RIMS-1689

Existence of nongeometric pro-p Galois sections of hyperbolic curves

By

Yuichiro HOSHI

January 2010

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

EXISTENCE OF NONGEOMETRIC PRO-P GALOIS SECTIONS OF HYPERBOLIC CURVES

YUICHIRO HOSHI

JANUARY 2010

Abstract. In the present paper, we construct a *nongeometric* pro-p Galois section of a proper hyperbolic curve over a number field, as well as over a p-adic local field. This yields a *negative answer* to the *pro-p Section Conjecture*. We also observe that there exists a proper hyperbolic curve over a number field which admits *infinitely many* conjugacy classes of pro-p Galois sections.

Contents

Introduction 1
0. Notations and Conventions 5
1. Galois sections and their geometricity 6
2. Pro-p outer Galois representations associated to certain coverings of tripods 8
3. Pro-p Galois sections of certain coverings of tripods 11
4. Existence of nongeometric pro-p Galois sections 16
References 17

Introduction

Generalities on the Section Conjecture:

Let $\mathfrak{Primes}$ be the set of all prime numbers, $\Sigma \subseteq \mathfrak{Primes}$ a nonempty subset of $\mathfrak{Primes}$, k a field of characteristic 0, $\overline{k}$ an algebraic closure of k, X a scheme which is geometrically connected and of finite type over k, and $\overline{x}\colon \operatorname{Spec}\overline{k} \to X$ a geometric point of X. By abuse of notation, we shall write $\overline{x}$ for the geometric points of $X \otimes_k \overline{k}$ and $\operatorname{Spec} k$ determined by the geometric point $\overline{x}$ of X. Moreover, we shall write

$$\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$$

for the maximal pro-Σ quotient of $\pi_1(X \otimes_k \overline{k}, \overline{x})$ — i.e., the *pro-Σ geometric fundamental group* of X — and

$$\pi_1(X, \overline{x})^{\underline{\Sigma}}$$

2000 *Mathematics Subject Classification.* 14H30.

for the quotient of $\pi_1(X, \overline{x})$ by the kernel of the natural surjection $\pi_1(X \otimes_k \overline{k}, \overline{x}) \twoheadrightarrow \pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$ — i.e., the *geometrically pro-Σ fundamental group* of X. Then the natural isomorphism $\mathrm{Gal}(\overline{k}/k) \simeq \pi_1(\mathrm{Spec}\, k, \overline{x})$ (cf. [4], Exposé V, Proposition 8.1) and the natural morphisms $X \otimes_k \overline{k} \to X$, $X \to \mathrm{Spec}\, k$ determine a commutative diagram of profinite groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(X \otimes_k \overline{k}, \overline{x}) & \longrightarrow & \pi_1(X, \overline{x}) & \longrightarrow & \mathrm{Gal}(\overline{k}/k) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma} & \longrightarrow & \pi_1(X, \overline{x})^{\underline{\Sigma}} & \longrightarrow & \mathrm{Gal}(\overline{k}/k) & \longrightarrow & 1 \end{array}$$

— where the horizontal sequences are *exact* (cf. [4], Exposé IX, Théorème 6.1), and the vertical arrows are *surjective*. Now we shall refer to a (continuous) section of the lower exact sequence of the above commutative diagram as a *pro-Σ Galois section* of X and to the $\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$-conjugacy class of a pro-Σ Galois section as the *conjugacy class* of the pro-Σ Galois section. Then it follows from the definition of the above commutative diagram that a k-rational point of X (i.e., a section of the structure morphism $X \to \mathrm{Spec}\, k$ of X) determines — up to composition with an inner automorphism arising from $\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$ — a pro-Σ Galois section of X, i.e., we have a natural map from the set $X(k)$ of k-rational points of X to the set $\mathrm{GS}^{\Sigma}(X/k)$ of conjugacy classes of pro-Σ Galois sections of X. Now the Section Conjecture may be stated as follows (cf. [3]):

> (**SC**): If k is a *finitely generated extension of the field of rational numbers*, and X is a *proper hyperbolic curve* over k, then this map $X(k) \to \mathrm{GS}^{\mathfrak{Primes}}(X/k)$ is *bijective*.

