HIROSHIMA MATH. J., **53** (2023), 63–85
doi:10.32917/h2021057

Belyi injectivity for outer representations on certain quotients of étale fundamental groups of hyperbolic curves of genus zero

Hiroyuki WATANABE

(Received November 30, 2021)
(Revised June 13, 2022)

ABSTRACT. In the present paper, we study certain quotients of the étale fundamental group of a hyperbolic curve over a field. We prove that the action of the outer automorphism group of a certain quotient of the étale fundamental group of a hyperbolic curve over an algebraically closed field on its conjugacy classes of open subgroups is faithful. Also, we prove that, if k is either a number field or a p-adic local field, then the outer Galois representation associated to a certain quotient of the geometric fundamental group of $\mathbb{P}_k^1 \setminus \{0, 1, \infty\}$ is injective.

CONTENTS

1. Introduction

Anabelian geometry is an area of arithmetic geometry in which one studies how much information about a variety is contained in its étale fundamental group or, equivalently, in the category of finite étale coverings of the variety.

In the present paper, we study *certain quotients* of the étale fundamental group of a hyperbolic curve over a field. This amounts to studying certain types of *full sub-Galois categories* of the Galois category of finite étale coverings of such a curve.

The full sub-Galois categories we will treat have less information than the original Galois category, but satisfy some properties which hold for the original Galois category.

2020 *Mathematics Subject Classification*. 14H30.
Key words and phrases. hyperbolic curve, outer Galois representation, Belyi injectivity.

If k is a field with algebraic closure $\bar{k}$ and X a geometrically connected scheme of finite type over k, then there is a natural exact sequence of étale fundamental groups:

$$1 \to \pi_1(X_{\bar{k}}) \to \pi_1(X) \to \pi_1(\mathrm{Spec}\, k) \to 1.$$

Note that $\pi_1(\mathrm{Spec}\, k)$ is naturally isomorphic, up to inner automorphism, to the absolute Galois group G_k of k. Thus, this exact sequence induces a group homomorphism [cf. §2]

$$\rho : G_k \to \mathrm{Out}(\pi_1(X_{\bar{k}})).$$

Belyi proved in [Bel], Corollary to Theorem 4 [cf. also [Bel], the discussion preceding Theorem 1], that, if k is a number field and $X = \mathbb{P}^1_k \backslash \{0, 1, \infty\}$, then ρ is *injective*. This injectivity plays an important role in various aspects of anabelian geometry and the study of the Grothendieck-Teichmüller group.

Belyi proved the injectivity of ρ by showing that the composite

$$G_k \to \mathrm{Out}(\pi_1(X_{\bar{k}})) \to \mathrm{Sym}(\mathfrak{Op}(\pi_1(X_{\bar{k}})))$$

[cf. the explanation of notation given below] is injective. This approach to proving the injectivity of ρ motivated Theorems A and B of the present paper.

Next, we introduce some notation.

A *full formation* [cf. Definition 3.1] is a set of isomorphism classes of finite groups which contains a class distinct from the class of trivial groups, and which is closed under the operations of passing to subgroups, quotients, and extensions.

Let Δ be a profinite group and $\mathcal{C}$ a full formation. For a closed normal subgroup $N \trianglelefteq \Delta$, we construct another closed normal subgroup $N_{\mathcal{C},\Delta} \trianglelefteq \Delta$ [cf. Definition 3.2] as follows:

$$N_{\mathcal{C},\Delta} := \bigcap_{N \subset V \underset{\text{open}}{\leq} \Delta} \ \bigcap_{\substack{U \underset{\text{open}}{\trianglelefteq} V \\ [V/U] \in \mathcal{C}}} U,$$

where $[V/U]$ denotes the isomorphism class of V/U [cf. Definition 3.1]. We shall write $\Sigma_{\mathcal{C}}$ [cf. Definition 3.1] for the set of prime numbers ℓ such that $[\mathbb{Z}/\ell\mathbb{Z}] \in \mathcal{C}$.

Let G be a profinite group. We shall write $\mathfrak{Op}(G)$ [cf. Definition 3.6] for the set of conjugacy classes of open subgroups of G. Then $\mathrm{Aut}(G)$ acts naturally on $\mathfrak{Op}(G)$, and $\mathrm{Inn}(G)$ is contained in the kernel of this action. In particular, we obtain a natural homomorphism

$$\mathrm{Out}(G) \to \mathrm{Sym}(\mathfrak{Op}(G)).$$

Our first main result is the following [cf. Proposition 3.5 and Theorem 3.8].

Theorem A. *Let X be a hyperbolic curve over an algebraically closed field of characteristic $p \geq 0$ with étale fundamental group Δ; $N \trianglelefteq \Delta$ a closed normal subgroup; $\mathcal{C}$ a full formation such that $\Sigma_{\mathcal{C}} \neq \{p\}$. Set $\Delta^* := \Delta/N^{\mathcal{C},\Delta}$. Then Δ^* is slim [cf. §2], and the homomorphism*

$$\mathrm{Out}(\Delta^*) \to \mathrm{Sym}(\mathfrak{Op}(\Delta^*))$$

is injective.

In the present paper, we also prove that the absolute Galois group of $\mathbb{Q}$ can be embedded in the outer automorphism group of certain nontrivial quotient groups of $\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash\{0, 1, \infty\})$.

Let k be a field of characteristic 0 with algebraic closure $\bar{k}$. If N is a closed normal subgroup of $\pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})$ which is also normal in $\pi_1(\mathbb{P}^1_k\backslash\{0, 1, \infty\})$, then we obtain a short exact sequence of profinite groups

$$1 \to \pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})/N \to \pi_1(\mathbb{P}^1_k\backslash\{0, 1, \infty\})/N \to \mathrm{Gal}(\bar{k}/k) \to 1.$$

This exact sequence induces an *outer Galois representation*

$$\rho_{k,N} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})/N).$$

Let N_0 [cf. Definition 4.1] denote the intersection of open subgroups U of $\pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})$ such that the finite étale covering of $\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\}$ corresponding to U is of genus 0.

Our second main result is the following [cf. Proposition 4.7 and Theorem 4.14]. Note that, as $N_0 \neq \{1\}$ [cf. Lemma 4.3], this is a nontrivial result.

Theorem B. *Assume that $N \subset N_0$. Then $\pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})/N_0$ is center-free, and the kernel of the natural outer representation*

$$\rho_{k,N} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{\bar{k}}\backslash\{0, 1, \infty\})/N)$$

is equal to the kernel of the natural restriction homomorphism $\mathrm{Gal}(\bar{k}/k) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\bar{k}$. In particular, if k is either a number field or a p-adic local field for some prime number p, then $\rho_{k,N}$ is injective.*

2. Notations and conventions

Sets: Let S be a set. Then we shall write $|S|$ for the *cardinality* of S. We shall write $\mathrm{Sym}(S)$ for the *group of permutations* of S, i.e., the group of bijections $S \xrightarrow{\sim} S$.

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 set, group, or ring of rational integers. For a prime number ℓ, the notation $\mathbb{Z}_\ell$ will be used to denote the ring of ℓ-adic integers. The notation $\mathbb{Q}_\ell$ will be used to denote the field of ℓ-adic numbers. A finite extension field of $\mathbb{Q}$ (resp. $\mathbb{Q}_\ell$) will be referred to as a number field (resp. an ℓ-adic local field).

Topological groups: Let G be a group and $H \leq G$ a subgroup. Then we shall write $Z_G(H)$ for the *centralizer* of H in G and $Z(G) := Z_G(G)$ for the *center* of G. We shall say that G is *center-free* if G has trivial center, i.e., $Z(G) = \{1\}$.

Let G be a group. Then we shall write $\hat{G}$ for the *profinite completion* of G, i.e., the inverse limit of quotient groups G/H of G, where H is a normal sugbroup of finite index in G.

We shall say that a profinite group G is *slim* if the centralizer $Z_G(U)$ of any open subgroup $U \leq G$ in G is trivial. A profinite group G is slim if and only if every open subgroup of G has trivial center [cf. [Mzk2], Remark 0.1.3].

Let G be a profinite group and U an open subgroup. Then we shall refer to

$$U^{\mathrm{nor}} := \bigcap_{g \in G} g^{-1} U g$$

as the *normal core* of U in G. We shall write G^{ab} for the *abelianization* of G, i.e., the quotient of G by the closure of the commutator subgroup of G. Let p be a prime number. Then we shall write

$$G^{(p)}$$

for the *maximal pro-p quotient* of G, i.e., the quotient of G by the intersection of all open normal subgroups $U \trianglelefteq G$ such that G/U is a p-group;

$$G^{\mathrm{ab},p}$$

for the *maximal abelian pro-p quotient* of G, i.e., the abelianization of $G^{(p)}$, or equivalently, the maximal pro-p quotient of G^{ab};

$$G^{(p\nmid)}$$

for the *maximal pro-prime-to-p quotient* of G, i.e., the quotient of G by the intersection of all open normal subgroups $U \trianglelefteq G$ whose index in G is prime to p.

