1)}$. Similarly, for every $\boldsymbol{m} = (1, m)$ such that $m \geq 2$ and $m \equiv 1 \bmod p-1$, we define $\sigma_{(1,m)}$ and $g_{(1,m)}$ by applying the above construction starting from $\sigma_{(1,p)}$.
- For $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv \boldsymbol{1} \bmod p-1$, we define $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ by applying the above construction starting from $\sigma_{(p,1)}$.

We have the following lemma.

Lemma 4.6. *For every $\boldsymbol{m} \in I$, $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ define the same element of A.*

Proof. Since A is abelian, $\epsilon_{1,m}$ and $\epsilon_{2,m}$ acts on A as idempotents for every $m \geq 0$. Moreover, the action of $\epsilon_{i,m}$ commutes with the conjugation by γ_1 and γ_2. Hence the assertion follows from the construction of $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$. $\square$

The following proposition shows that our constructed $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$ satisfy the assumption of the Conjecture 2.10:

Proposition 4.7. *For $\boldsymbol{m} \in I$, the following two assertions hold.*

1. *$\sigma_{\boldsymbol{m}}$ is contained in $F^{\boldsymbol{m}}G$ and the image of $\sigma_{\boldsymbol{m}}$ in $\mathfrak{g}_{|\boldsymbol{m}|}$ is contained in the $\chi^{\boldsymbol{m}}$-isotypic component of $\mathfrak{g}_{|\boldsymbol{m}|}$.*
2. *$\kappa_{\boldsymbol{m}}(\sigma_{\boldsymbol{m}})$ generates $\kappa_{\boldsymbol{m}}(F^{|\boldsymbol{m}|}G)$.*

Proof. First, by Lemma 4.3, the assertion of (1) hold for every $\boldsymbol{m} \in I_0$. For every $\boldsymbol{m} \in I$ which satisfies the assertion of (1), note that $\gamma_1 \sigma_{\boldsymbol{m}} \gamma_1 \sigma_{\boldsymbol{m}}^{-\chi_1^{m_1}(\gamma_1)} \in F^{\boldsymbol{m}+(1,0)}G$ by Corollary 3.10. Now we claim that

$$\sigma_{\boldsymbol{m}+(p-1,0)} = \left(\gamma_1 \sigma_{\boldsymbol{m}} \gamma_1 \sigma_{\boldsymbol{m}}^{-\chi_1^{m_1}(\gamma_1)}\right)^{(1,m_1)} \in F^{\boldsymbol{m}+(p-1,0)}G.$$

In fact, $\sigma_{\boldsymbol{m}+(p-1,0)}$ is contained in $F^{\boldsymbol{m}+(1,0)}G$. By the construction of $\sigma_{\boldsymbol{m}+(p-1,0)}$ (cf. Lemma 4.1),

$$\delta_1 \sigma_{\boldsymbol{m}+(p-1,0)} \delta_1^{-1} = \chi_1^{m_1}(\delta_1) \sigma_{\boldsymbol{m}+(p-1,0)}$$

holds in $\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}G$. However, by Corollary 3.10, it also holds that

$$\delta_1 \sigma_{\boldsymbol{m}+(p-1,0)} \delta_1^{-1} = \chi_1^{m_1+1}(\delta_1) \sigma_{\boldsymbol{m}+(p-1,0)}$$

in $\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}G$. Since $\chi_1(\delta_1) \in \mathbb{Z}_p^\times$ is of order $p-1$, it holds that $\sigma_{\boldsymbol{m}+(p-1,0)} = 0$ in $\mathrm{gr}_1^{\boldsymbol{m}+(1,0)}G$. In other words, $\sigma_{\boldsymbol{m}+(p-1,0)} \in F^{\boldsymbol{m}+(2,0)}G$. By repeating this argument, we obtain that $\sigma_{\boldsymbol{m}+(p-1,0)} \in F^{\boldsymbol{m}+(p-1,0)}G$. Hence it follows that $\sigma_{\boldsymbol{m}} \in F^{\boldsymbol{m}}G$ for every $\boldsymbol{m} \in I$. This proves the former assertion of (1). The latter assertion follows from the former assertion and Corollary 3.10.

To prove (2), it suffices to prove that $\kappa_{\boldsymbol{m}}(g_{\boldsymbol{m}})$ generates $\kappa_{\boldsymbol{m}}(F^{|\boldsymbol{m}|}G)$ for every $\boldsymbol{m} \in I$, by virtue of Lemma 4.6.

First, let $\boldsymbol{m}_0 \in I_0 \setminus \{(1,p)\}$. We prove the assertion of (2) for every $\boldsymbol{m}$ such that $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$. Recall that $A^{\boldsymbol{m}_0}$ is generated by (the image of) $g_{\boldsymbol{m}_0}$ if $\boldsymbol{m}_0 \neq (p,1)$, and generated by $g_{(p,1)}$ and $g_{(1,p)}$ if $\boldsymbol{m}_0 = (p,1)$.

For every $m \geq |\boldsymbol{m}_0|$ such that $m \equiv |\boldsymbol{m}_0| \bmod p-1$, let $A^{\boldsymbol{m}_0,m}$ be the image of $F^m G$ in $A^{\boldsymbol{m}_0}$. Note that $\kappa_{\boldsymbol{m}} \mid_{F^{|\boldsymbol{m}|}G}$ factors through $A^{\boldsymbol{m}_0,|\boldsymbol{m}|}/A^{\boldsymbol{m}_0,|\boldsymbol{m}|+(p-1)}$ for every $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$. We prove the following claim:

Claim. $A^{\boldsymbol{m}_0,m}$ is generated by $\{g_{\boldsymbol{m}}\}_{\boldsymbol{m}}$ where $\boldsymbol{m}$ ranges over the indexes $\boldsymbol{m} \in I$ such that $|\boldsymbol{m}| = m$ and $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$. Moreover, $\kappa_{\boldsymbol{m}}(g_{\boldsymbol{m}})$ generates the image of $\kappa_{\boldsymbol{m}}(A^{\boldsymbol{m}_0,m})$.

