Strong Indecomposability of the Profinite Grothendieck-Teichmüller Group

Arata Minamide and Shota Tsujimura

February 24, 2022

Abstract

In the present paper, by applying anabelian Grothendieck Conjecture-type results, we prove that the profinite *Grothendieck-Teichmüller group* GT satisfies *strong indecomposability* [i.e., the property that every open subgroup has no nontrivial product decomposition]. This gives an affirmative answer to an open problem — which naturally arises in the context of a famous open problem concerning the comparison of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and GT — posed in a first author's previous work.

2020 Mathematics Subject Classification: Primary 14H30; Secondary 14H25.

Key words and phrases: Grothendieck-Teichmüller group; strong indecomposability; absolute Galois group; étale fundamental group; hyperbolic curve; anabelian geometry.

Contents

Introduction

Let us recall that the [profinite] Grothendieck-Teichmüller group GT has been considered to be a combinatorial approximation of the absolute Galois group $G_{\mathbb{Q}}$ of the field of rational numbers $\mathbb{Q}$ [cf. Definition 3.1; Remark 3.1.2;

[3]; [5]; [6]; [7], Introduction]. Indeed, the natural faithful outer actions of $G_{\mathbb{Q}}$ and GT on the étale fundamental group of the projective line minus the three points 0, 1, ∞, over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ determine the inclusion

$$G_{\mathbb{Q}} \subseteq \mathrm{GT},$$

and there exists a famous open question concerning this inclusion [cf. [20], §1.4]:

Question 1: Is the natural inclusion $G_{\mathbb{Q}} \subseteq \mathrm{GT}$ bijective?

With regard to Question 1, in the authors' knowledge, there is no [strong] evidence to believe that the inclusion $G_{\mathbb{Q}} \subseteq \mathrm{GT}$ is bijective. Here, we note that André defined a p-adic avatar GT_p of GT and formulated a p-adic analogue of Question 1 by using his theory of tempered fundamental groups [cf. [1], [2]]. In this local setting, the second author constructed a natural splitting $\mathrm{GT}_p \twoheadrightarrow G_{\mathbb{Q}_p}$ of the inclusion $G_{\mathbb{Q}_p} \subseteq \mathrm{GT}_p$ — where $G_{\mathbb{Q}_p}$ denotes the absolute Galois group of the field of p-adic numbers [cf. [22], Corollary B]. It seems to the authors that the existence of such a splitting may be regarded as a strong evidence to believe that the inclusion $G_{\mathbb{Q}_p} \subseteq \mathrm{GT}_p$ is bijective. However, the construction of the splitting $\mathrm{GT}_p \twoheadrightarrow G_{\mathbb{Q}_p}$ heavily depends on a certain rigidity of tempered fundamental groups [cf. [22], Theorem C]. Thus, at the time of writing the present paper, the authors do not regard the existence of the splitting in the local setting as an evidence to believe that the inclusion $G_{\mathbb{Q}} \subseteq \mathrm{GT}$ is bijective.

Since Question 1 is far-reaching, the following question has been considered to be important in the literatures [cf., e.g., [20], §1.4]:

Question 2: Let $\mathbb{P}$ be a group-theoretic property that $G_{\mathbb{Q}}$ satisfies. Then does GT satisfy the property $\mathbb{P}$?

Concerning Question 2, for instance, Lochak-Schneps proved a remarkable result that the normalizer of a complex conjugation $\iota \in \mathrm{GT}$ coincides with the group [of order 2] generated by ι [cf. [9], Proposition 4, (ii)]. [Note that the analogous result for $G_{\mathbb{Q}}$ follows from the approximation theorem — cf. [17], Corollary 12.1.4.] On the other hand, the first author posed the following question [cf. [10], Introduction]:

Question 3: Is GT strongly indecomposable?

[Note that the strong indecomposability of $G_{\mathbb{Q}}$ follows from the fact that number fields are Hilbertian — cf. [4], Proposition 13.4.1; [4], Corollary 13.8.4.] We remark that the indecomposability of GT follows from Lochak-Schneps's result [cf. Remark 3.4.1]. However, this argument does not work for open subgroups of GT that do not contain ι. In the present paper, we also give a complete [much more general] affirmative answer to Question 3.

Let K ($\subseteq \overline{\mathbb{Q}}$) be a number field; Z a hyperbolic curve of genus 0 over K. Write $G_K \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{\mathbb{Q}}/K)$; $Z_{\overline{\mathbb{Q}}} \stackrel{\mathrm{def}}{=} Z \times_K \overline{\mathbb{Q}}$; $\Pi_{Z_{\overline{\mathbb{Q}}}}$ for the étale fundamental group of $Z_{\overline{\mathbb{Q}}}$ [relative to a suitable choice of basepoint];

$$\mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \subseteq \mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}})$$

for the subgroup of outer automorphisms of $\Pi_{Z_{\overline{\mathbb{Q}}}}$ that induce the identity automorphisms on the set of the conjugacy classes of cuspidal inertia subgroups of $\Pi_{Z_{\overline{\mathbb{Q}}}}$ [i.e., the stabilizer subgroups associated to pro-cusps of the pro-universal covering of the hyperbolic curve $Z_{\overline{\mathbb{Q}}}$]. Then the natural outer action of G_K on $\Pi_{Z_{\overline{\mathbb{Q}}}}$ determines an injection $G_K \hookrightarrow \mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ [cf. [8], Theorem C]. We shall regard G_K as a subgroup of $\mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ via this injection. Recall that, if we take Z to be the projective line minus the three points 0, 1, ∞, over K, then GT may be regarded as a closed subgroup of $\mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ [cf. Remark 3.1.1]. Then our main result is the following [cf. Theorem 3.4]:

Theorem A. *Let $G \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ be a closed subgroup such that G contains an open subgroup of G_K. Then G is strongly indecomposable. In particular, the Grothendieck-Teichmüller group* GT *is strongly indecomposable.*

Note that the first author proved that a pro-l analogue of Theorem A holds [cf. Remark 3.4.2; [10], Theorem 6.1]. However, the proof heavily depends on the [easily verified] fact that $\mathbb{Z}_l$ is indecomposable. In contrast, since $\widehat{\mathbb{Z}}$ is decomposable, a similar argument to the argument applied in the proof of [10], Theorem 6.1 does not work in our situation. To overcome this difficulty, we apply [highly nontrivial] Saidi-Tamagawa's result on the pro-prime-to-p version of the Grothendieck Conjecture for hyperbolic curves over finite fields of characteristic p [cf. [19], Theorem 1], together with some considerations on "almost surface groups" [cf. Lemma 2.2].

On the other hand, in our previous work [cf. [12]], we introduced the notion of the *strong internal indecomposability* — which is a stronger property than the strong indecomposability — of profinite groups. Recall that $\mathbb{Q}$ is Hilbertian. Then it follows from [12], Theorem A, (ii), that $G_{\mathbb{Q}}$ is strongly internally indecomposable. Thus, from the viewpoint of Question 3, it is natural to pose the following question, which may be regarded as a further generalization of [the second assertion of] Theorem A:

Question 4: Is GT strongly internally indecomposable?

However, at the time of writing the present paper, the authors do not know whether the answer to this question is affirmative or not.

The present paper is organized as follows. In §1, we recall some basic definitions and prove a certain group-theoretic lemma which reduces our problem concerning full profinite fundamental groups to a problem concerning pro-prime-to-p fundamental groups. In §2, by applying Grothendieck Conjecture-type results, we compute various Galois centralizers. In §3, we first recall the definition of the Grothendieck-Teichmüller group GT. Then we apply results obtained in §1, §2 to prove that GT is strongly indecomposable [cf. Theorem A].