Let G be a profinite group. Then we shall write $\mathrm{Aut}(G)$ for the group of automorphisms of the *profinite group* G. Conjugation by elements of G determines a homomorphism $G \to \mathrm{Aut}(G)$ whose image $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ is the normal subgroup of $\mathrm{Aut}(G)$ consisting of the *inner automorphisms* of G. We shall write $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ for the *outer automorphism group* of G.

Let

$$1 \to \Delta \to \Pi \to G \to 1$$

be an exact sequence of profinite groups. Then conjugation in Π by liftings of elements of G determines a homomorphism

$$\rho : G \to \mathrm{Out}(\Delta).$$

We shall refer to this homomorphism ρ as the *outer representation* determined by the exact sequence $1 \to \Delta \to \Pi \to G \to 1$.

Schemes: If x is a point of a scheme X, then we shall write $\kappa(x)$ for the *residue field* of x. If X is an integral scheme, then we shall write $K(X)$ for the *function field* of X, i.e., the residue field of the generic point of X.

Let X be a noetherian connected scheme and ξ a geometric point. Then we shall write $\pi_1(X;\xi)$ for the *étale fundamental group* of X relative to the base point ξ. We shall write Π_X for the étale fundamental group of X relative to some choice of base point. If X is geometrically connected and of finite type over a field k, and $\bar{k}$ is an algebraic closure of k that is *fixed* throughout the discussion, then we shall write $\Delta_X := \Pi_{X \times_k \bar{k}}$ for the *geometric fundamental group* of X [relative to $\bar{k}$].

Let k be a field. Then we shall write G_k for the *absolute Galois group* of k relative to some choice of separable closure K of k. Here, we recall that G_k is determined up to inner automorphism by k, i.e., independently of the choice of separable closure of k, and that there is a natural outer isomorphism

$$G_k \xrightarrow{\sim} \Pi_{\operatorname{Spec} k}.$$

Curves: Let k be a field. Then we shall say that X is a *smooth curve* over k if X is a scheme of dimension 1 that is separated, geometrically connected, of finite type, and smooth over k. Recall that if X is a smooth curve over k, then there exist a smooth projective curve X^{cpt} over k and an open immersion $\iota : X \hookrightarrow X^{\mathrm{cpt}}$. Such a pair $(X^{\mathrm{cpt}}, \iota)$ is unique up to unique isomorphism. We shall refer to this X^{cpt} [and ι] as the *compactification* of X. We shall say that a smooth curve X over k is *of type* (g,r) if X^{cpt} is of genus g, and the closed subset $X^{\mathrm{cpt}} \backslash X$ of X^{cpt} equipped with the reduced induced subscheme structure is finite étale of degree r over k. A *hyperbolic curve* over k is a smooth curve over k of type (g,r) such that $2g-2+r>0$. Note that a smooth curve over an algebraically closed field of type (g,r) is hyperbolic if and only if (g,r) is *not* equal to one of the following: $(0,0)$; $(0,1)$; $(0,2)$; $(1,0)$. If X is a smooth curve over k and $U \le \Pi_X$ is an open subgroup, then, we define the *genus* g_U of U to be the genus of the isomorphism class of finite étale coverings of X determined by the conjugacy class of U.

3. Faithfulness of the action on conjugacy classes of open subgroups

In this section, we prove Theorem A.

DEFINITION 3.1. Let $\mathcal{G}$ denote the *set of isomorphism classes of finite groups.* [Here, we observe that $\mathcal{G}$ is indeed a set.] For a finite group G, we shall write $[G]$ for the isomorphism class to which G belongs. A subset $\mathcal{C}$ of $\mathcal{G}$ is called a *formation* if it contains the class of trivial groups [i.e., groups with only one element]. A formation $\mathcal{C}$ is said to be *nontrivial* if it contains some class different from the class of trivial groups. A nontrivial formation $\mathcal{C}$ is said to be a *full formation* if it is closed under the operations of passing to subgroups, quotients, and extensions. Let $\mathcal{C}$ be a formation. Then we shall write $\Sigma_{\mathcal{C}}$ for the set of prime numbers ℓ such that $[\mathbb{Z}/\ell\mathbb{Z}] \in \mathcal{C}$. Note that if $\mathcal{C}$ is a full formation, then $\Sigma_{\mathcal{C}}$ is nonempty, and $\ell \in \Sigma_{\mathcal{C}}$ if and only if $\mathcal{C}$ contains all isomorphism classes of finite ℓ-groups.

DEFINITION 3.2. Let Δ be a profinite group and $\mathcal{C}$ a formation. If $N \trianglelefteq \Delta$ is a closed normal subgroup, then we define:

$$N_{\mathcal{C},\Delta} := \bigcap_{N \subset V \underset{\text{open}}{\leq} \Delta} \ \bigcap_{\substack{U \underset{\text{open}}{\trianglelefteq} V \\ [V/U] \in \mathcal{C}}} U.$$

Note that $N_{\mathcal{C},\Delta}$ is a closed normal subgroup of Δ contained in N.

REMARK 3.3. Note that $N_{\mathcal{C},\Delta} \subset N$. Indeed,

$$N_{\mathcal{C},\Delta} = \bigcap_{N \subset V \underset{\text{open}}{\leq} \Delta} \ \bigcap_{\substack{U \underset{\text{open}}{\trianglelefteq} V \\ [V/U] \in \mathcal{C}}} U \subset \bigcap_{N \subset V \underset{\text{open}}{\leq} \Delta} V = N.$$

Furthermore, $N_{\mathcal{C},\Delta}$ coincides with the kernel $K_{N,\mathcal{C}}$ of the natural map from N to its *maximal pro-$\mathcal{C}$ quotient*. Indeed, N is a closed subgroup of the profinite group Δ, hence is itself a profinite group, so it makes sense to consider the maximal pro-$\mathcal{C}$ quotient of N. By definition,

$$K_{N,\mathcal{C}} = \bigcap_{\substack{H \underset{\text{open}}{\trianglelefteq} N \\ [N/H] \in \mathcal{C}}} H.$$

If V and U are open subgroups of Δ satisfying $N \subset V \leq \Delta$, $U \trianglelefteq V$, and $[V/U] \in \mathcal{C}$, then $U \cap N$ is an open normal subgroup of N, and there exists a natural injective homomorphism

$$N/U \cap N \hookrightarrow V/U.$$

Since $\mathcal{C}$ is a full formation, it follows that $[N/U \cap N] \in \mathcal{C}$. Hence

$$N_{\mathcal{C},\Delta} = N_{\mathcal{C},\Delta} \cap N = \bigcap_{N \subset V \underset{\text{open}}{\leq} \Delta} \ \bigcap_{\substack{U \underset{\text{open}}{\trianglelefteq} V \\ [V/U] \in \mathcal{C}}} (U \cap N) \supset K_{N,\mathcal{C}}.$$

Conversely, let $H \leq N$ be an open normal subgroup such that $[N/H] \in \mathcal{C}$. Then H is a closed subgroup of Δ, and thus

$$H = \bigcap_{H \subset W \underset{\text{open}}{\leq} \Delta} W.$$

If W satisfies the condition that $H \subset W \underset{\text{open}}{\leq} \Delta$, then

$$H \subset \bigcap_{n \in N} n^{-1} W n \trianglelefteq N \cdot \bigcap_{n \in N} n^{-1} W n,$$

and $\bigcap_{n \in N} n^{-1} W n$ is an *open* subgroup of Δ. [Indeed, since W is an *open* subgroup of Δ, it follows immediately that there are only finitely many conjugates of W in Δ.] Therefore, by replacing W by $\bigcap_{n \in N} n^{-1} W n$, we conclude that

$$H = \bigcap_{\substack{H \subset W \underset{\text{open}}{\leq} \Delta \\ W \trianglelefteq N \cdot W}} W.$$

Now let W be an open subgroup of Δ such that $H \subset W$ and $W \trianglelefteq N \cdot W$. Then $N \cdot W$ is an open subgroup of Δ containing N, and there exist natural homomorphisms

$$N/H \twoheadrightarrow N/N \cap W \xrightarrow{\sim} N \cdot W/W,$$

where the first arrow is a surjection, and the second one is an isomorphism. [Note that $N \cap W \trianglelefteq N$.] Since $\mathcal{C}$ is a full formation, it follows that $[N \cdot W/W] \in \mathcal{C}$. Therefore

$$K_{N,\mathcal{C}} = \bigcap_{\substack{H \underset{\text{open}}{\trianglelefteq} N \\ [N/H] \in \mathcal{C}}} \ \bigcap_{\substack{H \subset W \underset{\text{open}}{\leq} \Delta \\ W \trianglelefteq N \cdot W}} W \supset N_{\mathcal{C},\Delta}.$$

Hence $N_{\mathcal{C},\Delta} = K_{N,\mathcal{C}}$. In particular, $N_{\mathcal{C},\Delta}$ is in fact *independent* of the group Δ containing N.