Let us prove the claim by induction on m. First, we know that the claim holds for $m = |\boldsymbol{m}_0|$. We prove the claim for $m+(p-1)$, assuming it is true for m. Take an arbitrary element $x \in A^{\boldsymbol{m}_0,m+(p-1)}$. By induction hypothesis, the element x can be written as

$$x = \sum f_{\boldsymbol{m}}(T_1,T_2) g_{\boldsymbol{m}}$$

for some $f_{\boldsymbol{m}}(T_1,T_2) \in \mathbb{Z}_p[[T_1,T_2]]$ where $\boldsymbol{m}$ ranges over the indexes $\boldsymbol{m} \in I$ such that $|\boldsymbol{m}| = m$ and $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$.

Since $x \in A^{\boldsymbol{m}_0,m+(p-1)}$, Lemma 2.9 (2) implies that $\kappa_{\boldsymbol{n}}(x) = 0$ holds for every $\boldsymbol{n} = (n_1,n_2)$ such that $|\boldsymbol{n}| = m$ and $\boldsymbol{n} \equiv \boldsymbol{m}_0 \bmod p-1$. Hence

$$\begin{aligned}
\kappa_{\boldsymbol{n}}(x) &= \sum \kappa_{\boldsymbol{n}}(f_{\boldsymbol{m}}(T_1,T_2) g_{\boldsymbol{m}}) \\
&= \sum f_{\boldsymbol{m}}(\chi_1^{n_1}(\gamma_1)-1, \chi_2^{n_2}(\gamma_2)-1) \kappa_{\boldsymbol{n}}(g_{\boldsymbol{m}}) \\
&= f_{\boldsymbol{n}}(\chi_1^{n_1}(\gamma_1)-1, \chi_2^{n_2}(\gamma_2)-1) \kappa_{\boldsymbol{n}}(g_{\boldsymbol{n}}) = 0.
\end{aligned}$$

Note that $\kappa_{\boldsymbol{n}}(g_{\boldsymbol{n}})$ generates $\kappa_{\boldsymbol{n}}(F^{|\boldsymbol{n}|}G)$ by induction hypothesis. Moreover, the submodule $\kappa_{\boldsymbol{n}}(F^{|\boldsymbol{n}|}G) \subset \mathbb{Z}_p(\boldsymbol{n})$ is nonzero by Theorem 2.8 (2), its following remark and Lemma 2.9. Therefore, it follows that $\kappa_{\boldsymbol{n}}(g_{\boldsymbol{n}}) \neq 0$, hence $f_{\boldsymbol{n}}(\chi_1^{n_1}(\gamma_1)-1, \chi_2^{n_2}(\gamma_2)-1) = 0$. In other words, the power series $f_{\boldsymbol{n}}(T_1,T_2)$ is contained in the ideal $(T_1 - \chi_1^{n_1}(\gamma_1)+1, T_2 - \chi_2^{n_2}(\gamma_2)+1)$. Since

$$\begin{aligned}
(T_1 - \chi_1^{n_1}(\gamma_1)+1) g_{\boldsymbol{n}} &= (\gamma_1 - \chi_1^{n_1}(\gamma_1)) g_{\boldsymbol{n}} = g_{\boldsymbol{n}+(p-1,0)} \\
(T_2 - \chi_2^{n_2}(\gamma_2)+1) g_{\boldsymbol{n}} &= (\gamma_2 - \chi_2^{n_2}(\gamma_2)) g_{\boldsymbol{n}} = g_{\boldsymbol{n}+(0,p-1)},
\end{aligned}$$

it follows that $f_{\boldsymbol{n}}(T_1,T_2) g_{\boldsymbol{n}}$ can be written as a $\mathbb{Z}_p[[T_1,T_2]]$-linear combination of $g_{\boldsymbol{n}+(p-1,0)}$ and $g_{\boldsymbol{n}+(0,p-1)}$. By repeating this argument, it follows that every $x \in A^{\boldsymbol{m}_0,m+(p-1)}$ can be written as a $\mathbb{Z}_p[[T_1,T_2]]$-linear combination of $\{g_{\boldsymbol{m}}\}_{\boldsymbol{m}}$, where $\boldsymbol{m} \in I$ ranges over the indexes which satisfy $|\boldsymbol{m}| = m+(p-1)$ and $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$. This concludes the first half of the claim.

Finally, note that $\kappa_{\boldsymbol{m}}$ factors through $A^{\boldsymbol{m}_0,m}/A^{\boldsymbol{m}_0,m+(p-1)}$, which is proved to be generated by the image of $\{g_{\boldsymbol{m}}\}_{\boldsymbol{m}}$ where $\boldsymbol{m} \in I$ ranges over the indexes such that $|\boldsymbol{m}| = m$ and $\boldsymbol{m} \equiv \boldsymbol{m}_0 \bmod p-1$. Moreover, if $\boldsymbol{n} \neq \boldsymbol{m}$ is one of such an index, $\kappa_{\boldsymbol{m}}(g_{\boldsymbol{n}}) = 0$ since the image of $g_{\boldsymbol{n}}$ in $A^{\boldsymbol{m}_0,m}/A^{\boldsymbol{m}_0,m+(p-1)}$ is contained in the $\chi^{\boldsymbol{n}}$-isotypic component. This completes the proof of the claim, hence the proof of (2). $\square$

4.2 Group-theoretic lemmas

In this subsection, we complete a proof of Theorem 2.13. First, we prepare a series of lemmas which are required to prove the theorem. We note that the following lemma is a generalization of Lemma 3.1 in [Sha02] to the case of a free pro-p group of countably infinite rank.