Notations and Conventions

Numbers: The notation $\mathfrak{Primes}$ will be used to denote the set of prime numbers. The notation $\mathbb{Q}$ will be used to denote the field of rational numbers. The notation $\mathbb{Z}$ will be used to denote the ring of integers. The notation $\widehat{\mathbb{Z}}$ will be used to denote the profinite completion of the underlying additive group of $\mathbb{Z}$. The notation $\mathbb{Z}_{\geq 1}$ will be used to denote the set of positive integers. We shall refer to a finite extension field of $\mathbb{Q}$ as a *number field*. If p is a prime number, then the notation $\mathbb{Z}_p$ will be used to denote the ring of p-adic integers; the notation $\mathbb{F}_p$ will be used to denote the finite field of cardinality p. If A is a commutative ring, then the notation $A^\times$ will be used to denote the group of units of A.

Fields: Let F be a perfect field; $\overline{F}$ an algebraic closure of F. Then we shall write $\mathrm{char}(F)$ for the characteristic of F; $G_F \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{F}/F)$.

Schemes: Let S be a scheme. Then we shall write $\mathrm{Aut}(S)$ for the group of automorphisms of S. Let K be a field; $K \subseteq L$ a field extension; X an algebraic variety [i.e., a separated, of finite type, and geometrically integral scheme] over K. Then we shall write $X_L \stackrel{\mathrm{def}}{=} X \times_K L$; $\mathrm{Aut}_K(X)$ for the group of automorphisms of X over K; $\mathbb{P}^1_K$ for the projective line over K.

Profinite groups: Let $\Sigma \subseteq \mathfrak{Primes}$ be a nonempty subset of prime numbers; G a profinite group. Then we shall write G^Σ for the maximal pro-Σ quotient of G; $\mathrm{Aut}(G)$ for the group of automorphisms of G [in the category of profinite groups], $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ for the group of inner automorphisms of G, and $\mathrm{Out}(G) \stackrel{\mathrm{def}}{=} \mathrm{Aut}(G)/\mathrm{Inn}(G)$. If p is a prime number, then we shall also write $G^p \stackrel{\mathrm{def}}{=} G^{\{p\}}$; $G^{(p)'} \stackrel{\mathrm{def}}{=} G^{\mathfrak{Primes}\setminus\{p\}}$.

Suppose that G is topologically finitely generated. Then G admits a basis of *characteristic open subgroups* [cf. [18], Proposition 2.5.1, (b)], which thus induces a *profinite topology* on the groups $\mathrm{Aut}(G)$ and $\mathrm{Out}(G)$.

Fundamental groups: Let S be a connected locally Noetherian scheme. Then we shall write Π_S for the étale fundamental group of S, relative to a suitable choice of basepoint. [Note that, for any field F, $\Pi_{\mathrm{Spec}(F)} \cong G_F$.]

1 Preliminaries

In the present section, we recall some basic definitions and prove a certain group-theoretic lemma [cf. Lemma 1.4] which will be applied in §3.

First, we recall basic notions concerning profinite groups.

Definition 1.1 ([15], Notations and Conventions; [15], Definition 3.1)**.** Let G be a profinite group; $H \subseteq G$ a closed subgroup of G.

(i) We shall write $Z_G(H)$ for the *centralizer* of H in G, i.e., the closed subgroup $\{g \in G \mid ghg^{-1} = h \text{ for any } h \in H\}$; $Z(G) \stackrel{\mathrm{def}}{=} Z_G(G)$; $N_G(H)$ for the *normalizer* of H in G, i.e., the closed subgroup $\{g \in G \mid gHg^{-1} = H\}$.

(ii) We shall say that G is *slim* if $Z_G(U) = \{1\}$ for every open subgroup U of G.

(iii) We shall say that G is *decomposable* if there exist nontrivial normal closed subgroups $H_1 \subseteq G$ and $H_2 \subseteq G$ such that $G = H_1 \times H_2$. We shall say that G is *indecomposable* if G is not decomposable. We shall say that G is *strongly indecomposable* if every open subgroup of G is indecomposable.

Definition 1.2 ([14], Definition 1.1, (iii))**.** Let G, Q be profinite groups; $q : G \twoheadrightarrow Q$ an epimorphism [in the category of profinite groups]; p a prime number; $\Sigma \subseteq \mathfrak{Primes}$ a nonempty subset of prime numbers. Then we shall say that Q is an *almost pro-*Σ*-maximal quotient* of G if there exists a normal open subgroup $N \subseteq G$ such that $\mathrm{Ker}(q)$ coincides with the kernel of the natural surjection $N \twoheadrightarrow N^{\Sigma}$. If $\Sigma = \{p\}$, then we shall also say that Q is an *almost pro-*p*-maximal quotient* of G.

Next, we prove a certain group-theoretic lemma which will be applied in §3.

Lemma 1.3. *Let G be a profinite group; $\{G_i\}_{i\in I}$ a directed subset of the set of characteristic open subgroups of G — where $j \geq i \Leftrightarrow G_j \subseteq G_i$ — such that*

$$\bigcap_{i\in I} G_i = \{1\}.$$

Write $\phi_i : \mathrm{Out}(G) \to \mathrm{Out}(G/G_i)$ for the natural homomorphism. Then

$$\bigcap_{i\in I} \mathrm{Ker}(\phi_i) = \{1\}.$$

Proof. Let $\sigma \in \bigcap_{i\in I} \mathrm{Ker}(\phi_i)$ ($\subseteq \mathrm{Out}(G)$) be an element; $\tilde{\sigma} \in \mathrm{Aut}(G)$ a lifting of $\sigma \in \mathrm{Out}(G)$. For each $i \in I$, write $\tilde{\sigma}_i \in \mathrm{Aut}(G/G_i)$ for the automorphism induced by $\tilde{\sigma}$. Then since $\sigma \in \mathrm{Ker}(\phi_i)$, it holds that $\tilde{\sigma}_i$ is an inner automorphism. Let $\gamma_i \in G/G_i$ be an element which determines the inner automorphism $\tilde{\sigma}_i$. Write

$$C_i \stackrel{\mathrm{def}}{=} \gamma_i \cdot Z(G/G_i) \subseteq G/G_i.$$

Here, we note that, if $i_1 \geq i_2$ ($i_1, i_2 \in I$), then the natural surjection $G/G_{i_1} \twoheadrightarrow G/G_{i_2}$ induces a map $C_{i_1} \to C_{i_2}$. Observe that since C_i ($i \in I$) is a finite nonempty set, the inverse limit $\varprojlim_{i\in I} C_i$ is nonempty. Let

$$\gamma \in \varprojlim_{i\in I} C_i \quad (\subseteq \varprojlim_{i\in I} G/G_i = G)$$

[cf. [18], Corollary 1.1.6] be an element. Then it follows immediately from the various definitions involved that $\tilde{\sigma}$ is an inner automorphism determined by γ. This completes the proof of Lemma 1.3. $\square$

Lemma 1.4. *Let G be a topologically finitely generated profinite group; $S \subseteq \mathfrak{Primes}$ a finite subset. Then the natural homomorphism*

$$\mathrm{Out}(G) \longrightarrow \prod_{p \in \mathfrak{Primes} \setminus S} \mathrm{Out}(G^{(p)'})$$

is injective.

Proof. Since G is topologically finitely generated, there exists a directed subset $\{G_i\}_{i \in I}$ of the set of characteristic open subgroups of G — where $j \geq i \iff G_j \subseteq G_i$ — such that

$$\bigcap_{i \in I} G_i = \{1\}$$

[cf. [18], Proposition 2.5.1, (b)]. Fix such a family. For each $i \in I$, let $p_i \in \mathfrak{Primes} \setminus S$ be such that p_i does not divide the order of the finite group G/G_i. Then the natural surjection $G \twoheadrightarrow G/G_i$ factors through the natural surjection $G \twoheadrightarrow G^{(p_i)'}$. Thus, Lemma 1.4 follows immediately from Lemma 1.3. □

Next, we recall basic notions related to hyperbolic curves.