Proposition 3.4. *Let X be a hyperbolic curve over an algebraically closed field k of characteristic $p \geq 0$ with étale fundamental group Π_X; $U \trianglelefteq \Pi_X$ an open normal subgroup; $\ell \neq p$ a prime number. Then the natural action of Π_X/U on $U^{\mathrm{ab},\ell}$ induced by conjugation is faithful.*

PROOF. Write $Y \to X$ for the finite Galois covering corresponding to $U \trianglelefteq \Pi_X$ [so Y is also a hyperbolic curve over k]. Then Π_X/U may be naturally identified with $\mathrm{Aut}(Y/X)$, and $U^{\mathrm{ab},\ell}$ with $\Pi_Y^{\mathrm{ab},\ell}$. Under these identifications, the natural action $\Pi_X/U \curvearrowright U^{\mathrm{ab},\ell}$ coincides with the natural action

$$\mathrm{Aut}(Y/X) \curvearrowright \Pi_Y^{\mathrm{ab},\ell}.$$

[Note that the choice of a base point for Y is not a matter of concern since we are only interested in the present discussion in abelianizations.]

Suppose that $\mathrm{id}_Y \neq \sigma \in \mathrm{Aut}(Y/X)$ acts trivially on $\Pi_Y^{\mathrm{ab},\ell}$. Write $\tilde{\sigma}$ for the extension of σ to Y^{cpt}.

Case 1: $g_Y \geq 2$. The existence of the natural surjection

$$\Pi_Y^{\mathrm{ab},\ell} \twoheadrightarrow \Pi_{Y^{\mathrm{cpt}}}^{\mathrm{ab},\ell}$$

and natural isomorphisms

$$\mathrm{Hom}_{\mathrm{cont}}(\Pi_{Y^{\mathrm{cpt}}}^{\mathrm{ab},\ell}, \mathbb{Z}_\ell(1)) \cong H^1_{\text{ét}}(Y^{\mathrm{cpt}}, \mathbb{Z}_\ell(1)) \cong T_\ell(\mathbf{Pic}^0(Y^{\mathrm{cpt}}))$$

implies that the natural action of $\tilde{\sigma}$ on $T_\ell(\mathbf{Pic}^0(Y^{\mathrm{cpt}}))$ is trivial. Here, "$\mathrm{Hom}_{\mathrm{cont}}$" denotes the group of continuous homomorphisms of topological groups, "$\mathbf{Pic}^0$" denotes the Picard group of invertible sheaves of degree 0, and "T_ℓ" denotes the ℓ-adic Tate module of an abelian group. Thus, by the Lefschetz-Weil fixed point formula, the number n of fixed points of $\tilde{\sigma}$, counted with their multiplicities, is

$$n = 1 - \mathrm{Tr}(\tilde{\sigma} \mid T_\ell(\mathbf{Pic}^0(Y^{\mathrm{cpt}}))) + 1 = 2 - 2g_Y < 0,$$

which is a contradiction. [This argument is based on the argument of [DM], Lemma 1.14.]

Case 2: $g_Y = 0$. We may assume without loss of generality that $Y^{\mathrm{cpt}} = \mathbb{P}^1_k$. Note that since Y is hyperbolic, it is an affine curve, and $Y^{\mathrm{cpt}} \setminus Y$ consists of three or more points. We claim that $\tilde{\sigma}$ fixes each point of $Y^{\mathrm{cpt}} \setminus Y$. By [MT], Proposition 5.2 (v), there exists a natural exact sequence

$$\begin{aligned} 0 &\to \mathrm{Hom}_{\mathrm{cont}}(\Pi_{Y^{\mathrm{cpt}}}, \mathbb{Q}_\ell(1)) \to \mathrm{Hom}_{\mathrm{cont}}(\Pi_Y, \mathbb{Q}_\ell(1)) \\ &\to \bigoplus_{P \in Y^{\mathrm{cpt}} \setminus Y} \mathbb{Q}_\ell \to H^2_{\text{ét}}(Y^{\mathrm{cpt}}, \mathbb{Q}_\ell(1)) \to H^2_{\text{ét}}(Y, \mathbb{Q}_\ell(1)). \end{aligned}$$

In our case, we can rewrite this sequence as follows:

$$\begin{aligned} 0 &\to \mathrm{Hom}_{\mathrm{cont}}(\Pi_{Y^{\mathrm{cpt}}}^{\mathrm{ab},\ell}, \mathbb{Q}_\ell(1)) \to \mathrm{Hom}_{\mathrm{cont}}(\Pi_Y^{\mathrm{ab},\ell}, \mathbb{Q}_\ell(1)) \\ &\xrightarrow{\varphi} \bigoplus_{P \in Y^{\mathrm{cpt}} \setminus Y} \mathbb{Q}_\ell e_P \xrightarrow{\psi} \mathbb{Q}_\ell \to 0, \end{aligned}$$

where e_P is the $1 \in \mathbb{Q}_\ell$ in the direct summand corresponding to $P \in Y^{\mathrm{cpt}} \setminus Y$, and ψ is the *codiagonal* morphism, i.e., the homomorphism that sends each e_P to $1 \in \mathbb{Q}_\ell$. Then $\tilde{\sigma}$ acts naturally on $\bigoplus_{P \in Y^{\mathrm{cpt}} \setminus Y} \mathbb{Q}_\ell e_P$ by permutation of the e_P. Write $\tilde{\sigma}^*$ for the automorphism of $\bigoplus_{P \in Y^{\mathrm{cpt}} \setminus Y} \mathbb{Q}_\ell e_P$ induced by $\tilde{\sigma}$. Then, for each $P \in Y^{\mathrm{cpt}} \setminus Y$,

$$\tilde{\sigma}^*(e_{\tilde{\sigma}(P)} - e_P) = e_P - e_{\tilde{\sigma}^{-1}(P)}.$$

However, since $e_{\sigma(P)} - e_P \in \ker \psi = \operatorname{im} \varphi$ and $\tilde{\sigma}$ acts trivially on $\Pi_Y^{\mathrm{ab},\ell}$, hence also trivially on $\operatorname{im} \varphi$, we have

$$e_P - e_{\tilde{\sigma}^{-1}(P)} = \tilde{\sigma}^*(e_{\tilde{\sigma}(P)} - e_P) = e_{\tilde{\sigma}(P)} - e_P.$$

This implies that $P = \tilde{\sigma}(P)$. Hence $\tilde{\sigma}$ fixes each point of $Y^{\mathrm{cpt}} \setminus Y$, so $\tilde{\sigma}$ is an automorphism of $\mathbb{P}_k^1$ which has three or more fixed points. Thus $\tilde{\sigma} = \mathrm{id}_{\mathbb{P}_k^1}$, which is a contradiction.