Lemma 4.8. *Let $\mathcal{F}$ be a pro-p group strongly generated by y and $\{x_i\}_{i\geq 1}$. For each $i \geq 1$, let $x_{i,1} \coloneqq x_i$ and inductively define*

$$x_{i,j+1} \coloneqq [y, x_{i,j}]x_{i,j}^{pa_{i,j}}$$

for some $a_{i,j} \in \mathbb{Z}_p$ for every $j \geq 1$. Let H be the normal closure of $\{x_i\}_{i\geq 1}$ in $\mathcal{F}$. Then the following two assertions hold:

1. *H is strongly generated by $\{x_{i,j}\}_{i,j\geq 1}$.*
2. *If $\mathcal{F}$ is a free pro-p group on y and $\{x_i\}_{i\geq 1}$, then H is a free pro-p group on the set $\{x_{i,j}\}_{i,j\geq 1}$.*

Proof. First, let $\mathcal{K}$ be a free pro-p group on the set $\{\tilde{x}_{i,j}\}_{i,j\geq 1}$. We define a two-variable filtration on this group to be

$$\mathcal{K}_{i,j} \coloneqq \langle \tilde{x}_{i',j'} \mid i' \geq i \text{ or } j' \geq j\rangle_{\text{normal}}$$

for every $i, j \geq 1$. Note that $\mathcal{K}/\mathcal{K}_{i,j}$ is a free pro-p group of finite rank.

We define an automorphism $\phi\colon \mathcal{K} \xrightarrow{\sim} \mathcal{K}$ by $\phi(\tilde{x}_{i,j}) \coloneqq \tilde{x}_{i,j+1}\tilde{x}_{i,j}^{1-pa_{i,j}}$ for every $i, j \geq 1$. It is straightforward to see that ϕ preserves $\{\mathcal{K}_{i,j}\}_{i,j\geq 1}$. Hence it defines an element of $\mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$, which is defined to be the group of automorphisms of $\mathcal{K}$ preserving $\{\mathcal{K}_{i,j}\}_{i,j\geq 1}$.

First, note that $\mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$ is naturally isomorphic to the projective limit $\varprojlim_{(i,j)} \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K}/\mathcal{K}_{i,j})$ whose transition maps are obvious ones. The latter group has a natural structure of a profinite group since each $\mathrm{Aut}_{\mathrm{fil}}(\mathcal{K}/\mathcal{K}_{i,j})$ is a closed subgroup of $\mathrm{Aut}(\mathcal{K}/\mathcal{K}_{i,j})$ which is a profinite group by congruence topology and every projective limit of profinite groups is a profinite group. Hence a homomorphism $\mathbb{Z} \to \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$ corresponding to ϕ uniquely extends to a homomorphism $\hat{\mathbb{Z}} \to \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$. We claim that this homomorphism factors through the natural projection $\hat{\mathbb{Z}} \to \mathbb{Z}_p$.

Let us set $M \coloneqq \mathcal{K}^{\mathrm{ab}}/p$ and let $M_{i,j} \subset M$ be the image of $\mathcal{K}_{i,j}$ in M. Since taking the maximal abelian quotient and taking modulo p are both right exact, $M/M_{i,j}$ is naturally isomorphic to $(\mathcal{K}/\mathcal{K}_{i,j})^{\mathrm{ab}}/p$. Note that the kernel of

$$\mathrm{Aut}_{\mathrm{fil}}(\mathcal{K}) \xrightarrow{\sim} \varprojlim \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K}/\mathcal{K}_{i,j}) \to \mathrm{Aut}_{\mathrm{fil}}(M) \xrightarrow{\sim} \varprojlim \mathrm{Aut}_{\mathrm{fil}}(M/M_{i,j})$$

is a pro-p group since the kernel of $\mathrm{Aut}(\mathcal{K}/\mathcal{K}_{i,j}) \to \mathrm{Aut}(M/M_{i,j})$ is so. Therefore, it suffices to prove that the homomorphism $\hat{\mathbb{Z}} \to \mathrm{Aut}_{\mathrm{fil}}(M)$ corresponding to the image of ϕ factors through $\hat{\mathbb{Z}} \to \mathbb{Z}_p$.

By the construction of ϕ, it follows that $\phi^{p^n} \in \ker(\mathrm{Aut}_{\mathrm{fil}}(M) \to \mathrm{Aut}_{\mathrm{fil}}(M/M_{p^n,p^n}))$. In fact, a direct computation shows that $\phi^p(\tilde{x}_{i,j}) = \tilde{x}_{i,j+p} + \tilde{x}_{i,j}$ holds on M

for every (i,j) and iterating ϕ^p verifies the claim. Hence the image of ϕ in $\mathrm{Aut}_{\mathrm{fil}}(M) \cong \varprojlim \mathrm{Aut}_{\mathrm{fil}}(M/M_{p^n,p^n})$ is a pro-p group.

By the above argument, we proved that $\mathbb{Z} \to \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$ naturally extends to a homomorphism $\mathbb{Z}_p \to \mathrm{Aut}_{\mathrm{fil}}(\mathcal{K})$, so we can form a semi-direct product $K \rtimes \mathbb{Z}_p$.

There is a homomorphism $\mathcal{K} \to H$ sending $\tilde{x}_{i,j}$ to $x_{i,j}$ for every $i,j \geq 1$ because the set $\{x_{i,j}\}_{i,j\geq 1}$ converges to 1. Since the action of ϕ on K is the same as the conjugation by y on H, we can extend this homomorphism to $\mathcal{K} \rtimes \mathbb{Z}_p \to \mathcal{F}$ by sending ϕ to y, which is surjective by its construction. Hence $K \to H$ is also surjective by usual diagram chasing. This proves (1). Moreover, if $\mathcal{F}$ is a free pro-p group, the universal property of $\mathcal{F}$ assures the existence of the inverse of $\mathcal{K} \rtimes \mathbb{Z}_p \to \mathcal{F}$. Hence $\mathcal{K} \to H$ is injective. This proves (2). □

Corollary 4.9. *Let $r \geq 1$ and $\mathcal{F}$ be a pro-p group strongly generated by y_1, y_2 and $\{x_i\}_{1\leq i\leq r}$. For each $1 \leq i \leq r$, let $x_{i,(0,0)} := x_i$ and we inductively define*

$$x_{i,(j+1,0)} := [y_1, x_{i,(j,0)}]x_{i,(j,0)}^{pa_{i,j}}$$

for some $a_{i,j} \in \mathbb{Z}_p$ and $j \geq 0$. Similarly, for each $1 \leq i \leq r$ and each $j \geq 0$, define

$$x_{i,(j,k+1)} := [y_2, x_{i,(j,k)}]x_{i,(j,k)}^{pb_{i,j,k}}$$

for some $b_{i,j,k} \in \mathbb{Z}_p$ and $k \geq 0$.