Definition 1.5 ([15], Definition 2.1)**.**

(i) Let k be a field; $\overline{k}$ an algebraic closure of k; X a smooth curve [i.e., a one-dimensional, smooth, separated, of finite type, and geometrically connected scheme] over k. Write $\overline{X}_{\overline{k}}$ for the smooth compactification of $X_{\overline{k}}$ over $\overline{k}$. Then we shall say that X is a *smooth curve of type* (g, r) over k if the genus of $X_{\overline{k}}$ is g, and the cardinality of the underlying set of $\overline{X}_{\overline{k}} \setminus X_{\overline{k}}$ is r. If X is a smooth curve of type (g, r) over k, and $2g - 2 + r > 0$, then we shall say that X is a *hyperbolic curve* over k.

(ii) Let $n \in \mathbb{Z}_{\geq 1}$ be an element; k a field; X a hyperbolic curve over k. Write

$$X_n \stackrel{\mathrm{def}}{=} X^{\times n} \setminus (\bigcup_{1 \leq i < j \leq n} \Delta_{i,j}),$$

where $X^{\times n}$ denotes the fiber product of n copies of X over k; $\Delta_{i,j}$ denotes the diagonal divisor of $X^{\times n}$ associated to the i-th and j-th components. We shall refer to X_n as the *n-th configuration space* associated to X.

The following notations will be used in §2, §3.

Definition 1.6. Let k be a field; $\overline{k}$ an algebraic closure of k; Z an algebraic variety over k. Then we have an exact sequence of profinite groups

$$1 \longrightarrow \Pi_{Z_{\overline{k}}} \longrightarrow \Pi_Z \longrightarrow G_k \longrightarrow 1.$$

We shall write $\rho_Z : G_k \to \mathrm{Out}(\Pi_{Z_{\overline{k}}})$ for the outer representation determined by the above exact sequence. Let $\Sigma \subseteq \mathfrak{Primes}$ be a nonempty subset of prime numbers. Then we shall write

$$\rho_Z^{\Sigma} : G_k \to \mathrm{Out}(\Pi^{\Sigma}_{Z_{\overline{k}}})$$

for the outer representation induced by ρ_Z;

$$\Pi_Z^{[\Sigma]} \stackrel{\mathrm{def}}{=} \Pi_Z/\mathrm{Ker}(\Pi_{Z_{\overline{k}}} \twoheadrightarrow \Pi^{\Sigma}_{Z_{\overline{k}}}).$$

Let p be a prime number. If $\Sigma = \{p\}$ (respectively, $\Sigma = \mathfrak{Primes} \setminus \{p\}$), then we shall also write $\rho_Z^p \stackrel{\mathrm{def}}{=} \rho_Z^{\Sigma}$; $\Pi_Z^{[p]} \stackrel{\mathrm{def}}{=} \Pi_Z^{[\Sigma]}$ (respectively, $\rho_Z^{(p)'} \stackrel{\mathrm{def}}{=} \rho_Z^{\Sigma}$; $\Pi_Z^{[p]'} \stackrel{\mathrm{def}}{=} \Pi_Z^{[\Sigma]}$).

2 Computations of various Galois centralizers

In the present section, by applying Grothendieck Conjecture-type results, we compute various Galois centralizers. These computations will be applied in §3.

Definition 2.1. Let k be an algebraically closed field; $\Sigma \subseteq \mathfrak{Primes}$ a nonempty subset of prime numbers such that $\mathrm{char}(k) \notin \Sigma$; Z a hyperbolic curve over k; Q an almost pro-Σ maximal quotient of Π_Z. Then we shall write

$$\mathrm{Out}^{|\mathrm{C}|}(Q) \subseteq \mathrm{Out}(Q)$$

for the subgroup of outer automorphisms of Q that induce the identity automorphisms on the set of the conjugacy classes of cuspidal inertia subgroups of Q, where the cuspidal inertia subgroups of Q may be defined as the images of the cuspidal inertia subgroups of Π_Z via the natural surjection $\Pi_Z \twoheadrightarrow Q$.

Next, we observe the following applications [cf. Lemmas 2.2, 2.3, 2.4] of highly nontrivial Grothendieck Conjecture-type results [cf. [13], Theorem A; [19], Theorem 1]:

Lemma 2.2. *Let l be a prime number; $n \in \mathbb{Z}_{\geq 1}$; $K \subseteq \overline{\mathbb{Q}}$ a number field; $Z \subseteq \mathbb{P}^1_K \setminus \{0, 1, \infty\}$ an open subscheme obtained by forming the complement of a finite subset of K-rational points of $\mathbb{P}^1_K \setminus \{0, 1, \infty\}$. [In particular, Z is a hyperbolic curve of genus 0 over K.] Write $(\mathbb{P}^1_{\overline{\mathbb{Q}}} \supseteq)\ Y_{\overline{\mathbb{Q}}} \to Z_{\overline{\mathbb{Q}}}\ (\subseteq \mathbb{P}^1_{\overline{\mathbb{Q}}})$ for the finite étale Galois covering of $Z_{\overline{\mathbb{Q}}}$ of degree n determined by $t \mapsto t^n$;*

$$Q \stackrel{\mathrm{def}}{=} \Pi_{Z_{\overline{\mathbb{Q}}}}/\mathrm{Ker}(\Pi_{Y_{\overline{\mathbb{Q}}}} \twoheadrightarrow \Pi^{l}_{Y_{\overline{\mathbb{Q}}}}); \quad \rho : G_K \to \mathrm{Out}(Q)$$

for the homomorphism induced by the outer representation $G_K \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ [where we regard G_K as a subgroup of $\mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ via the natural outer action of G_K on $\Pi_{Z_{\overline{\mathbb{Q}}}}$ — cf. [8], Theorem C]. Then

$$Z_{\mathrm{Out}^{|\mathrm{C}|}(Q)}(\mathrm{Im}(\rho)) = \{1\}.$$

Proof. Let $\sigma \in Z_{\mathrm{Out}^{|\mathbf{C}|}(Q)}(\mathrm{Im}(\rho))$ be an element. Recall that

- σ induces the identity automorphism on the set of the conjugacy classes of cuspidal inertia subgroups [which are pro-cyclic subgroups] of Q;
- the normal open subgroup $\Pi_{Y_{\overline{\mathbb{Q}}}} \subseteq \Pi_{Z_{\overline{\mathbb{Q}}}}$ [determined by the finite étale Galois covering $Y_{\overline{\mathbb{Q}}} \to Z_{\overline{\mathbb{Q}}}$] may be characterized as the normal open subgroup topologically generated by the cuspidal inertia subgroups of $\Pi_{Z_{\overline{\mathbb{Q}}}}$ that is not associated to the cusps 0, ∞, and the [unique] closed subgroups of the cuspidal inertia subgroups of $\Pi_{Z_{\overline{\mathbb{Q}}}}$ associated to the cusps 0, ∞, of index n.