Case 3: $g_Y = 1$. Note that since Y is hyperbolic, it is an affine curve. By a similar argument to the argument given in Case 1, the number n of fixed points of $\tilde{\sigma}$, counted with their multiplicities, is

$$n = 2 - 2g_Y = 0.$$

Therefore $\tilde{\sigma}$ has no fixed point. However, by a similar argument to the argument given in Case 2, $\tilde{\sigma}$ fixes each point of $Y^{\mathrm{cpt}} \setminus Y \neq \emptyset$. This is a contradiction. □

Proposition 3.5. *Let X be a hyperbolic curve over an algebraically closed field k of characteristic $p \geq 0$ with étale fundamental group Δ; $N \trianglelefteq \Delta$ a closed normal subgroup; $\mathcal{C}$ a full formation such that $\Sigma_{\mathcal{C}} \neq \{p\}$. Then $\Delta / N_{\mathcal{C},\Delta}$ is slim.*

Proof. Fix a prime number $\ell \in \Sigma_{\mathcal{C}} \setminus \{p\} \neq \emptyset$. Let $U \trianglelefteq \Delta / N_{\mathcal{C},\Delta}$ be an open normal subgroup. Suppose that $Z(U) = Z_U(U)$ contains an element u which is not the identity element. Then there exists an open normal subgroup $V \trianglelefteq \Delta$ such that $u \notin V \trianglelefteq U$. Write $\tilde{U}$ [resp. $\tilde{V}$] for the inverse image of U [resp. V] under the natural quotient map $\Delta \twoheadrightarrow \Delta / N_{\mathcal{C},\Delta}$. Then $\tilde{U}$ is isomorphic to the étale fundamental group of a hyperbolic curve over k. Clearly the natural homomorphism $\tilde{U}/\tilde{V} \to U/V$ is an isomorphism of groups, and since $\mathcal{C}$ is a *full* formation such that $\ell \in \Sigma_{\mathcal{C}}$, the natural homomorphism $\tilde{V}^{\mathrm{ab},\ell} \to V^{\mathrm{ab},\ell}$ is an isomorphism of profinite groups. Therefore, by Proposition 3.4, the natural action $U/V \curvearrowright V^{\mathrm{ab},\ell}$ induced by conjugation is faithful. Since $u \in Z(U)$, $u \bmod V$ acts trivially on $V^{\mathrm{ab},\ell}$. This contradicts the assumption that $u \notin V$. Thus $Z(U) = \{1\}$. Hence $\Delta / N_{\mathcal{C},\Delta}$ is slim, as desired. □

Definition 3.6. Let G be a profinite group. Then we shall write $\mathfrak{Op}(G)$ for the set of conjugacy classes of open subgroups of G.

Observe that $\mathrm{Aut}(G)$ acts naturally on $\mathfrak{Op}(G)$, and $\mathrm{Inn}(G)$ is contained in the kernel of this action. In particular, we obtain a natural homomorphism

$$\mathrm{Out}(G) \to \mathrm{Sym}(\mathfrak{Op}(G)).$$

LEMMA 3.7. *Let G be a profinite group and σ an automorphism of G acting trivially on $\mathfrak{Op}(G)$. Then for every closed subgroup H of G, there exists an element $g \in G$ such that*

$$\sigma(H) = g^{-1}Hg.$$

In other words, σ acts trivially on the set of conjugacy classes of closed subgroups of G.

PROOF. Let $\mathcal{A}$ denote the set of open subgroups of G containing H. Then $\mathcal{A}$ is a directed set with respect to inclusion. For every $U \in \mathcal{A}$, by our assumption, there exists an element $g_U \in G$ such that $\sigma(U) = g_U^{-1}Ug_U$. Thus the map

$$\mathcal{A} \to G$$
$$U \mapsto g_U$$

determines a "net" in G. Since G is compact, there exists a subnet $\mathcal{B} \to G$ converging to some element $g \in G$. Next, fix $V \in \mathcal{B}$. For every $W \in \mathcal{B}$ contained in V,

$$g_W\sigma(H)g_W^{-1} \subset g_W\sigma(W)g_W^{-1} = W \subset V,$$
$$g_W^{-1}Hg_W \subset g_W^{-1}Wg_W = \sigma(W) \subset \sigma(V).$$

Taking the limit, we obtain

$$g\sigma(H)g^{-1} \subset V,$$
$$g^{-1}Hg \subset \sigma(V).$$

Thus

$$\sigma(H) \subset \bigcap_{V \in \mathcal{B}} g^{-1}Vg = g^{-1}Hg,$$
$$g^{-1}Hg \subset \bigcap_{V \in \mathcal{B}} \sigma(V) = \sigma(H),$$

hence $\sigma(H) = g^{-1}Hg$, as desired. □

THEOREM 3.8. *Let X be a hyperbolic curve over an algebraically closed field of characteristic $p \geq 0$ with étale fundamental group Δ; $N \trianglelefteq \Delta$ a closed* *normal subgroup; $\mathcal{C}$ a full formation such that $\Sigma_{\mathcal{C}} \neq \{p\}$. Set $\Delta^* := \Delta/N_{\mathcal{C},\Delta}$. Then the homomorphism*

$$\mathrm{Out}(\Delta^*) \to \mathrm{Sym}(\mathfrak{Op}(\Delta^*))$$

is injective.

Proof. Let σ be an automorphism of Δ^* that acts trivially on $\mathfrak{Op}(\Delta^*)$ and $\ell \in \Sigma_{\mathcal{C}} \setminus \{p\}$. Set

$$\mathcal{A} := \{U \trianglelefteq \Delta^* \mid U \text{ is open}\}.$$

Then $\mathcal{A}$ is a directed set with respect to inclusion.

For each $U \in \mathcal{A}$, σ acts naturally on U and thus on $U^{\mathrm{ab},\ell}$. Let $\bar{\sigma}^U$ denote the automorphism induced by σ on $U^{\mathrm{ab},\ell}$. Note that $U^{\mathrm{ab},\ell}$ is a free $\mathbb{Z}_\ell$-module of rank ≥ 2. Let

$$\varphi_U : \Delta^*/U \to \mathrm{Aut}(U^{\mathrm{ab},\ell}) \;\; (\cong GL_d(\mathbb{Z}_\ell) \text{ for some integer } d \geq 2)$$

be the action induced by conjugation, which, by Proposition 3.4 and a similar argument to the argument applied to prove Proposition 3.5, is *injective*.

Let $\{g_{U,1}, \dots, g_{U,n}\} \subset \Delta^*$ be a complete system of representatives of Δ^*/U, where $n := [\Delta^* : U]$. For $g \in \Delta^*$, write $\bar{g}$ for the image of g in Δ^*/U. Write $\lambda_1^{(i)}, \dots, \lambda_{s_i}^{(i)}$ for the eigenvalues of the automorphism on $U^{\mathrm{ab},\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ induced by $(\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}_{U,i})$; $W_1^{(i)}, \dots, W_{s_i}^{(i)}$ for the corresponding eigenspaces.

Now for every $\mathbb{Z}_\ell$-submodule V of rank 1 of $U^{\mathrm{ab},\ell}$, by Lemma 3.7,

$$\bar{\sigma}^U(V) = \varphi_U(\bar{g}_{U,i_V})(V)$$

for some $i_V \in \{1, \dots, n\}$. This shows that

$$U^{\mathrm{ab},\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \bigcup_{i,j} W_j^{(i)}.$$

Since $\mathbb{Q}_\ell$ is an infinite field, this implies that $U^{\mathrm{ab},\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = W_j^{(i)}$ for some i, j. Since $U^{\mathrm{ab},\ell} \subset U^{\mathrm{ab},\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, we conclude that $(\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}_{U,i})$ is multiplication by $\lambda_j^{(i)}$. In particular, $(\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}_{U,i}) \in \mathrm{Sc}(\mathrm{Aut}(U^{\mathrm{ab},\ell}))$, where we write $\mathrm{Sc}(-)$ for the subgroup given by multiplication by elements of $\mathbb{Z}_\ell^\times$. This shows that, if we denote by f_U the following composite map of sets

$$\Delta^* \twoheadrightarrow \Delta^*/U \xrightarrow{\varphi_U} \mathrm{Aut}(U^{\mathrm{ab},\ell}) \xrightarrow{(\bar{\sigma}^U)^{-1} \circ (-)} \mathrm{Aut}(U^{\mathrm{ab},\ell}),$$

then

$$C_U := f_U^{-1}(\mathrm{Sc}(\mathrm{Aut}(U^{\mathrm{ab},\ell}))) \neq \emptyset.$$

Since f_U is continuous, C_U is closed in Δ^*. Moreover, one verifies easily that if $U_1, U_2 \in \mathcal{A}$ such that $U_1 \subset U_2$, then $C_{U_1} \subset C_{U_2}$. [Indeed, if $g \in C_{U_1}$, then

$$(\bar{\sigma}^{U_1})^{-1} \circ \varphi_{U_1}(gU_1)$$

is multiplication by some $\lambda \in \mathbb{Z}_\ell^\times$. The inclusion $U_1 \subset U_2$ induces a $\mathbb{Z}_\ell$-linear map $U_1^{\mathrm{ab},\ell} \to U_2^{\mathrm{ab},\ell}$, whose image is open. Clearly $(\bar{\sigma}^{U_2})^{-1} \circ \varphi_{U_2}(gU_2)$ acts on the image of this linear map by multiplication by λ. Since any two automorphisms of a finite free $\mathbb{Z}_\ell$-module coincide if and only if they coincide on an open submodule of the module, we thus conclude that $(\bar{\sigma}^{U_2})^{-1} \circ \varphi_{U_2}(gU_2)$ is multiplication by λ, hence that $g \in C_{U_2}$.] Since Δ^* is compact, we thus conclude that $\bigcap_{U \in \mathcal{A}} C_U \neq \emptyset$. Let $g \in \bigcap_{U \in \mathcal{A}} C_U$. Then

$$(\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}) \in \mathrm{Sc}(\mathrm{Aut}(U^{\mathrm{ab},\ell})) \subset Z(\mathrm{Aut}(U^{\mathrm{ab},\ell}))$$

for all $U \in \mathcal{A}$. In particular, for any $h \in \Delta^*$,

$$(\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}) \circ \varphi_U(\bar{h}) = \varphi_U(\bar{h}) \circ (\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}),$$

hence

$$\varphi_U(\overline{gh}) = \varphi_U(\bar{g}) \circ \varphi_U(\bar{h}) = (\bar{\sigma}^U) \circ \varphi_U(\bar{h}) \circ (\bar{\sigma}^U)^{-1} \circ \varphi_U(\bar{g}) = \varphi_U(\overline{\sigma(h)g}).$$

Since φ_U is injective, this implies that $\sigma(h)gh^{-1}g^{-1} \in U$. Since $\bigcap_{U \in \mathcal{A}} U = \{1\}$, we conclude that $\sigma(h)gh^{-1}g^{-1} = 1$, i.e., $\sigma(h) = ghg^{-1}$. Thus σ is an inner automorphism, as desired. □

4. Belyi injectivity for outer representations

In this section, we prove Theorem B.