Moreover, let $z_{(0,0)} := [y_1, y_2]$ and define

$$z_{(i+1,0)} := [y_1, z_{(i,0)}]z_{(i,0)}^{p\alpha_i}$$

for some $\alpha_i \in \mathbb{Z}_p$ and $i \geq 0$. Finally, for each $i \geq 0$, we define

$$z_{(i,j+1)} := [y_2, z_{(i,j)}]z_{(i,j)}^{p\beta_{i,j}}$$

for some $\beta_{i,j} \in \mathbb{Z}_p$ and each $j \geq 0$. Let H be the normal closure of $\{x_i\}_{1\leq i\leq r}$ and $z_{(0,0)} = [y_1, y_2]$ in $\mathcal{F}$. Then H is strongly generated by $\{x_{i,(j,k)}\}_{\substack{1\leq i\leq r\\ j,k\geq 0}}$ and $\{z_{i,j}\}_{i,j\geq 0}$.

Proof. We may assume that $\mathcal{F}$ is a free pro-p group on y_1, y_2 and $\{x_i\}_{1\leq i\leq r}$. First, let $\mathcal{F}_1$ be the kernel of $\mathcal{F} \to \mathbb{Z}_p$ defined by $y_1 \mapsto 1$, $y_2 \mapsto 0$ and $x_i \mapsto 0$ for all $1 \leq i \leq r$. Then Lemma 4.8 implies that $\mathcal{F}_1$ is a free pro-p group on y_2, $\{z_{(i,0)}\}_{i\geq 0}$ and $\{x_{i,(j,0)}\}_{1\leq i\leq r, j\geq 0}$.

Secondly, observe that H is the kernel of a homomorphism $\mathcal{F}_1 \to \mathbb{Z}_p$ defined by $y_2 \mapsto 1$, $z_{(i,0)} \mapsto 0$ for all $i \geq 0$ and $x_{i,(j,0)} \mapsto 0$ for all $1 \leq i \leq r, j \geq 0$. By applying Lemma 4.8 again, it follows that H is a free pro-p group on $\{z_{i,j}\}_{i\geq 0, j\geq 0}$ and $\{x_{i,(j,k)}\}_{\substack{1\leq i\leq r\\ j,k\geq 0}}$ as desired. □

The following lemma is used to compare the filtration $\{F^m G\}_{m\geq 1}$ on G with a certain canonical filtration on G associated to $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$.

Lemma 4.10. *Let $\mathcal{G}$ be a free pro-p group on the set $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$.*

1. *There exists a unique descending central filtration* $\{\tilde{F}^m\mathcal{G}\}_{m\geq 1}$ *which satisfies the following universal property:* (i) $\tilde{\sigma}_{\boldsymbol{m}} \in \tilde{F}^{|\boldsymbol{m}|}\mathcal{G}$ *for every* $\boldsymbol{m} \in I$. (ii) *If* $\{F^m\mathcal{G}\}_{m\geq 1}$ *is a descending central filtration satisfying* (i), *then* $\tilde{F}^m\mathcal{G} \subset F^m\mathcal{G}$ *holds for every* $m \geq 1$.

2. *The graded Lie algebra* $\bigoplus_{m\geq 1} \tilde{F}^m\mathcal{G}/\tilde{F}^{m+1}\mathcal{G}$ *is freely generated by the image of* $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$.

3. $\bigcap_{m\geq 1} \tilde{F}^m\mathcal{G} = \{1\}$.

Proof. We construct $\{\tilde{F}^m\mathcal{G}\}_{m\geq 1}$ as follows: First, let $\tilde{F}^1\mathcal{G} := \mathcal{G}$. For $m \geq 2$, we inductively define $\tilde{F}^m\mathcal{G}$ as

$$\tilde{F}^m\mathcal{G} := \langle \{\tilde{\sigma}_{\boldsymbol{m}}\}_{|\boldsymbol{m}|\geq m}, \{[\tilde{F}^{m'}\mathcal{G}, \tilde{F}^{m''}\mathcal{G}]\}_{\substack{m'<m, m''<m \\ m\leq m'+m''}} \rangle_{\text{normal}}.$$

Since $[\tilde{F}^m\mathcal{G}, \tilde{F}^1\mathcal{G}] \subset \tilde{F}^m\mathcal{G}$, it follows that $\tilde{F}^{m+1}\mathcal{G} \subset \tilde{F}^m\mathcal{G}$ for every $m \geq 1$. Apparently, $\{\tilde{F}^m\mathcal{G}\}_{m\geq 1}$ is a descending central filtration which satisfies (i) in the assertion of (1). Moreover, if $\{F^m\mathcal{G}\}_{m\geq 1}$ is a descending central filtration satisfying (i), then $F^1\mathcal{G} = \tilde{F}^1\mathcal{G} = \mathcal{G}$. By induction on m, one can easily show that $\tilde{F}^m\mathcal{G} \subset F^m\mathcal{G}$ holds for every $m \geq 1$. Hence $\{\tilde{F}^m\mathcal{G}\}_{m\geq 1}$ also satisfies (ii). The uniqueness is clear. The proof of (2) is similar to that of [Iha01, p.263, 5].