Thus, any lifting $\in \mathrm{Aut}(Q)$ of σ induces an automorphism of $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$. Let $\tilde{\sigma} \in \mathrm{Aut}(Q)$ be a lifting of σ such that the automorphism $\tilde{\sigma}|_{\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}} \in \mathrm{Aut}(\Pi^{l}_{Y_{\overline{\mathbb{Q}}}})$ induced by $\tilde{\sigma}$ preserves the $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$-conjugacy class of cuspidal inertia subgroups of $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$ associated to the cusp 1. Here, we note that since $\tilde{\sigma}$ preserves the Q-conjugacy class of cuspidal inertia subgroups of Q associated to the cusp 0 (respectively, ∞), and the finite étale Galois covering $Y_{\overline{\mathbb{Q}}} \to Z_{\overline{\mathbb{Q}}}$ is totally ramified over the cusp 0 (respectively, ∞), it holds that $\tilde{\sigma}|_{\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}}$ preserves the $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$-conjugacy class of cuspidal inertia subgroups of $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$ associated to the cusp 0 (respectively, ∞). Write

$$\sigma_Y : \Pi^{l}_{Y_{\overline{\mathbb{Q}}}} \xrightarrow{\sim} \Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$$

for the outer automorphism determined by $\tilde{\sigma}|_{\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}} \in \mathrm{Aut}(\Pi^{l}_{Y_{\overline{\mathbb{Q}}}})$. Observe that since the outer action of G_K, together with σ_Y, on $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$ preserves the $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$-conjugacy class of cuspidal inertia subgroups of $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$ associated to the cusp 1, it follows from our assumption that $\sigma \in Z_{\mathrm{Out}^{|\mathbf{C}|}(Q)}(\mathrm{Im}(\rho))$ that σ_Y commutes with the outer action of G_K on $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$. Then it follows from the Grothendieck Conjecture [cf. [13], Theorem A] that σ_Y arises from a unique isomorphism $f : Y_{\overline{\mathbb{Q}}} \xrightarrow{\sim} Y_{\overline{\mathbb{Q}}}$ of schemes over $\overline{\mathbb{Q}}$. Note that since $\tilde{\sigma}|_{\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}}$ induces the identity automorphism on the set of the $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$-conjugacy classes of cuspidal inertia subgroups of $\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}$ associated to the cusps 0, 1, ∞, it holds that f induces the identity automorphism on the subset $\{0, 1, \infty\} \subseteq \mathbb{P}^1_{\overline{\mathbb{Q}}}$. In particular, we conclude that f is the identity automorphism, hence that σ_Y is the identity outer automorphism. Recall that the automorphism $\tilde{\sigma}|_{\Pi^{l}_{Y_{\overline{\mathbb{Q}}}}} \in \mathrm{Aut}(\Pi^{l}_{Y_{\overline{\mathbb{Q}}}})$ is the restriction of $\tilde{\sigma} \in \mathrm{Aut}(Q)$. Thus, since Q is slim [cf. [15], Proposition 1.4], it follows from [10], Lemma 1.6, that $\tilde{\sigma}$ is an inner automorphism, hence that σ is the identity outer automorphism. This completes the proof of Lemma 2.2. □

Lemma 2.3. *Let p be a prime number; $\Sigma \subseteq \mathfrak{Primes}$ a nonempty subset of prime numbers such that $p \notin \Sigma$; k a finite field of characteristic p. In the notation of*

Definition 1.6, suppose that Z is a hyperbolic curve of genus 0 over k such that all cusps of Z are k-rational. Write $\rho \stackrel{\text{def}}{=} \rho_Z^\Sigma$. Then the following hold:

(i) Suppose that $\Sigma = \mathfrak{Primes}\setminus\{p\}$. Then the natural homomorphism $\mathrm{Aut}(Z_{\overline{k}}) \to \mathrm{Out}(\Pi_{Z_{\overline{k}}}^\Sigma)$ determines an isomorphism

$$\mathrm{Aut}(Z_{\overline{k}}) \xrightarrow{\sim} Z_{\mathrm{Out}(\Pi_{Z_{\overline{k}}}^\Sigma)}(\rho(G_k)).$$

(ii) Let l be a prime number $\neq p$. Suppose that $\Sigma = \{l\}$ or $\Sigma = \mathfrak{Primes} \setminus \{p\}$. Then, if we write $\chi_\Sigma : \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{k}}}^\Sigma) \to (\widehat{\mathbb{Z}}^\Sigma)^\times$ for the pro-Σ cyclotomic character [which is obtained by considering the actions on the cuspidal inertia subgroups of $\Pi_{Z_{\overline{k}}}^\Sigma$], then the natural composite

$$Z_{\mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{k}}}^\Sigma)}(\rho(G_k)) \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{k}}}^\Sigma) \xrightarrow{\chi_\Sigma} (\widehat{\mathbb{Z}}^\Sigma)^\times$$

is injective.

Proof. First, we verify assertion (i). Write $\mathrm{Out}_{G_k}(\Pi_Z^{[p]'})$ for the group of $\Pi_{Z_{\overline{k}}}^{(p)'}$-outer automorphisms of $\Pi_Z^{[p]'}$ that lie over G_k [cf. Definition 1.6]. Then since $\Pi_{Z_{\overline{k}}}^{(p)'}$ is center-free [cf. [15], Proposition 1.4], it is well-known that the natural homomorphism

$$\mathrm{Out}_{G_k}(\Pi_Z^{[p]'}) \to Z_{\mathrm{Out}(\Pi_{Z_{\overline{k}}}^{(p)'})}(\rho(G_k))$$

is an isomorphism [cf. [21], Lemma 7.1]. On the other hand, since G_k is abelian, it follows immediately from [19], Theorem 1, together with the definition of $\mathrm{Out}_{G_k}(\Pi_Z^{[p]'})$, that

$$\mathrm{Aut}(Z_{\overline{k}}/Z) \xrightarrow{\sim} \mathrm{Out}_{G_k}(\Pi_Z^{[p]'}),$$

where $\mathrm{Aut}(Z_{\overline{k}}/Z) \subseteq \mathrm{Aut}(Z_{\overline{k}})$ denotes the subgroup consisting of automorphisms of $Z_{\overline{k}}$ that induce automorphisms of Z compatible with the natural morphism $Z_{\overline{k}} \to Z$.

Next, we verify the following assertion:

Claim 2.3.A: The inclusion $\mathrm{Aut}(Z_{\overline{k}}/Z) \subseteq \mathrm{Aut}(Z_{\overline{k}})$ is bijective.

Indeed, let $\alpha \in \mathrm{Aut}(Z_{\overline{k}})$ be an element; $\sigma \in G_k$ ($\hookrightarrow \mathrm{Aut}(Z_{\overline{k}})$). Then since G_k is abelian, it follows that

$$\gamma \stackrel{\text{def}}{=} \sigma \circ \alpha \circ \sigma^{-1} \circ \alpha^{-1} \in \mathrm{Aut}_{\overline{k}}(Z_{\overline{k}}).$$

Next, we note that γ induces the identity automorphism on the set of cusps of $Z_{\overline{k}}$. Thus, we conclude that $\gamma = 1$, hence that α induces a unique automorphism $\in \mathrm{Aut}(Z)$ compatible with the natural morphism $Z_{\overline{k}} \to Z$. This completes the proof of Claim 2.3.A.

Thus, by applying Claim 2.3.A, we obtain a natural isomorphism

$$\phi : \mathrm{Aut}(Z_{\overline{k}}) \xrightarrow{\sim} Z_{\mathrm{Out}(\Pi^{(p)'}_{Z_{\overline{k}}})}(\rho(G_k)).$$

This completes the proof of assertion (i).