DEFINITION 4.1. Let k be a field, $\bar{k}$ an algebraic closure of k, and X a smooth geometrically connected curve over k. Write Δ_X for the étale fundamental group of $X_{\bar{k}} := X \times_k \bar{k}$ [relative to some choice of base point]. Let g be a nonnegative integer. Write

$$N_{g,X} := \bigcap_{\substack{U \leq \Delta_X \\ \text{open} \\ g_U = g}} U, \qquad N_{\leq g,X} := \bigcap_{\substack{U \leq \Pi_X \\ \text{open} \\ g_U \leq g}} U.$$

Thus $N_{g,X}$ and $N_{\leq g,X}$ are closed normal subgroups of Π_X, hence also of Δ_X.

REMARK 4.2. Let k be an algebraically closed field of characteristic 0 and K/k a field extension such that K is also an algebraically closed field. Further let X be a smooth connected curve over k. As is well-known [cf., e.g., assertion (a) of the proof of [Mzk1, Proposition 2.3]], base-change from k to K

yields an isomorphism $\Pi_{X_K} \xrightarrow{\sim} \Pi_X$ [for suitable choices of base points]. For each integer $g \geq 0$, this isomorphism clearly maps N_{g,X_K} onto $N_{g,X}$ and $N_{\leq g,X_K}$ onto $N_{\leq g,X}$. In particular, $N_{g,X}$ and $N_{\leq g,X}$ are *independent* of the algebraically closed base field over which one considers X.

Next, recall that we have [for suitable choices of base points] a natural short exact sequence

$$1 \to \Delta_X \to \Pi_X \to G_k \to 1.$$

For a closed normal subgroup N of Δ_X which is also normal in Π_X, we can construct a new short exact sequence:

$$1 \to \Delta_X/N \to \Pi_X/N \to G_k \to 1.$$

Thus we obtain an outer representation

$$\rho_{k,N} : G_k \to \mathrm{Out}(\Delta_X/N).$$

The goal of this section is to show [cf. Theorem 4.14 below] that $\ker \rho_{k,N}$ is equal to the kernel of the natural restriction homomorphism [which is well-defined up to composition with an inner automorphism]

$$G_k \to G_{\mathbb{Q}}$$

if $X = \mathbb{P}^1_k \backslash \{0, 1, \infty\}$ and N is contained in $N_{0,X}$.

To ensure the *nontriviality* of this result, we prove the following.

Lemma 4.3. *Let k be an algebraically closed field of characteristic* 0*, X a smooth curve over k of type $(0,r)$ with $r \geq 3$, and g a nonnegative integer. Then $N_{\leq g} := N_{\leq g,X} \neq \{1\}$.*

To prove Lemma 4.3, we use the following theorem, which, prior to its proof, was known as the Guralnick-Thompson Conjecture [cf. [FM]].

Theorem 4.4. *For each nonnegative integer g, there exists a finite set $\mathcal{E}(g)$ of isomorphism classes of finite simple groups such that if X is a compact Riemann surface of genus g, $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ is a finite branched cover, and S is a nonabelian composition factor of the monodromy group* $\mathrm{Mon}(X, \phi)$ *of (X, ϕ) [cf. Remark* 4.5 *below], then either S is isomorphic to an alternating group, or S belongs to a class of $\mathcal{E}(g)$.*

Remark 4.5. The *monodromy group* of a finite branched cover $q : Y \to X$ of Riemann surfaces with respect to a base point $x \in X$ which is not a branch point of q is the image of the natural homomorphism

$$\pi_1(X; x) \to \mathrm{Sym}(q^{-1}(x)).$$

Since, as is well-known, any finite branched cover of a Riemann surface that arises from an algebraic curve is itself algebrizable, we may restate the above theorem as follows:

> For each nonnegative integer g, there exists a finite set $\mathcal{E}(g)$ of isomorphism classes of finite simple groups such that if X is a smooth curve over $\mathbb{C}$ of genus g, $D \subsetneq \mathbb{P}^1_{\mathbb{C}}$ is a closed subset, $\phi : X \to \mathbb{P}^1_{\mathbb{C}} \backslash D$ is a finite étale morphism with Galois closure $Y \to \mathbb{P}^1_{\mathbb{C}}$, and S is a nonabelian composition factor of $\mathrm{Aut}(Y/\mathbb{P}^1_{\mathbb{C}}) = \Pi_{\mathbb{P}^1_{\mathbb{C}}}/\Pi_Y$, then either S is isomorphic to an alternating group, or S belongs to a class of $\mathcal{E}(g)$.

PROOF (Lemma 4.3). By Remark 4.2, we may assume that $k = \mathbb{C}$. For each integer i, let $\mathcal{E}(i)$ be as in Theorem 4.4, and write

$$\mathcal{E}_{\leq g} := \bigcup_{0 \leq i \leq g} \mathcal{E}(i).$$

Since there are infinitely many simple groups that are neither cyclic nor isomorphic to an alternating group [such as the projective special linear groups $PSL_2(\mathbb{F}_p)$, for $p \geq 5$], there exists a finite simple group G such that G is neither cyclic, alternating, nor isomorphic to a group that determines a class of $\mathcal{E}_{\leq g}$. Since the genus of an open normal subgroup of Π_X can be arbitrarily large [cf. our assumption that $r \geq 3$], there exists an open normal subgroup V of Π_X such that the *rank* of V as a free profinite group is $\geq |G|$. [Note that any open subgroup of Π_X is a free profinite group of finite rank.] Let $V \twoheadrightarrow G$ be a surjection [which exists in light of our assumption on the rank of V as a free profinite group] and write W for the kernel of this surjection.

Now suppose that $N_{\leq g} = \{1\}$. Then $N_{\leq g} \subset W$, and thus it follows from the compactness of $\Pi_X \backslash W$ that there exist open subgroups $U_1, \dots, U_n$ of Π_X such that $g_{U_j} \leq g$ and $\cap_{j \geq 1} U_j \subset W$. Let U_j^{nor} denote the normal core $\cap_{\sigma \in \Pi_X} \sigma^{-1} U_j \sigma$ of U_j. For a finite group G, write $\mathrm{CF}(G)$ for the set of isomorphism classes of composition factors of G. By considering the short exact sequence

$$1 \to U_1^{\mathrm{nor}}/\cap_{j \geq 1} U_j^{\mathrm{nor}} \to \Pi_X/\cap_{j \geq 1} U_j^{\mathrm{nor}} \to \Pi_X/U_1^{\mathrm{nor}} \to 1$$

and applying the Jordan-Hölder theorem, we conclude that

$$\mathrm{CF}(\Pi_X/\cap_{j \geq 1} U_j^{\mathrm{nor}}) = \mathrm{CF}(\Pi_X/U_1^{\mathrm{nor}}) \cup \mathrm{CF}(U_1^{\mathrm{nor}}/\cap_{j \geq 1} U_j^{\mathrm{nor}}).$$