Finally, we prove (3). Let F_n be a free pro-p group on the set $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I, |\boldsymbol{m}|\leq n}$ for every $n \geq 2$. Since $\mathcal{G}$ is naturally isomorphic to the projective limit of $\varprojlim_n F_n$, it suffices to prove that the image of $\bigcap_{m\geq 1} \tilde{F}^m G$ in F_n is trivial for every $n \geq 2$.

For an integer $m \geq n$, we know that the image of $\tilde{F}^m\mathcal{G}$ in F_n is normally generated by the image of

$$\{[\tilde{F}^{m'}\mathcal{G}, \tilde{F}^{m''}\mathcal{G}]\}_{\substack{m'<m, m''<m \\ m\leq m'+m''}}.$$

We claim that the image of $\tilde{F}^m\mathcal{G}$ in F_n contained in the r_m-th component $F_n(r_m)$ of the descending central series of F_n, where

$$r_m := \left\lfloor \frac{m}{n} \right\rfloor + 1$$

for every $m \geq 1$. Once this claim is proved, then the image of $\bigcap_{m\geq 1} \tilde{F}^m\mathcal{G}$ in F_n is contained in $\bigcap_{m\geq n} F_n(r_m) = \{1\}$, hence (3) follows.

The claim holds for $m \leq 2n-1$. Assume that the claim also holds for every $m \leq kn-1$ for some $k \geq 2$ and we prove the claim for $m = kn, kn+1, \dots (k+1)n-1$ in order. Write $m = kn + r$ for some $0 \leq r \leq n-1$.

Let m', m'' are positive integers less than m which satisfy $m' + m'' \geq m$ and write $m' = k'n + r$, $m' = k''n + r'$ for some $0 \leq k', k'' \leq k$ and $0 \leq r', r'' \leq n-1$. Since

$$m' + m'' = (k' + k'')n + (r' + r'') \geq m = kn + r,$$

It holds that

$$r_{m'} + r_{m''} = (k' + k'') + 2 \geq (k+1) + \frac{n + r - (r' + r'')}{n}.$$

Since $\frac{n+r-(r'+r'')}{n} \geq \frac{2-n}{n} > -1$, it holds that

$$r_{m'} + r_{m''} \geq r_m.$$

Therefore, the image of $[\tilde{F}^{m'}\mathcal{G}, \tilde{F}^{m''}\mathcal{G}]$ is contained in $[F_n(r_{m'}), F_n(r_{m''})] \subset F_n(r_{m'} + r_{m''}) \subset F_n(r_m)$. Hence the image of $\tilde{F}^m\mathcal{G}$ is contained in $F_n(r_m)$, as desired. □

The next lemma gives an explicit set of generators of the group G:

Lemma 4.11. *The Galois group $G = \mathrm{Gal}(\Omega/K(p))$ is generated by γ_1, γ_2 and $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0 \setminus \{(p-1,p-1)\}}$.*

Proof. Recall that the image of $\sigma_{\boldsymbol{m}}$ in $A = \mathrm{Gal}(\Omega/K(p^\infty))^{\mathrm{ab}}$ is equal to $t_{\boldsymbol{m}}$ for every $\boldsymbol{m} \in I_0$ and $t_{(p-1,p-1)}$ is the commutator $[\gamma_1, \gamma_2]$ of γ_1 and γ_2. By Lemma 4.2 and definition of $\{t_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0}$, it follows that A is generated by the image of $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0}$ as a $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K(p))]]$-module, which is equivalent to saying that $\mathrm{Gal}(\Omega/K(p^\infty))$ is normally generated by $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0}$. Hence γ_1, γ_2 and $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0 \setminus \{(p-1,p-1)\}}$ generates G as desired. □

Proof of Theorem 2.13. By Lemma 4.11 above, the group G is generated by γ_1, γ_2 and $\{\sigma_{\boldsymbol{m}}(= g_{\boldsymbol{m}})\}_{\boldsymbol{m} \in I_0 \setminus \{(p-1,p-1)\}}$. We recall the discussion occurring at defining $\sigma_{\boldsymbol{m}}$ and $g_{\boldsymbol{m}}$ for $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \equiv \mathbf{1} \bmod p-1$: there were two ways to construct them starting from $\sigma_{(p,1)}$ and $\sigma_{(1,p)}$, but they yield the same elements on $A = \mathrm{Gal}(\Omega/K(p^\infty))^{\mathrm{ab}}$. Hence, by applying Corollary 4.9 to $\mathcal{F} = G$, $y_1 = \gamma_1$, $y_2 = \gamma_2$ and $\{x_i\}_{1 \leq i \leq r} = \{g_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I_0}$, it follows that $F^1G = \mathrm{Gal}(\Omega/K(p^\infty))$ is strongly generated by $\{g_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$. Moreover, by Lemma 4.6, it follows that $\{\sigma_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$ also strongly generates F^1G.

In the following, we prove that $F^1G \to F^1G^*$ is an isomorphism, which is equivalent to saying that $\Omega = \Omega^*$. Let $\mathcal{G}$ be a free pro-p group on the set $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m} \in I}$, $p \colon \mathcal{G} \to F^1G$ a surjective homomorphism sending $\tilde{\sigma}_{\boldsymbol{m}}$ to $\sigma_{\boldsymbol{m}}$ for every $\boldsymbol{m} \in I$ and $p^* \colon \mathcal{G} \to F^1G^*$ a compositum of p with a natural surjection $F^1G \to F^1G^*$. Through the surjection p^*, the group $\mathcal{G}$ comes equipped with a descending central filtration denoted by $\{F^m\mathcal{G}\}_{m \geq 1}$. Note that its associated graded Lie algebra is isomorphic to $\mathfrak{g}$ and that

$$\ker(p^*) = (p^*)^{-1}(\{1\}) = (p^*)^{-1}(\bigcap_{m \geq 1} F^m G^*) = \bigcap_{m \geq 1} F^m \mathcal{G}.$$