Next, we verify assertion (ii). If $\Sigma = \{l\}$, then the desired conclusion follows immediately from the latter half of the proof of [16], Proposition 2.2.4. Thus, we may assume without loss of generality that $\Sigma = \mathfrak{Primes} \setminus \{p\}$. Write $\mathrm{Aut}^{|C|}(Z_{\overline{k}}) \subseteq \mathrm{Aut}(Z_{\overline{k}})$ for the subgroup of automorphisms of $Z_{\overline{k}}$ that induce the identity automorphisms on the set of cusps of $Z_{\overline{k}}$; $\chi' \stackrel{\mathrm{def}}{=} \chi_{\mathfrak{Primes}\setminus\{p\}}$. Then ϕ induces a composite

$$\mathrm{Aut}^{|C|}(Z_{\overline{k}}) \xrightarrow{\sim} Z_{\mathrm{Out}^{|C|}(\Pi^{(p)'}_{Z_{\overline{k}}})}(\rho(G_k)) \subseteq \mathrm{Out}^{|C|}(\Pi^{(p)'}_{Z_{\overline{k}}}) \xrightarrow{\chi'} (\widehat{\mathbb{Z}}^{(p)'})^{\times}.$$

Observe that this composite factors as the composite of the natural injection $\mathrm{Aut}^{|C|}(Z_{\overline{k}}) \hookrightarrow G_{\mathbb{F}_p}$ with the pro-prime-to-p cyclotomic character $G_{\mathbb{F}_p} \hookrightarrow (\widehat{\mathbb{Z}}^{(p)'})^{\times}$. Thus, we conclude that the natural composite

$$Z_{\mathrm{Out}^{|C|}(\Pi^{(p)'}_{Z_{\overline{k}}})}(\rho(G_k)) \subseteq \mathrm{Out}^{|C|}(\Pi^{(p)'}_{Z_{\overline{k}}}) \xrightarrow{\chi'} (\widehat{\mathbb{Z}}^{(p)'})^{\times}$$

is injective. This completes the proof of assertion (ii), hence of Lemma 2.3. □

Remark 2.3.1. It is natural to pose the following question:

> Question: In the notation of Lemma 2.3, (i), (ii), can the assumptions on the subset of prime numbers $\Sigma \subseteq \mathfrak{Primes}$ be dropped?

However, at the time of writing the present paper, the authors do not know whether the answer to this question is affirmative or not.

Lemma 2.4. *Let l be a prime number; $K \subseteq \overline{\mathbb{Q}}$ a number field. In the notation of Definition 1.6, suppose that $k = K$, and Z is a hyperbolic curve over K. Write $\rho \stackrel{\mathrm{def}}{=} \rho^l_Z$. Then $\mathrm{Im}(\rho)$ is nonabelian.*

Proof. Let us recall that, since K is l-cyclotomically full, it holds that $\mathrm{Im}(\rho)$ is infinite [cf. [10], Definition 4.1; [10], Lemma 4.2, (iv)]. Suppose that $\mathrm{Im}(\rho)$ is abelian. Then since $\mathrm{Im}(\rho) \subseteq Z_{\mathrm{Out}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\mathrm{Im}(\rho))$, the centralizer $Z_{\mathrm{Out}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\mathrm{Im}(\rho))$ is infinite. However, since $\mathrm{Aut}_K(Z)$ is finite, this contradicts the Grothendieck Conjecture for hyperbolic curves over number fields [cf. [13], Theorem A]. Thus, we conclude that $\mathrm{Im}(\rho)$ is nonabelian. This completes the proof of Lemma 2.4. □

3 Strong indecomposability of GT

In the present section, we prove that the Grothendieck-Teichmüller group GT is strongly indecomposable. This gives a complete affirmative solution to the problem posed by the first author of the present paper in [10], Introduction.

First, we begin by recalling the definition of GT.

Definition 3.1. Write $X \stackrel{\text{def}}{=} \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$; X_2 for the second configuration space associated to X; $p_i : \Pi_{X_2} \to \Pi_X$ for the outer surjection induced by the i-th projection $X_2 \to X$, where $i = 1, 2$. Then we shall denote

$$\mathrm{Out}^{\mathrm{FC}}(\Pi_{X_2}) \subseteq \mathrm{Out}(\Pi_{X_2})$$

by the subgroup of outer automorphisms $\sigma \in \mathrm{Out}(\Pi_{X_2})$ such that, for $i = 1, 2$,

- $\sigma(\mathrm{Ker}(p_i)) = \mathrm{Ker}(p_i)$;
- σ induces a permutation on the set of the conjugacy classes of cuspidal inertia subgroups of $\mathrm{Ker}(p_i)$, where we note that $\mathrm{Ker}(p_i)$ may be naturally identified with the étale fundamental group of a hyperbolic curve of type $(0, 4)$ over $\overline{\mathbb{Q}}$. [Recall that the cuspidal inertia subgroups of the étale fundamental group of this hyperbolic curve may be defined as the stabilizer subgroups associated to pro-cusps of the pro-universal covering of the hyperbolic curve.]

Recall that $X_2 \stackrel{\sim}{\to} \mathcal{M}_{0,5}$, where $\mathcal{M}_{0,5}$ denotes the moduli stack over $\overline{\mathbb{Q}}$ of hyperbolic curves of type $(0, 5)$. Then we have a natural action of the symmetric group $\mathfrak{S}_5$ on X_2 by permuting ordered marked points. This action determines an inclusion $\mathfrak{S}_5 \subseteq \mathrm{Out}(\Pi_{X_2})$. Then we shall write

$$\mathrm{GT} \stackrel{\text{def}}{=} \mathrm{Out}^{\mathrm{FC}}(\Pi_{X_2}) \cap Z_{\mathrm{Out}(\Pi_{X_2})}(\mathfrak{S}_5) \ (\subseteq \mathrm{Out}(\Pi_{X_2})).$$

We shall refer to GT as the *Grothendieck-Teichmüller group*. Since the natural homomorphism $\mathrm{Out}^{\mathrm{FC}}(\Pi_{X_2}) \to \mathrm{Out}(\Pi_X)$ induced by p_1 is injective [cf. [8], Theorem B], GT may be regarded as a closed subgroup of $\mathrm{Out}(\Pi_X)$.

Remark 3.1.1. In the notation of Definitions 2.1, 3.1, we note that since the symmetric group $\mathfrak{S}_3$ is center-free, it follows immediately from the various definitions involved that $\mathrm{GT} \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_X)$.

Remark 3.1.2. The Grothendieck-Teichmüller group GT was originally introduced by V.G. Drinfeld [cf. [3]]. Let us note that, a priori, the original definition is different from the above definition. However, it follows from a remarkable theorem proved by Harbater-Schneps [cf. [6]] that these two definitions are equivalent. Moreover, it follows from [7], Theorem C, that

$$\mathrm{Out}(\Pi_{X_2}) = \mathrm{GT} \times \mathfrak{S}_5.$$

Remark 3.1.3. Let us observe that there exists a natural homomorphism $G_{\mathbb{Q}} \to$ GT. Note that it follows from Belyi's theorem that this homomorphism determines an injection

$$G_{\mathbb{Q}} \subseteq \mathrm{GT}.$$

With regard to the above inclusion, let us recall the following famous open question [cf. [20], §1.4]:

Question: Is the inclusion $G_{\mathbb{Q}} \subseteq \mathrm{GT}$ bijective?

From the viewpoint of this question, the comparison of group-theoretic properties of $G_{\mathbb{Q}}$ and GT has been considered to be important.

Lemma 3.2. *Let l be a prime number; $K \subseteq \overline{\mathbb{Q}}$ a number field. In the notation of Definition 1.6, suppose that $k = K$, and Z is a hyperbolic curve of genus* 0 *over K. Write*

$$\rho_l : \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \to \mathrm{Out}^{|\mathrm{C}|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})$$

for the natural homomorphism. Let

$$G \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \ (\subseteq \mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}}))$$

be a closed subgroup such that

- *G contains an open subgroup of G_K, where we regard G_K as a subgroup of $\mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ via the natural outer action of G_K on $\Pi_{Z_{\overline{\mathbb{Q}}}}$ [cf. [8], Theorem C];*
- *there exist normal closed subgroups $G_1 \subseteq G$ and $G_2 \subseteq G$ such that $G = G_1 \times G_2$.*

Then $\rho_l(G_1) = \{1\}$ or $\rho_l(G_2) = \{1\}$.