Since

$$U_1^{\mathrm{nor}}/\cap_{j \geq 1} U_j^{\mathrm{nor}} \cong (U_1^{\mathrm{nor}} \cdot \cap_{j \geq 2} U_j^{\mathrm{nor}})/\cap_{j \geq 2} U_j^{\mathrm{nor}}$$

and

$$(U_1^{\mathrm{nor}} \cdot \cap_{j \geq 2} U_j^{\mathrm{nor}}) / \cap_{j \geq 2} U_j^{\mathrm{nor}} \trianglelefteq \Pi_X / \cap_{j \geq 2} U_j^{\mathrm{nor}},$$

we conclude that

$$\mathrm{CF}(U_1^{\mathrm{nor}} / \cap_{j \geq 1} U_j^{\mathrm{nor}}) \subset \mathrm{CF}(\Pi_X / \cap_{j \geq 2} U_j^{\mathrm{nor}})$$

and hence

$$\mathrm{CF}(\Pi_X / \cap_{j \geq 1} U_j^{\mathrm{nor}}) \subset \mathrm{CF}(\Pi_X / U_1^{\mathrm{nor}}) \cup \mathrm{CF}(\Pi_X / \cap_{j \geq 2} U_j^{\mathrm{nor}}).$$

Thus, by applying induction on n, we conclude that

$$\mathrm{CF}(\Pi_X / \cap_{j \geq 1} U_j^{\mathrm{nor}}) \subset \bigcup_{j \geq 1} \mathrm{CF}(\Pi_X / U_j^{\mathrm{nor}}).$$

In particular,

$$\mathrm{CF}(\Pi_X / \cap_{j \geq 1} U_j^{\mathrm{nor}}) \subset \mathcal{C} \cup \mathcal{A} \cup \mathcal{E}_{\leq g},$$

where we write $\mathcal{C}$ for the set of isomorphism classes of finite simple cyclic groups and $\mathcal{A}$ for the set of isomorphism classes of alternating groups. Since $\cap_{j \geq 1} U_j^{\mathrm{nor}} \trianglelefteq W \trianglelefteq V \trianglelefteq \Pi_X$, G appears as a composition factor of $\Pi_X / \cap_{j \geq 1} U_j^{\mathrm{nor}}$. This contradicts the choice of G. Hence $N_{\leq g} \neq \{1\}$. □

REMARK 4.6. In the pro-ℓ case, where ℓ is a prime number, the analogue of Lemma 4.3 is *false* for $g = 0$. Namely,

$$\bigcap_{\substack{U \underset{\mathrm{open}}{\leq} \Pi_X^{(\ell)} \\ g_U = 0}} U = \{1\},$$

where U ranges over the open subgroups of $\Pi_X^{(l)}$ such that the genus g_U of the inverse image of U in Π_X is 0 [cf. [AI, Theorem 1B]]. On the other hand, if ℓ is a prime number distinct from 2, then the analogue of Lemma 4.3 for the pro-prime-to-ℓ case holds, i.e.,

$$\bigcap_{\substack{U \underset{\mathrm{open}}{\leq} \Pi_X^{(\ell \not{})} \\ g_U \leq g}} U \neq \{1\}$$

for every $g \in \mathbb{Z}_{\geq 0}$. Indeed, there are infinitely many isomorphism classes of finite simple groups which are neither cyclic nor alternating groups, and whose order is prime to ℓ. [Indeed, consider, for instance, for $\ell \neq 5$, the Suzuki groups ${}^2B_2(2^{2(\ell-1)i+1})$, $i \in \mathbb{Z}_{\geq 1}$, whose order is

$$2^{4(\ell-1)i+2}(2^{4(\ell-1)i+2} + 1)(2^{2(\ell-1)i+1} - 1);$$

for $\ell = 5$, the Chevalley groups $G_2(5i+2)$, $i \in \mathbb{Z}_{\geq 1}$ such that $5i+2$ is prime [a condition that holds for infinite many i, by Dirichlet's theorem on arithmetic progressions], whose order is

$$(5i+2)^6((5i+2)^6 - 1)((5i+2)^2 - 1).]$$

This proves the assertion, by applying a similar argument to the argument applied in the proof of Lemma 4.3. Note that, as every finite group of odd order is solvable by the Feit-Thompson theorem, this proof does not work for $\ell = 2$.

PROPOSITION 4.7. *Let k be an algebraically closed field of characteristic* 0 *and X a smooth curve over k of type $(0, r)$ with $r \geq 3$. Write $N_0 := N_{0,X}$. Then Π_X/N_0 is center-free.*

PROOF. Let $\gamma \in Z(\Pi_X/N_0)$. Fix an open subgroup U of Π_X of genus 0 and write $Y = \mathbb{P}_k^1 \backslash \{P_1, \dots, P_s\}$ [where $P_1, \dots, P_s$ are distinct k-valued points of $\mathbb{P}_k^1$] for the corresponding smooth curve [so U may be identified with Π_Y]. Then we may naturally identify U^{ab} with the quotient group of the group $\hat{\mathbb{Z}}P_1 + \cdots + \hat{\mathbb{Z}}P_s$ of formal sums over the set $\{P_1, \dots, P_s\}$ by the diagonal $\hat{\mathbb{Z}} \cdot (P_1 + \cdots + P_s)$. For each $n \in \mathbb{Z}_{>0}$, let $f_n : \mathbb{P}_k^1 \to \mathbb{P}_k^1$ be a cyclic ramified covering of degree n that is totally ramified over the points P_1, P_2 of the codomain and unramified over the other points of the codomain. Then the restriction

$$f_n : f_n^{-1}(\mathbb{P}_k^1 \backslash \{P_1, \dots, P_s\}) \to \mathbb{P}_k^1 \backslash \{P_1, \dots, P_s\}$$

is an abelian covering that corresponds to the following subgroup of Π_Y^{ab}:

$$(n\hat{\mathbb{Z}}P_1 + n\hat{\mathbb{Z}}P_2 + \hat{\mathbb{Z}}P_3 + \cdots + \hat{\mathbb{Z}}P_s)/(n\hat{\mathbb{Z}} \cdot (P_1 + \cdots + P_s)).$$

Therefore, by replacing P_1, P_2 by various P_i, P_j and applying the same argument, we conclude that

$$\bigcap H = \{0\},$$

where H ranges over the set of subgroups of Π_Y^{ab} which correspond to abelian coverings of Y of genus 0. From this fact, one verifies immediately that the natural surjection $\Pi_Y^{\mathrm{ab}} = U^{\mathrm{ab}} \twoheadrightarrow (U/N_0)^{\mathrm{ab}}$ is an isomorphism. Hence, in particular, if we write $N_{\Pi_X}(U)$ for the normalizer of U in Π_X, then it follows immediately from Proposition 3.4 that the natural conjugation action

$$N_{\Pi_X}(U)/U = (N_{\Pi_X}(U)/N_0)/(U/N_0) \to \mathrm{Aut}((U/N_0)^{\mathrm{ab}})$$

is injective. [Note that, since $N_{\Pi_X}(U)$ is an open subgroup of Π_X, it is isomorphic to the étale fundamental group of a hyperbolic curve over k.]

Since $\gamma \in Z(\Pi_X/N_0) \subset N_{\Pi_X}(U)/N_0 = N_{\Pi_X/N_0}(U/N_0)$, it follows that $\gamma \in U/N_0$. Since

$$\bigcap_{g_U=0} U = N_0,$$

we conclude that $\gamma = 1$. Thus Π_X/N_0 is center-free. □

The following well-known result of Belyi [cf. [Bel], Theorem 4 and its proof] plays an important role in the proof of Theorem 4.14 below.

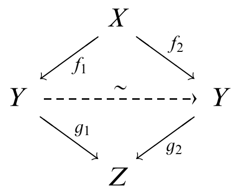
Theorem 4.8 (Belyi). *Let* $\overline{\mathbb{Q}}$ *be an algebraic closure of* $\mathbb{Q}$*,* X *a projective smooth curve over* $\overline{\mathbb{Q}}$*, and* $f : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ *a nonconstant morphism. Then there exists a nonconstant polynomial* $g \in \mathbb{Q}[t]$ *over* $\mathbb{Q}$ *such that the composite*

$$X \xrightarrow{f} \mathbb{P}^1_{\overline{\mathbb{Q}}} \xrightarrow{g} \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

is unramified over the complement of the points 0, 1, ∞ *in the codomain of* g.

To show the main result of this section, we need a few lemmas.

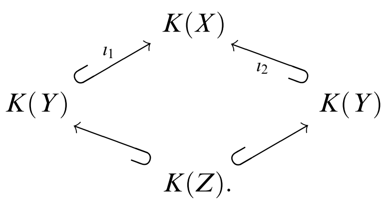
Lemma 4.9. *Let* k *be an algebraically closed field of characteristic* 0*;* X, Y, Z *proper smooth curves over* k*;* $f_1, f_2 : X \to Y$ *and* $g_1, g_2 : Y \to Z$ *nonconstant morphisms over* k *satisfying* $\deg f_1 = \deg f_2$ *and* $g_1 \circ f_1 = g_2 \circ f_2$*. [Here, "*$\deg(-)$*" denotes the degree of a morphism.] Suppose that there exists a closed point* $z \in Z$ *such that* $(g_1 \circ f_1)^{-1}(z)$ *consists of only one point* $x \in X$*. [Note that* x *is necessarily a closed point.] Then there exists an automorphism* λ *of* Y *over* k *such that* $\lambda \circ f_1 = f_2$*, i.e., such that the triangles of the diagram*



commute.