The injectivity of p^* is hence equivalent to $\bigcap_{m \geq 1} F^m\mathcal{G} = \{1\}$. By Lemma 4.10 (1), the group $F^m\mathcal{G}$ contains $\tilde{F}^m\mathcal{G}$ for every $m \geq 1$. Hence we have the following commutative diagram:

$$\begin{tikzcd}
\left(\bigoplus_{m\geq 1} \tilde{F}^m\mathcal{G}/\tilde{F}^{m+1}\mathcal{G}\right)\otimes\mathbb{Q}_p \arrow[r] & \left(\bigoplus_{m\geq 1} F^m\mathcal{G}/F^{m+1}\mathcal{G}\right)\otimes\mathbb{Q}_p \cong \mathfrak{g}\otimes\mathbb{Q}_p \\
\bigoplus_{m\geq 1} \tilde{F}^m\mathcal{G}/\tilde{F}^{m+1}\mathcal{G} \arrow[u, hook] \arrow[r] & \bigoplus_{m\geq 1} F^m\mathcal{G}/F^{m+1}\mathcal{G}. \arrow[u, hook]
\end{tikzcd}$$

Since we assume the analogue of the Deligne-Ihara conjecture (Conjecture 2.10), it holds that $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$ freely generates $\bigoplus_{m\geq 1}(F^m\mathcal{G}/F^{m+1}\mathcal{G})\otimes\mathbb{Q}_p$. However, by Lemma 4.10 (2), the Lie algebra $\bigoplus_{m\geq 1}(\tilde{F}^m\mathcal{G}/\tilde{F}^{m+1}\mathcal{G})\otimes\mathbb{Q}_p$ is also generated by $\{\tilde{\sigma}_{\boldsymbol{m}}\}_{\boldsymbol{m}\in I}$, which forces an upper horizontal homomorphism in the diagram to be an isomorphism. Therefore, a lower horizontal homomorphism in the diagram is injective. This is equivalent to saying that two filtrations $\{\tilde{F}^m\mathcal{G}\}_{m\geq 1}$ and $\{F^m\mathcal{G}\}_{m\geq 1}$ coincide with each other (as is observed by induction on m). Therefore, by Lemma 4.10 (3), it holds that

$$\bigcap_{m\geq 1} F^m\mathcal{G} = \bigcap_{m\geq 1} \tilde{F}^m\mathcal{G} = \{1\}$$

which shows the injectivity of $p^*\colon \mathcal{G}\to F^1G^*$. Hence it follows that $p\colon \mathcal{G}\to F^1G$. This concludes the proof. $\square$

A Appendix : pro-p outer Galois representation associated to the thrice-punctured projective line

The purpose of this appendix is simply to explain previous results on the pro-p outer Galois representation of the thrice-punctured projective line for comparison with the case of once-punctured CM elliptic curves. For more details on the pro-p outer Galois representation associated to the thrice-punctured projective line, please see the beautifully written lecture by Ihara [Iha02].

Let Π be the pro-p geometric fundamental group of the thrice-punctured projective line $T \coloneqq \mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}$[4] with respect to a fixed (possibly tangential) basepoint and

$$\rho_{T,p}\colon G_{\mathbb{Q}}\to \mathrm{Out}(\Pi)$$

be the pro-p outer representation associated to T. By using the $\mathbb{Q}$-rational tangential basepoint $\vec{01}$ (cf. Deligne [Del89] or Nakamura [Nak99]), we can lift this representation to

$$\rho_{T,\vec{01},p}\colon G_{\mathbb{Q}}\to \mathrm{Aut}(\Pi).$$

Note that, by using tangential basepoints ($\vec{01}$ and $\vec{10}$), we can identify Π with the pro-p completion of the free group of rank two in such a way that there

[4] T stands for “tripod”.

exists a free basis $\{x, y\}$ such that x and y generate inertia subgroups at 0 and 1 respectively and the Galois group $G_{\mathbb{Q}}$ acts on Π through $\rho_{T,\vec{01},p}$ by

$$\begin{aligned} \sigma(x) &= x^{\chi_{\mathrm{cyc}}(\sigma)} \\ \sigma(y) &= f_\sigma y^{\chi_{\mathrm{cyc}}(\sigma)} f_\sigma^{-1} \end{aligned}$$

with some $f_\sigma \in \Pi(2)$ which is uniquely determined by σ.

A.1 Ihara's power series and Soulé characters

We recall the construction of Ihara's power series. First, observe that the action of the Galois group $G_{\mathbb{Q}(\mu_{p^\infty})}$ on $\Pi(2)/[\Pi(2), \Pi(2)]$ through $\rho_{T,\vec{01},p}$ is $\mathbb{Z}_p[[\Pi^{\mathrm{ab}}]]$-linear.

Since $\Pi(2)/[\Pi(2), \Pi(2)]$ is a free $\mathbb{Z}_p[[\Pi^{\mathrm{ab}}]]$-module of rank one generated by $[x, y]$, the action of $G_{\mathbb{Q}(\mu_{p^\infty})}$ determines a homomorphism

$$\alpha_{0,3} \colon G^{\mathrm{ab}}_{\mathbb{Q}(\mu_{p^\infty})} \to \mathrm{Aut}\,(\Pi(2)/[\Pi(2), \Pi(2)]) \xleftarrow{\sim} \mathbb{Z}_p[[\Pi^{\mathrm{ab}}]]^\times.$$

In the following, we shall identify $\mathbb{Z}_p[[\Pi^{\mathrm{ab}}]]$ with the power series ring in two variables $\mathbb{Z}_p[[T_1, T_2]]$ by putting $T_1 \coloneqq x - 1$ and $T_2 \coloneqq y - 1$ and regard $\mathbb{Z}_p[[T_1, T_2]]$ as a subring of $\mathbb{Q}_p[[U_1, U_2]]$ where $U_i \coloneqq \log(1 + T_i)$ for $i = 1, 2$.