Proof. First, by replacing K by a finite extension of K, we may assume without loss of generality that $G_K \subseteq G$. Let $\mathfrak{p}$ be a maximal ideal of the ring of integers of K such that

- the characteristic of the residue field at $\mathfrak{p}$ is not equal to l, and
- Z has good reduction at $\mathfrak{p}$;

$F \in G_K$ $(\subseteq G)$ a lifting of the Frobenius element at $\mathfrak{p}$. We shall write,

- for each $i = 1, 2$, $\mathrm{pr}_i : G \twoheadrightarrow G_i$ for the natural projection;
- $I \subseteq G_K$ for the closed subgroup topologically generated by F, where we note that I is isomorphic to $\widehat{\mathbb{Z}}$;
- $I_1 \stackrel{\mathrm{def}}{=} \mathrm{pr}_1(I) \times \{1\} \subseteq G_1 \times G_2 = G$, $I_2 \stackrel{\mathrm{def}}{=} \{1\} \times \mathrm{pr}_2(I) \subseteq G_1 \times G_2 = G$.

Here, we note that, since I is abelian, it holds that

$$I \subseteq I_1 \times I_2 \subseteq Z_G(I),$$

hence that

$$\rho_l(I) \subseteq \rho_l(I_1) \cdot \rho_l(I_2) \subseteq Z_{\rho_l(G)}(\rho_l(I)).$$

Thus, since Z has good reduction at $\mathfrak{p}$, it follows immediately from Lemma 2.3, (ii), together with the theory of specialization isomorphism, that we have the composite of natural injections

$$\rho_l(I) \subseteq \rho_l(I_1) \cdot \rho_l(I_2) \subseteq Z_{\rho_l(G)}(\rho_l(I)) \subseteq Z_{\mathrm{Out}^{|C|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l(I)) \hookrightarrow \mathbb{Z}_l^\times.$$

Note that since $\rho_l(I)$ is infinite [cf. [10], Lemma 4.2, (iv)], it holds that $\rho_l(I_1)$ is infinite, or $\rho_l(I_2)$ is infinite. We may assume without loss of generality that

$$\rho_l(I_1) \text{ is infinite.}$$

Observe that every infinite closed subgroup of $\mathbb{Z}_l^\times$ is an open subgroup. In particular, $\rho_l(I_1) \cap \rho_l(I) \subseteq \rho_l(I)$ is an open subgroup. Then since $G_2 \subseteq Z_G(I_1)$, there exists an open subgroup ${}^\dagger I \subseteq I$ such that

$$\rho_l(G_2) \subseteq Z_{\mathrm{Out}^{|C|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l({}^\dagger I)) \hookrightarrow \mathbb{Z}_l^\times$$

[cf. Lemma 2.3, (ii)].

Suppose that $\rho_l(G_2)$ is infinite. Then since $\rho_l(I) \subseteq Z_{\mathrm{Out}^{|C|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l({}^\dagger I))$ ($\hookrightarrow \mathbb{Z}_l^\times$), it holds that $\rho_l(G_2) \cap \rho_l(I) \subseteq \rho_l(I)$ is an open subgroup. On the other hand, since $G_1 \subseteq Z_G(G_2)$, there exists an open subgroup ${}^\ddagger I \subseteq {}^\dagger I$ ($\subseteq I$) such that

$$\rho_l(G_1) \subseteq Z_{\mathrm{Out}^{|C|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l({}^\ddagger I)) \hookrightarrow \mathbb{Z}_l^\times$$

[cf. Lemma 2.3, (ii)]. In particular, the closed subgroups

$$\rho_l(G_K) \subseteq \rho_l(G) = \rho_l(G_1) \cdot \rho_l(G_2) \subseteq Z_{\mathrm{Out}^{|C|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l({}^\ddagger I)) \hookrightarrow \mathbb{Z}_l^\times$$

are abelian. This contradicts Lemma 2.4. Thus, we conclude that $\rho_l(G_2)$ is finite. Then there exists a finite extension L ($\subseteq \overline{\mathbb{Q}}$) of K such that $\rho_l(G_2) \subseteq Z_{\mathrm{Out}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})}(\rho_l(G_L))$. Thus, since $\rho_l(G_2)$ induces the identity automorphism on the set of the conjugacy classes of cuspidal inertia subgroups of $\Pi^l_{Z_{\overline{\mathbb{Q}}}}$, it follows immediately from [13], Theorem A, that $\rho_l(G_2) = \{1\}$. This completes the proof of Lemma 3.2. $\square$

Definition 3.3. Let G be a profinite group; Π a topologically finitely generated profinite group; $G \to \mathrm{Out}(\Pi)$ a continuous homomorphism. Then we shall write

$$\Pi \overset{\mathrm{out}}{\rtimes} G$$

for the profinite group obtained by pulling-back the continuous homomorphism $G \to \mathrm{Out}(\Pi)$ via the natural surjection $\mathrm{Aut}(\Pi) \twoheadrightarrow \mathrm{Out}(\Pi)$.

Theorem 3.4. *Let $K \subseteq \overline{\mathbb{Q}}$ be a number field; Z a hyperbolic curve of genus* 0 *over K;*

$$G \subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})\ (\subseteq \mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}}))$$

a closed subgroup such that G contains an open subgroup of G_K, where we regard G_K as a subgroup of $\mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}})$ *via the natural outer action of G_K on* $\Pi_{Z_{\overline{\mathbb{Q}}}}$ *[cf. [8], Theorem C]. Then G is strongly indecomposable. In particular, the Grothendieck-Teichmüller group* GT *is strongly indecomposable [cf. Remark 3.1.1].*

Proof. First, since every open subgroup of G contains an open subgroup of G_K, it suffices to prove that G is indecomposable. Next, by replacing K by a finite extension of K, we may assume without loss of generality that $G_K \subseteq G$, and all cusps of Z are K-rational. Moreover, we may assume without loss of generality that Z is an open subscheme of $\mathbb{P}^1_K \setminus \{0, 1, \infty\}$ obtained by forming the complement of a finite subset of K-rational points of $\mathbb{P}^1_K \setminus \{0, 1, \infty\}$.

Suppose that there exist normal closed subgroups $G_1 \subseteq G$ and $G_2 \subseteq G$ such that

$$G = G_1 \times G_2.$$

We shall write,

- for each $i = 1, 2$, $\mathrm{pr}_i : G \twoheadrightarrow G_i$ for the natural projection;
- for each $n \in \mathbb{Z}_{\geq 1}$, $(\mathbb{P}^1_{\overline{\mathbb{Q}}} \supseteq)\ {}^nY_{\overline{\mathbb{Q}}} \to Z_{\overline{\mathbb{Q}}}\ (\subseteq \mathbb{P}^1_{\overline{\mathbb{Q}}})$ for the finite étale Galois covering of $Z_{\overline{\mathbb{Q}}}$ of degree n determined by $t \mapsto t^n$;
- for each $l \in \mathfrak{Primes}$, $Q_{n,l} \overset{\mathrm{def}}{=} \Pi_{Z_{\overline{\mathbb{Q}}}}/\mathrm{Ker}(\Pi_{{}^nY_{\overline{\mathbb{Q}}}} \to \Pi^l_{{}^nY_{\overline{\mathbb{Q}}}})$;
- $\rho_{n,l} : \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \to \mathrm{Out}^{|\mathrm{C}|}(Q_{n,l})$ for the natural homomorphism [cf. the second bullet in the proof of Lemma 2.2]; $\rho_l \overset{\mathrm{def}}{=} \rho_{1,l}$.