Proof. The following argument is based on the argument of [Ritt], Sections III and IV.

We have a commutative diagram of field extensions:



The existence of an automorphism as asserted in the statement of Lemma 4.9 is equivalent to the condition that $\iota_1(K(Y)) = \iota_2(K(Y))$.

Since X (resp. Z) is smooth over k, the point x (resp. z) determines a discrete valuation w on $K(X)$ (resp. v on $K(Z)$) which is trivial on k. Write $K(X)_w$ (resp. $K(Z)_v$) for the completion of $K(X)$ (resp. $K(Z)$) with respect to w (resp. v). Since x is the unique point of X lying over z, $K(X)_w$ is naturally isomorphic to $K(X) \otimes_{K(Z)} K(Z)_v$. By the Cohen structure theorem, $K(Z)_v$ is isomorphic to a field of formal Laurent series $k((t))$. In particular, the absolute Galois group of $K(Z)_v$ is isomorphic to $\hat{\mathbb{Z}}$. Therefore $K(X)_w/K(Z)_v$ is Galois, and its Galois group is a cyclic group. In particular, the field extension $K(X)_w/K(Z)_v$ has at most one intermediate field of a given degree over $K(Z)_v$. Since $[K(X) : \iota_1(K(Y))] = [K(X) : \iota_2(K(Y))]$, we have $\iota_1(K(Y)) \otimes_{K(Z)} K(Z)_v = \iota_2(K(Y)) \otimes_{K(Z)} K(Z)_v$. By faithfully flat descent, we thus conclude that $\iota_1(K(Y)) = \iota_2(K(Y))$, as desired. □

COROLLARY 4.10. *Let k be a field of characteristic 0 and f_1, f_2, g_1, g_2 nonconstant polynomials in an indeterminate t with coefficients in k satisfying* $\deg g_1 = \deg g_2$ *and* $g_1 \circ f_1 = g_2 \circ f_2$. *Then* $f_2 = af_1 + b$ *for some* $a, b \in k$.

PROOF. Let $\bar{k}$ be an algebraic closure of k, and regard f_1, f_2, g_1, g_2 as endomorphisms of $\mathbb{P}^1_{\bar{k}}$. Note that since $\deg g_1 = \deg g_2$ and $g_1 \circ f_1 = g_2 \circ f_2$, it follows that $\deg f_1 = \deg f_2$. Then $(g_1 \circ f_1)^{-1}(\infty) = \{\infty\}$ and thus by Lemma 4.9,

$$f_2 = \frac{af_1 + b}{cf_1 + d}$$

for some $a, b, c, d \in \bar{k}$ with $ad - bc \neq 0$. Since the left-hand side is a nonconstant polynomial, we may assume that $c = 0$ and $d = 1$. Thus

$$f_2 = af_1 + b.$$

Finally, since f_1 is nonconstant, the k-rationality of the coefficients of f_2 implies that $a, b \in k$. □

LEMMA 4.11. *Let $1 \to \Delta \to \Pi \to G \to 1$ be an exact sequence of profinite groups and N, M closed subgroups of Δ which are normal in Π. Write ρ_N (resp. ρ_M) for the outer representation* $G \to \mathrm{Out}(\Delta/N)$ *(resp.* $G \to \mathrm{Out}(\Delta/M)$*) determined by the exact sequence. Suppose that $N \subset M$. Then* $\ker \rho_N \subset \ker \rho_M$.

PROOF. Write

$$\mathrm{Aut}^{M/N}(\Delta/N) := \{\sigma \in \mathrm{Aut}(\Delta/N) \mid \sigma(M/N) = M/N\}$$

and

$$\mathrm{Out}^{M/N}(\Delta/N) := \mathrm{Aut}^{M/N}(\Delta/N)/\mathrm{Inn}(\Delta/N).$$

Then ρ_N and ρ_M factor as follows:

$$\begin{array}{ccc} & & \mathrm{Out}(\Delta/N) \\ & \nearrow & \\ G \longrightarrow \mathrm{Out}^{M/N}(\Delta/N) & & \\ & \searrow & \\ & & \mathrm{Out}(\Delta/M). \end{array}$$

The assertion follows immediately. □

Write $X_{\mathbb{Q}} := \mathbb{P}^1_{\mathbb{Q}} \backslash \{0, 1, \infty\}$ and $X_{\bar{\mathbb{Q}}} := \mathbb{P}^1_{\bar{\mathbb{Q}}} \backslash \{0, 1, \infty\}$. Recall that, for any Galois category $\mathscr{C}$ and fiber functor F, with associated fundamental group Π [so F induces an equivalence of categories Φ between $\mathscr{C}$ and the category of finite sets on which Π acts continuously], and any closed normal subgroup $N \trianglelefteq \Pi$, the equivalence Φ induces a natural equivalence between the category of finite sets on which Π/N acts continuously and the *full subcategory* of $\mathscr{C}$ whose objects are finite coproducts of connected objects X of $\mathscr{C}$ such that the open subgroup of Π corresponding to X contains N. Thus we obtain a natural homomorphism

$$\psi : \mathrm{Out}(\Delta_{X_{\mathbb{Q}}}/N_{g, X_{\mathbb{Q}}}) \to \mathrm{Sym}(\{\text{isomorphism classes of connected coverings } Y \text{ of } X_{\bar{\mathbb{Q}}} \text{ with } \Pi_Y \supset N_{g, X_{\mathbb{Q}}}\}).$$

THEOREM 4.12. *Write* $N_0 := N_{0, X_{\mathbb{Q}}}$. *Then the composite*

$$G_{\mathbb{Q}} \xrightarrow{\rho_{\mathbb{Q}, N_0}} \mathrm{Out}(\Delta_{X_{\mathbb{Q}}}/N_0) \xrightarrow{\psi} \mathrm{Sym}(\{\textit{isomorphism classes of connected coverings } Y \textit{ of } X_{\bar{\mathbb{Q}}} \textit{ with } \Pi_Y \supset N_0\})$$

[cf. Definition 4.1 *and the following discussion] is injective. In particular,* $\rho_{\mathbb{Q}, N_0}$ *is injective.*

PROOF. The following argument is based on the argument of [Sch], Section II.

Observe that, by transport of structure, the action of $G_{\mathbb{Q}}$ on the set of isomorphism classes of connected coverings Y of $X_{\bar{\mathbb{Q}}}$ with $\Pi_Y \supset N_0$ can be described explicitly as follows: For $\tau \in G_{\mathbb{Q}}$ and $[Y]$ an isomorphism class of a connected covering $Y \to X_{\bar{\mathbb{Q}}}$, $\psi(\tau)([Y])$ is the class of the base-change of Y over $X_{\bar{\mathbb{Q}}}$ by the morphism

$$\mathrm{id}_{X_{\mathbb{Q}}} \times (\tau^*)^{-1} : X_{\bar{\mathbb{Q}}} \xrightarrow{\sim} X_{\bar{\mathbb{Q}}}.$$

Let $\sigma \in G_{\mathbb{Q}}$ be an element which is not the identity, $\alpha \in \bar{\mathbb{Q}}$ such that $\sigma(\alpha) \neq \alpha$, and $f(t)$ a polynomial with coefficients in $\bar{\mathbb{Q}}$ whose derivative is given by $t^3(t-1)^2(t-\alpha)$. Then, by Belyi's theorem [cf. Theorem 4.8], there exists a polynomial $g(t)$ with coefficients in $\mathbb{Q}$ such that $g \circ f$ is branched at most over 0, 1, ∞. Write $Y_\alpha := (g \circ f)^{-1}(X_{\bar{\mathbb{Q}}})$ [where we regard g and f as endomorphisms of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$]. Since Y_α has genus 0, $\Pi_{Y_\alpha} \supset N_0$. Write $[Y_\alpha]$ for the isomorphism class of Y_α.