In his paper [Iha86b], Ihara conjectured the following explicit formula for $\alpha_{0,3}(\sigma)$ for every $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ and proved the conjecture for regular primes. Later, the formula was fully proved by Ihara-Kaneko-Yukinari:

Theorem A.1 (Ihara-Kaneko-Yukinari [IKY87]). *For every $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$,*

$$\alpha_{0,3}(\sigma) = \sum_{m \geq 3\colon \, odd} \frac{\kappa_m(\sigma)}{1 - p^{m-1}} \sum_{i+j=m} \frac{U_1^{m_1} U_2^{m_2}}{m_1! m_2!}.$$

Here, for every odd $m \geq 3$, $\kappa_m \colon G^{\mathrm{ab}}_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$ is the m-th Soulé character defined below.

In [Sou81], Soulé introduced characters $\kappa_m \colon G^{\mathrm{ab}}_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$ for every odd $m \geq 3$. If we fix a basis $(\zeta_n)_n \in T_p(\mathbb{G}_m) = \mathbb{Z}_p(1)$ (i.e. $\zeta_n \in \mu_{p^n}$ is a primitive p^n-th root of unity which satisfies $\zeta_{n+1}^p = \zeta_n$ for each $n \in \mathbb{Z}_{\geq 0}$), κ_m corresponds to the following Kummer character for every $n \geq 1$:

$$\zeta_n^{\kappa_m(\sigma)} = \frac{\sigma\left(\left(\prod_{1 \leq a \leq p^n, (a,p)=1} (1 - \zeta_n^a)^{a^{m-1}}\right)^{\frac{1}{p^n}}\right)}{\left(\prod_{1 \leq a \leq p^n, (a,p)=1} (1 - \zeta_n^a)^{a^{m-1}}\right)^{\frac{1}{p^n}}}.$$

The Soulé characters depend on the choice of $(\zeta_n)_n \in \mathbb{Z}_p(1)$, but such ambiguities are only multiples by $\mathbb{Z}_p^\times$.

The important properties of the Soulé characters are the following : κ_m is nonzero for every odd $m \geq 3$ and, moreover, is surjective for all odd $m \geq 3$ if and only if the Vandiver conjecture holds for p (for more details, see Soulé [Sou81] and Ichimura-Sakaguchi [IS87]).

A.2 Deligne-Ihara conjecture and its consequence

Let $\Omega_T^* := \bar{\mathbb{Q}}^{\ker(\rho_{T,p})}$ and Ω_T the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p (and the infinite place ∞, if $p = 2$).

Lemma A.2. *Ω_T^* is contained in Ω_T.*

Proof. The claim follows from the fact that T has good reduction everywhere and $\rho_{T,p}(G_{\mathbb{Q}(\mu_p)})$ is contained in $\ker(\mathrm{Out}(\Pi) \to \mathrm{Aut}(\Pi^{\mathrm{ab}}/p))$, which is a pro-$p$ group. $\square$

Anderson and Ihara [AI88, Theorem 2 (IV)] already observed that Ω_T^* is a pro-p nonabelian infinite Galois extension over $\mathbb{Q}(\mu_{p^\infty})$. In that paper, Ω_T^* is proved to be generated by higher circular p-units, which are certain generalization of cyclotomic p-units. Moreover, they asked the following question [AI88, page 272, (a)]:

Is Ω_T^* equal to Ω_T?

Sharifi [Sha02] uses the Deligne-Ihara conjecture to answer this question affirmatively. To state the Deligne-Ihara conjecture, we introduce a descending central filtration on the pro-p mapping class group of type $(0,3)$ induced by the descending central series of $\Pi_{0,3}$. We define

$$\tilde{\Gamma}_{0,3} := \{f \in \mathrm{Aut}(\Pi) \mid f \text{ preserves the conjugacy class of inertia subgroups at each cusp}\}$$

and $\Gamma_{0,3} := \tilde{\Gamma}/\mathrm{Inn}(\Pi)$. The latter group $\Gamma_{0,3}$ is called *the pro-p mapping class group of type* $(0,3)$. The group $\tilde{\Gamma}_{0,3}$ comes equipped with a descending central filtration $\{F^m\tilde{\Gamma}_{0,3}\}_{m\geq 1}$ defined by

$$F^m\tilde{\Gamma}_{0,3} := \ker\left(\tilde{\Gamma}_{0,3} \to \mathrm{Aut}(\Pi/\Pi(m+1))\right).$$

This filtration naturally induces a descending central filtration $\{F^m\Gamma_{0,3}\}_{m\geq 1}$ of $\Gamma_{0,3}$ by taking $F^m\Gamma_{0,3}$ to be the image of $F^m\tilde{\Gamma}_{0,3}$ under the natural projection.

Note that the absolute Galois group $G_{\mathbb{Q}}$ has a descending central filtration $\{F^mG_{\mathbb{Q}}\}_{m\geq 1}$ where $F^mG_{\mathbb{Q}} := \rho_{T,p}^{-1}(F^m\Gamma_{0,3})$. We denote the m-th graded quotient $F^mG_{\mathbb{Q}}/F^{m+1}G_{\mathbb{Q}}$ by $\mathfrak{t}_m$ and then the direct sum $\mathfrak{t} := \bigoplus_{m\geq 1}\mathfrak{t}_m$ naturally has a structure of graded Lie algebra over $\mathbb{Z}_p$, with its bracket product induced by commutators.

By definition, each graded quotient $\mathfrak{t}_m$ is naturally embedded into $F^m\Gamma_{0,3}/F^{m+1}\Gamma_{0,3}$, which is a free $\mathbb{Z}_p$-module of finite rank. Moreover, the group $G_{\mathbb{Q}}/F^1G_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ acts on $\mathfrak{t}_m$ through χ_{cyc}^m. Hence $\mathfrak{t}_m$ is isomorphic to a finite direct sum of the m-th Tate twist $\mathbb{Z}_p(m)$.