Note that ${}^1Y_{\overline{\mathbb{Q}}} = Z_{\overline{\mathbb{Q}}}$, and $Q_{1,l} = \Pi^l_{Z_{\overline{\mathbb{Q}}}}$.

Next, by applying Lemma 3.2, we have the following assertion:

> Claim 3.4.A: Let $l \in \mathfrak{Primes}$ be an element. Then $\rho_l(G_1) = \{1\}$ or $\rho_l(G_2) = \{1\}$.

Next, we verify the following assertion:

> Claim 3.4.B: Let $n \in \mathbb{Z}_{\geq 1}$ be an element; $l \in \mathfrak{Primes}$ such that $\rho_l(G_1) = \{1\}$. Then $\rho_{n,l}(G_1) = \{1\}$.

Indeed, let $H \subseteq G$, $H_1 \subseteq G_1$, and $H_2 \subseteq G_2$ be normal open subgroups such that

- $H = H_1 \times H_2$;
- there exists an injection $H \hookrightarrow \mathrm{Out}^{|\mathrm{C}|}(\Pi_{{}^nY_{\overline{\mathbb{Q}}}})$;

- there exists an injection $\Pi_{{}^nY_{\overline{\mathbb{Q}}}} \overset{\mathrm{out}}{\rtimes} H \hookrightarrow \Pi_{Z_{\overline{\mathbb{Q}}}} \overset{\mathrm{out}}{\rtimes} G$ that is compatible with the inclusions between respective subgroups $\Pi_{{}^nY_{\overline{\mathbb{Q}}}} \subseteq \Pi_{Z_{\overline{\mathbb{Q}}}}$ and quotients $H \subseteq G$.

[Note that the existence of such normal open subgroups $H \subseteq G$, $H_1 \subseteq G_1$, and $H_2 \subseteq G_2$ follows from a similar argument to the argument applied in the proof of [22], Lemma 1.2.] Then it follows immediately from Lemma 3.2, together with [15], Proposition 1.4, that $\rho_{n,l}(H_1) = \{1\}$ or $\rho_{n,l}(H_2) = \{1\}$. Suppose that $\rho_{n,l}(H_2) = \{1\}$. Here, we note that since $Q^l_{n,l} \overset{\sim}{\to} \Pi^l_{Z_{\overline{\mathbb{Q}}}}$, it holds that ρ_l factors as the composite of $\rho_{n,l}$ with the natural homomorphism $\mathrm{Out}^{|\mathrm{C}|}(Q_{n,l}) \to \mathrm{Out}^{|\mathrm{C}|}(\Pi^l_{Z_{\overline{\mathbb{Q}}}})$. In particular, $\rho_l(H_2) = \{1\}$. Then our assumption that $\rho_l(G_1) = \{1\}$ implies that $\rho_l(G_1 \times H_2) = \{1\}$, hence that $\rho_l(G_K) \subseteq \rho_l(G)$ is finite. This is a contradiction [cf. [10], Lemma 4.2, (iv)]. Thus, we conclude that $\rho_{n,l}(H_1) = \{1\}$, hence that $\rho_{n,l}(G_1)$ is finite. In particular, there exists a finite extension L $(\subseteq \overline{\mathbb{Q}})$ of K such that $\rho_{n,l}(G_1) \subseteq Z_{\mathrm{Out}^{|\mathrm{C}|}(Q_{n,l})}(\rho_{n,l}(G_L))$. Finally, it follows immediately from Lemma 2.2 that $\rho_{n,l}(G_1) = \{1\}$. This completes the proof of Claim 3.4.B.

Write $\chi : \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \to \widehat{\mathbb{Z}}^\times$ for the cyclotomic character [which is obtained by considering the actions on the cuspidal inertia subgroups of $\Pi_{Z_{\overline{\mathbb{Q}}}}$]. Then it follows immediately from Claims 3.4.A, 3.4.B, that $\chi(G_1) = \{1\}$ or $\chi(G_2) = \{1\}$. In particular, we may assume without loss of generality that

$$\chi(G_1) = \{1\}.$$

For each $p \in \mathfrak{Primes}$, write

$$\rho^{(p)'} : \mathrm{Out}(\Pi_{Z_{\overline{\mathbb{Q}}}}) \to \mathrm{Out}(\Pi^{(p)'}_{Z_{\overline{\mathbb{Q}}}})$$

for the natural homomorphism.

Next, we verify the following assertion:

> Claim 3.4.C: There exists a finite subset $S \subseteq \mathfrak{Primes}$ such that, for each $p \in \mathfrak{Primes} \setminus S$, it holds that $\rho^{(p)'}(G_1) = \{1\}$.

Indeed, let $\mathfrak{p}$ be a maximal ideal of the ring of integers of K such that Z has good reduction at $\mathfrak{p}$; $F \in G_K \subseteq G$ a lifting of the Frobenius element at $\mathfrak{p}$. Write $p \in \mathfrak{Primes}$ for the characteristic of the residue field at $\mathfrak{p}$; $I \subseteq G_K$ for the closed subgroup topologically generated by F; $I_1 \overset{\mathrm{def}}{=} \mathrm{pr}_1(I) \times \{1\}$; $I_2 \overset{\mathrm{def}}{=} \{1\} \times \mathrm{pr}_2(I)$. Then since I is abelian, it holds that

$$I \subseteq I_1 \times I_2 \subseteq Z_G(I).$$

Then it follows immediately from Lemma 2.3, (ii), together with the theory of specialization isomorphism, that our assumption that $\chi(I_1) \subseteq \chi(G_1) = \{1\}$ implies that $\rho^{(p)'}(I_1) = \{1\}$. In particular, $\rho^{(p)'}(I) \subseteq \rho^{(p)'}(I_2)$. Thus, since $\chi(G_1) = \{1\}$, and $G_1 \subseteq Z_G(I_2)$, we conclude from Lemma 2.3, (ii), that

$\rho^{(p)'}(G_1) = \{1\}$. Observe that there exists a finite subset $S \subseteq \mathfrak{Primes}$ such that Z has good reduction at any maximal ideal of the ring of integers of K that lies over a prime number $\in \mathfrak{Primes} \setminus S$. Thus, we obtain the desired conclusion. This completes the proof of Claim 3.4.C.

Finally, by applying Claim 3.4.C and Lemma 1.4, we conclude that $G_1 = \{1\}$, hence that G is indecomposable. This completes the proof of Theorem 3.4. $\square$

Remark 3.4.1. Let $\iota \in G_{\mathbb{Q}} \subseteq \mathrm{GT}$ be a complex conjugation; $H \subseteq \mathrm{GT}$ a closed subgroup such that H contains a GT-conjugate of ι. Then

H is *indecomposable*.

Indeed, suppose that there exist normal closed subgroups $H_1 \subseteq H$ and $H_2 \subseteq H$ such that

$$H = H_1 \times H_2.$$

By replacing H by a suitable GT-conjugate of H, we may assume without loss of generality that $\iota \in H$. Then there exist 2-torsion elements $\iota_1 \in H_1 \subseteq H$ and $\iota_2 \in H_2 \subseteq H$ such that $\iota = \iota_1 \cdot \iota_2$. Note that ι_1 and ι_2 commute with ι. Recall that

$$\langle \iota \rangle = N_{\mathrm{GT}}(\langle \iota \rangle),$$

where $\langle \iota \rangle$ denotes the closed subgroup generated by ι [cf. [9], Proposition 4, (ii)]. Thus, since $\iota \neq 1$, we conclude that $\iota_1 = \iota$ or $\iota_2 = \iota$. In the case where $\iota_1 = \iota$ (respectively, $\iota_2 = \iota$), since ι_1 (respectively, ι_2) commutes with H_2 (respectively, H_1), and $\langle \iota \rangle = N_{\mathrm{GT}}(\langle \iota \rangle)$, it holds that $H_2 = \{1\}$ (respectively, $H_1 = \{1\}$).