Observe that the isomorphism class $\psi \circ \rho_{\mathbb{Q}, N_0}(\sigma)([Y_\alpha])$ is represented by

$$Z := (g \circ f^\sigma)^{-1}(X_{\bar{\mathbb{Q}}}) \xrightarrow{g \circ f^\sigma} X_{\bar{\mathbb{Q}}} \subset \mathbb{P}^1_{\bar{\mathbb{Q}}},$$

where f^σ is a polynomial obtained by applying σ to the coefficients of f. Suppose that $\psi \circ \rho_{\mathbb{Q}, N_0}(\sigma)([Y_\alpha]) = [Y_\alpha]$. Then there exists an isomorphism h from Y_α to Z over $X_{\bar{\mathbb{Q}}}$. Passing to compactifications, we obtain the following diagram:

$$\begin{array}{ccc} \mathbb{P}^1_{\bar{\mathbb{Q}}} & \xrightarrow{\quad h \quad} & \mathbb{P}^1_{\bar{\mathbb{Q}}} \\ \Big\downarrow f & & \Big\downarrow f^\sigma \\ \mathbb{P}^1_{\bar{\mathbb{Q}}} & & \mathbb{P}^1_{\bar{\mathbb{Q}}} \\ & {\searrow}^{g} \quad {\swarrow}_{g} & \\ & \mathbb{P}^1_{\bar{\mathbb{Q}}}. & \end{array}$$

Since h is an isomorphism and

$$\begin{aligned} \{\infty\} &= (g \circ f)^{-1}(\infty) \\ &= (g \circ f^\sigma \circ h)^{-1}(\infty) \\ &= h^{-1}((g \circ f^\sigma)^{-1}(\infty)) \\ &= h^{-1}(\infty), \end{aligned}$$

we conclude that h is a linear polynomial, i.e., $h(t) = ct + d$. Then by Corollary 4.10, there exist constants $a, b \in \bar{\mathbb{Q}}$ such that

$$f^\sigma(ct + d) = af(t) + b.$$

Differentiating both sides, we obtain

$$c(ct + d)^3(ct + d - 1)^2(ct + d - \sigma(\alpha)) = at^3(t-1)^2(t-\alpha).$$

Comparing the orders of zeroes of both sides of this last relation, we conclude that $\sigma(\alpha) = \alpha$, a contradiction. Thus $\psi \circ \rho_{\mathbb{Q}, N_0}(\sigma)([Y_\alpha]) \neq [Y_\alpha]$, and therefore $\psi \circ \rho_{\mathbb{Q}, N_0}$ is injective, as desired. $\square$

Corollary 4.13. *Let k be a field of characteristic* 0. *Write*

$$N_0 := N_{0, \mathbb{P}^1_k \setminus \{0,1,\infty\}};$$
$$\rho_{k,N_0} : G_k \to \mathrm{Out}(\Delta_{\mathbb{P}^1_k \setminus \{0,1,\infty\}}/N_0)$$

for the outer representation associated to N_0. *Then* $\ker \rho_{k,N_0}$ *is equal to the kernel of the natural restriction homomorphism* $\varphi : G_k \to G_{\mathbb{Q}}$ *[which is well-defined up to composition with an inner automorphism].*

Proof. For a field K, write $X_K := \mathbb{P}^1_K \setminus \{0,1,\infty\}$ and $N_{0,K} := N_{0,X_K}$. Base-changing from $\mathbb{Q}$ to k yields a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{X_k} & \longrightarrow & \Pi_{X_k} & \longrightarrow & G_k & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow \varphi & & \\ 1 & \longrightarrow & \Delta_{X_{\mathbb{Q}}} & \longrightarrow & \Pi_{X_{\mathbb{Q}}} & \longrightarrow & G_{\mathbb{Q}} & \longrightarrow & 1. \end{array}$$

By Remark 4.2, the left-hand vertical arrow is an isomorphism, and this isomorphism maps $N_{0,k}$ $(= N_0)$ onto $N_{0,\mathbb{Q}}$. Therefore we obtain a commutative diagram:

$$\begin{array}{ccc} G_k & \xrightarrow{\rho_{k,N_{0,k}}} & \mathrm{Out}(\Delta_{X_k}/N_{0,k}) \\ \downarrow \varphi & & \downarrow \wr \\ G_{\mathbb{Q}} & \overset{\rho_{\mathbb{Q},N_{0,\mathbb{Q}}}}{\hookrightarrow} & \mathrm{Out}(\Delta_{X_{\mathbb{Q}}}/N_{0,\mathbb{Q}}), \end{array}$$

where the right-hand vertical arrow is an isomorphism, and the lower horizontal arrow is injective by Theorem 4.12. Thus $\ker \rho_{N_{0,k}} = \ker \varphi$. □

Theorem 4.14. *Let k be a field of characteristic* 0. *Write* $X_k := \mathbb{P}^1_k \setminus \{0,1,\infty\}$. *Suppose that N is a closed normal subgroup of* Δ_{X_k} *which is also normal in* Π_{X_k}. *Assume that* $N \subset N_{0,X_k}$. *Then the kernel of the natural outer representation*

$$\rho_{k,N} : G_k \to \mathrm{Out}(\Delta_{X_k}/N)$$

is equal to the kernel of the natural restriction homomorphism $G_k \to G_{\mathbb{Q}}$ *[which is well-defined up to composition with an inner automorphism]. In particular, if k is either a number field or a p-adic local field for some prime number p, then* $\rho_{k,N}$ *is injective.*

Proof. First we observe that the various assertions of Theorem 4.14 hold when $N = \{1\}$. Indeed, this follows from a similar argument to the argument applied to prove Corollary 4.13, together with the original Belyi theorem, which asserts that the natural outer representation $G_{\mathbb{Q}} \to \mathrm{Out}(\Delta_{X_{\mathbb{Q}}})$ is injective [cf. [Bel], Corollary to Theorem 4 and the discussion preceding Theorem 1].

Now the various assertions of Theorem 4.14 follow immediately from Corollary 4.13 and Lemma 4.11. Here, we apply Lemma 4.11 *twice*, i.e., once to compare $\ker \rho_{k,N}$ to $\ker \rho_{k,N_{0,X_k}}$ and once to compare $\ker \rho_{k,\{1\}}$ to $\ker \rho_{k,N}$, and thus we obtain $\ker \rho_{k,\{1\}} \subset \ker \rho_{k,N} \subset \ker \rho_{k,N_{0,X_k}}$. □

REMARK 4.15. Note that it follows immediately from Belyi's Theorem [cf. Theorem 4.8] that

$$N_g := N_{g,X_k} \subset N_{0,X_k} =: N_0$$

for every $g \in \mathbb{Z}_{\geq 0}$. In particular, it follows from Theorem 4.14 that the kernel of the natural outer representation

$$G_k \to \mathrm{Out}(\Delta_{X_k}/N_g)$$

is equal to the kernel of the natural restriction homomorphism $G_k \to G_{\mathbb{Q}}$.

Acknowledgement

I would like to thank Professors Shinichi Mochizuki and Yuichiro Hoshi for helpful discussions, valuable advice, and warm encouragement. Without their help, this paper could not have been written. Also, I would like to thank Professor Akio Tamagawa for helpful comments and the referee for a useful suggestion that resulted in Remark 3.3.

References

[AI] G. Anderson and Y. Ihara, Pro-l branched coverings of $\mathbb{P}^1$ and higher circular l-units, Part 1, Annals of Math. **128** (1988), pp. 271–293.

[Bel] G. V. Belyĭ, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR Ser. Mat. **43:2** (1979), pp. 269–276; English transl. in Math. USSR-Izv. **14** (1980), pp. 247–256.

[DM] P. Deligne and D. Mumford, The irreducibility of the moduli space of curves of given genus, IHES Publ. Math. **36** (1969), pp. 75–109.

[FM] D. Fronhardt and K. Magaard, Composition factors of monodromy groups, Annals of Math. (2) **154** (2001), pp. 327–345.

[Mzk1] S. Mochizuki, The Absolute Anabelian Geometry of Canonical Curves, Kazuya Kato's fiftieth birthday, Doc. Math. 2003, Extra Vol., pp. 609–640.

[Mzk2] S. Mochizuki, The Absolute Anabelian Geometry of Hyperbolic Curves, Galois Theory and Modular Forms (K. Hashimoto et al., eds.), Developments in Mathematics **11**, Kluwer Academic Publishers (2004), pp. 77–122.

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

[Ritt] J. F. Ritt, Prime and composite polynomials, Trans. Amer. Math. Sot. **23** (1922), pp. 51–66.

[Sch] L. Schneps, Dessins d'enfants on the Riemann sphere, The Grothendieck theory of dessins d'enfants (L. Schneps, ed.), London Mathematical Society Lecture Note Series **200**, Cambridge University Press (1994), pp. 44–77.

Hiroyuki Watanabe
Mitsubishi UFJ Morgan Stanley Securities Co., Ltd.
Otemachi Financial City Grand Cube,
1-9-2*, Otemachi, Chiyoda-ku, Tokyo* 100-8127
E-mail: watanabe.iutabc777@gmail.com