For every odd $m \geq 3$, the restricted character $\kappa_m \mid_{F^mG_{\mathbb{Q}}}$ is nonzero and $\kappa_m \mid_{F^mG_{\mathbb{Q}}}$ factors through $F^mG_{\mathbb{Q}} \to \mathfrak{t}_m$ (cf. Ihara [Iha89]). Take an arbitrary element $\sigma_m \in F^mG_{\mathbb{Q}}$ so that $\kappa_m(\sigma_m)$ generates $\kappa_m(F^mG_{\mathbb{Q}})$ and denote the image of σ_m in $\mathfrak{t}_m$ by the same letter.

There is a famous conjecture, attributed to Deligne by Ihara [Iha89, page 300], states that $\{\sigma_m\}_{m\geq 3,\mathrm{odd}}$ forms a free basis of $\mathfrak{t}\otimes\mathbb{Q}_p$ as a $\mathbb{Q}_p$-graded Lie algebra.

Conjecture A.3 (The Deligne-Ihara conjecture, proved by Hain-Matsumoto [HM03] and Brown [Bro12])**.** *As a graded Lie algebra over $\mathbb{Q}_p$, $\mathfrak{t}\otimes\mathbb{Q}_p$ is freely generated by $\{\sigma_m\}_{m\geq 3,odd}$.*

In this result, Hain and Matsumoto established the generalization portion of the conjecture by using their theory of weighted completion and, Brown proved the freeness portion of the conjecture as a consequence of properties of motivic periods of the category of mixed Tate motives over $\mathrm{Spec}(\mathbb{Z})$.

Theorem A.4 (Sharifi [Sha02, Theorem 1.1])**.** *Assume $p>2$ is regular and Conjecture A.3 holds for p. Then the equality $\Omega_T^* = \Omega_T$ holds.*

By combining Theorem A.4 with the Deligne-Ihara conjecture, now a theorem of Hain-Matsumoto and Brown, Anderson-Ihara's question has an affirmative answer when $p>2$ is regular.

References

[AI88] Greg Anderson and Yasutaka Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293. MR 960948

[Asa95] Mamoru Asada, *Two properties of the filtration of the outer automorphism groups of certain groups*, Math. Z. **218** (1995), no. 1, 123–133.

[Bro12] Francis Brown, *Mixed Tate motives over* $\mathbb{Z}$, Ann. of Math. (2) **175** (2012), no. 2, 949–976.

[Del89] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 79–297.

[dS87] Ehud de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987, p-adic L functions.

[HM03] Richard Hain and Makoto Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of* $\mathbb{P}^1-\{0,1,\infty\}$, Compositio Math. **139** (2003), no. 2, 119–167.

[HM11] Yuichiro Hoshi and Shinichi Mochizuki, *On the combinatorial anabelian geometry of nodally nondegenerate outer representations*, Hiroshima Math. J. **41** (2011), no. 3, 275–342.

[Iha86a] Yasutaka Ihara, *On Galois representations arising from towers of coverings of* $\mathbf{P}^1\setminus\{0,1,\infty\}$, Invent. Math. **86** (1986), no. 3, 427–459.

[Iha86b] ______, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106.

[Iha89] ______, *The Galois representation arising from* $\mathbf{P}^1 - \{0, 1, \infty\}$ *and Tate twists of even degree*, Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 299–313.

[Iha01] ______, *On pro-p extensions of algebraic number fields (Recent topics related to Greenberg's generalized conjecture)*, no. 1200, 2001, Algebraic number theory and related topics (Japanese) (Kyoto, 2000).

[Iha02] ______, *Some arithmetic aspects of Galois actions in the pro-p fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 247–273.

[IKY87] Yasutaka Ihara, Masanobu Kaneko, and Atsushi Yukinari, *On some properties of the universal power series for Jacobi sums*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 65–86.

[IS87] H. Ichimura and K. Sakaguchi, *The nonvanishing of a certain Kummer character* χ_m *(after C. Soulé), and some related topics*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 53–64.

[Ish23] Shun Ishii, *On Kummer characters arising from the Galois actions on the pro-p fundamental groups of once-punctured CM elliptic curves*, submitted (2023).

[Jan89] Uwe Jannsen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology*, Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 315–360.

[Kan89] Masanobu Kaneko, *Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **36** (1989), no. 2, 363–372.

[Mat96] Makoto Matsumoto, *Galois representations on profinite braid groups on curves*, J. Reine Angew. Math. **474** (1996), 169–219.

[Nak95] Hiroaki Nakamura, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci. Univ. Tokyo **2** (1995), no. 1, 197–231.

[Nak99] ———, *Tangential base points and Eisenstein power series*, Aspects of Galois theory (Gainesville, FL, 1996), London Math. Soc. Lecture Note Ser., vol. 256, Cambridge Univ. Press, Cambridge, 1999, pp. 202–217.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[NT93] Hiroaki Nakamura and Hiroshi Tsunogai, *Some finiteness theorems on Galois centralizers in pro-l mapping class groups*, J. Reine Angew. Math. **441** (1993), 115–144.

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[RZ10] Luis Ribes and Pavel Zalesskii, *Profinite groups*, second ed., 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.

[Sha02] Romyar T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 275–284.

[Sou79] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979), no. 3, 251–295.

[Sou81] Christophe Soulé, *On higher p-adic regulators*, Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), Lecture Notes in Math., vol. 854, Springer, Berlin-New York, 1981, pp. 372–401.

[Tsu95] Hiroshi Tsunogai, *On the automorphism group of a free pro-l metaabelian group and an application to Galois representations*, Math. Nachr. **171** (1995), 315–324.

[Win81] Jean-Pierre Wintenberger, *Structure galoisienne de limites projectives d'unités locales*, Compositio Math. **42** (1980/81), no. 1, 89–103.