Remark 3.4.2. Let l be a prime number. In light of Lemma 2.3, (ii), it follows from a similar argument to the argument applied in the proof of [10], Theorem 6.1, that the pro-l analogue of Theorem 3.4 also holds. Thus, it is natural to pose the following question:

> Question: More generally, for each nonempty subset of prime numbers $\Sigma \subseteq \mathfrak{Primes}$, does the pro-$\Sigma$ analogue of Theorem 3.4 hold?

However, at the time of writing the present paper, the authors do not know whether the answer to this question is affirmative or not.

Remark 3.4.3. In our previous work [cf. [12]], we introduced the notion of the *strong internal indecomposability* of profinite groups. We shall say that a profinite group G is strongly internally indecomposable if, for every open subgroup $U \subseteq G$ and every nontrivial normal closed subgroup $J \subseteq U$, the centralizer of J in U is trivial [cf. [12], Definition 1.1, (vi); [12], Proposition 1.2]. Note that strongly internally indecomposable profinite groups are slim [cf. [12], Remark 1.1.1] and strongly indecomposable [cf. [12], Remark 1.1.2, (ii)]. Here, observe that since $\mathbb{Q}$ is Hilbertian [cf. [4], Proposition 13.4.1], $G_{\mathbb{Q}}$ is strongly internally indecomposable [cf. [12], Theorem A, (ii)]. Thus, it is natural to pose the following question:

Question: Is the Grothendieck-Teichmüller group GT strongly internally indecomposable?

However, at the time of writing the present paper, the authors do not know whether the answer to this question is affirmative or not.

Corollary 3.5. *In the notation of Theorem 3.4,* $\Pi_{Z_{\overline{\mathbb{Q}}}} \overset{\text{out}}{\rtimes} G$ *is strongly indecomposable.*

Proof. First, since $\Pi_{Z_{\overline{\mathbb{Q}}}}$ is center-free [cf. [15], Proposition 1.4], we have an exact sequence of profinite groups

$$1 \longrightarrow \Pi_{Z_{\overline{\mathbb{Q}}}} \longrightarrow \Pi_{Z_{\overline{\mathbb{Q}}}} \overset{\text{out}}{\rtimes} G \longrightarrow G \longrightarrow 1.$$

Next, since G contains an open subgroup of G_K, it follows immediately from the Grothendieck Conjecture for hyperbolic curves over number fields [cf. [13], Theorem A; [21], Theorem 0.4] that G ($\subseteq \mathrm{Out}^{|\mathrm{C}|}(\Pi_{Z_{\overline{\mathbb{Q}}}})$) is slim. Thus, since G is infinite, we conclude from Theorem 3.4, together with [10], Proposition 1.8, (i); [15], Proposition 1.4; [15], Proposition 3.2, that $\Pi_{Z_{\overline{\mathbb{Q}}}} \overset{\text{out}}{\rtimes} G$ is strongly indecomposable. This completes the proof of Corollary 3.5. $\square$

Acknowledgements

The authors would like to express deep gratitude to Professor Ivan Fesenko for stimulating discussions on this topic. Part of this work was done during their stay in University of Nottingham. The authors would like to thank their supports and hospitalities. The first author was supported by JSPS KAKENHI Grant Number 20K14285, and the second author was supported by JSPS KAKENHI Grant Number 18J10260. This research was also supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. This research was partially supported by EPSRC programme grant "Symmetries and Correspondences" EP/M024830.

References

[1] Y. André, Period mappings and differential equations: From $\mathbb{C}$ to $\mathbb{C}_p$, *MSJ Memoirs* **12**, *Math. Soc. of Japan, Tokyo* (2003).

[2] Y. André, On a geometric description of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and a p-adic avatar of $\widehat{GT}$, *Duke Math. J.* **119** (2003), pp. 1–39.

[3] V. G. Drinfeld, On quasitriangular quasi-Hopf algebras and a group closely connected with Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), *Algebra i Analiz* **2** (1990), pp. 149–181.

[4] M. Fried and M. Jarden, *Field arithmetic (Second edition)*, *Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, A Series of Modern Surveys in Mathematics* **11**, Springer-Verlag (2005).

[5] A. Grothendieck, Sketch of a programme, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, London Math. Soc. Lect. Note Ser. **242**, Cambridge Univ. Press (1997), pp. 245–283.

[6] D. Harbater and L. Schneps, Fundamental groups of moduli and the Grothendieck-Teichmüller group, *Trans. Amer. Math. Soc.* **352** (2000), pp. 3117–3148.

[7] Y. Hoshi, A. Minamide, and S. Mochizuki, *Group-theoreticity of numerical invariants and distinguished subgroups of configuration space groups*, RIMS Preprint **1870** (March 2017), available at the following URL
`http://www.kurims.kyoto-u.ac.jp/~motizuki/`

[8] Y. Hoshi and S. Mochizuki, On the combinatorial anabelian geometry of nodally nondegenerate outer representations, *Hiroshima Math. J.* **41** (2011), pp. 275–342.

[9] P. Lochak and L. Schneps, A cohomological interpretation of the Grothendieck-Teichmüller group, *Invent. Math.* **127** (1997), pp. 571–600.

[10] A. Minamide, Indecomposability of various profinite groups arising from hyperbolic curves, *Okayama Math. J.* **60** (2018), pp.175–208.

[11] A. Minamide and S. Tsujimura, Anabelian group-theoretic properties of the absolute Galois groups of discrete valuation fields, *J. Number Theory* (2022), available at the following URL
`https://doi.org/10.1016/j.jnt.2021.12.006`

[12] A. Minamide and S. Tsujimura, *Internal indecomposability of profinite groups*, preprint (February 2022), available at the following URL
`http://www.kurims.kyoto-u.ac.jp/~stsuji/`

[13] S. Mochizuki, The local pro-p anabelian geometry of curves, *Invent. Math.* **138** (1999), pp. 319–423.

[14] S. Mochizuki, Topics in absolute anabelian geometry I: Generalities, *J. Math. Sci. Univ. Tokyo* **19** (2012), pp. 139–242.

[15] S. Mochizuki and A. Tamagawa, The algebraic and anabelian geometry of configuration spaces, *Hokkaido Math. J.* **37** (2008), pp. 75–131.

[16] H. Nakamura, Galois rigidity of pure sphere braid groups and profinite calculus, *J. Math. Sci. Univ. Tokyo* **1** (1994), no. 1, pp. 71–136.

[17] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften* **323**, Springer-Verlag (2000).

[18] L. Ribes and P. Zaleskii, *Profinite groups*, *Ergebnisse der Mathematik und ihrer Grenzgebiete* **3**, Springer-Verlag (2000).

[19] M. Saidi and A. Tamagawa, A prime-to-p version of Grothendieck's anabelian conjecture for hyperbolic curves over finite fields of characteristic $p > 0$, *Publ. Res. Inst. Math. Sci.* **45** (2009), pp. 135–186.

[20] L. Schneps, The Grothendieck-Teichmüller group $\widehat{GT}$: a survey, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, *London Math. Soc. Lect. Note Ser.* **242**, Cambridge Univ. Press (1997), pp. 183–203.

[21] A. Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), pp. 135–194.

[22] S. Tsujimura, Combinatorial Belyi cuspidalization and arithmetic subquotients of the Grothendieck-Teichmüller group, *Publ. Res. Inst. Math. Sci.* **56** (2020), pp. 779–829.

(Arata Minamide) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan

Email address: minamide@kurims.kyoto-u.ac.jp

(Shota Tsujimura) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan

Email address: stsuji@kurims.kyoto-u.ac.jp