Note that one may also formulates a version of (**SC**) for *affine hyperbolic curves*.

Grothendieck proved the *injectivity* of the map $X(k) \to \mathrm{GS}^{\mathfrak{Primes}}(X/k)$ by means of a *well-known theorem of Mordell-Weil* (cf. e.g., [9], Theorem 2.1). On the other hand, the above conjecture — i.e., the *surjectivity* of the map appearing in (**SC**) — remains unsolved.

Pro-p version of the Section Conjecture:

Although the above conjecture (**SC**) remains unsolved, results related to this conjecture have been obtained by various authors:

- (I) An archimedean analogue of (**SC**), i.e., an analogue of (**SC**) for hyperbolic curves over the field of real numbers — cf. [8], §3.
- (II) The injectivity portion of the pro-p version of (**SC**) — i.e., the injectivity of the natural map $X(k) \to \mathrm{GS}^{\{p\}}(X/k)$ — in the case where k is a generalized sub-p-adic field (e.g., k is either a number field or a p-adic local field) — cf. [7], Theorem C

(and its proof); [8], Theorem 4.12 (and Remark following this theorem).

(III) The pro-p version of a birational analogue of (**SC**) for hyperbolic curves over p-adic local fields — cf. [10], Theorem A.

The validity of the above three results (I), (II), and (III) suggests the possibility of the validity of the assertion obtained by replacing the expression "finitely generated extension of the field of rational numbers" in the statement of (**SC**) by the expression "nonarchimedean local field". Moreover, the validity of the two results (II) and (III) suggests the possibility of the validity of the assertion obtained by replacing the notation "$\mathfrak{Primes}$" in the statement of (**SC**) by the notation "$\{p\}$" for some prime number p. That is to say, one is led to expect the validity of the following *pro-p Section Conjecture*:

> (***p*SC**): If k is either a *number field* (i.e., a finite extension of the field of rational numbers) or a *p-adic local field* (i.e., a finite extension of the field of p-adic rational numbers), and X is a *proper hyperbolic curve* over k, then the natural map $X(k) \to \mathrm{GS}^{\{p\}}(X/k)$ is *bijective*, or, equivalently — by the above result (II) — the natural map $X(k) \to \mathrm{GS}^{\{p\}}(X/k)$ is *surjective*.

Main results:

In the present paper, we construct a *counter-example* to the above conjecture (***p*SC**). The first main result of the present paper is as follows (cf. §4):

Theorem A (**Existence of nongeometric pro-*p* Galois sections**). *Let $\mathbb{Q}$ be the field of rational numbers, $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$, p an* **odd regular** *prime number, $\zeta_p \in \overline{\mathbb{Q}}$ a primitive p-th root of unity, $\mathbb{Q}^{\mathrm{unr}} \subseteq \overline{\mathbb{Q}}$ the maximal Galois extension of $\mathbb{Q}(\zeta_p)$ that is* **pro-*p*** *and* **unramified** *over every nonarchimedean prime of $\mathbb{Q}(\zeta_p)$ whose residue characteristic is $\neq p$, $k_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ a finite extension of $\mathbb{Q}(\zeta_p)$ contained in $\mathbb{Q}^{\mathrm{unr}}$, $T_{\mathrm{NF}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}\, k_{\mathrm{NF}}[t^{\pm 1}, 1/(t-1)]$ — where t is an indeterminate — $U_{\mathrm{NF}} \to T_{\mathrm{NF}}$ a connected finite étale covering of T_{NF}, and X_{NF} the (uniquely determined) smooth compactification of U_{NF} over (a finite extension of) k_{NF}. Suppose that the following four conditions are satisfied:*

(A) *X_{NF} is* **of genus ≥ 2**.

(B) *$X_{\mathrm{NF}}(k_{\mathrm{NF}}) \neq \emptyset$. (In particular, X_{NF}, hence also U_{NF}, is* **geometrically connected** *over k_{NF}; thus, X_{NF} and U_{NF} are* **hyperbolic curves** *over k_{NF} [cf. condition (A)].)*

(C) *The finite étale covering $U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}} \to T_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}$ is* **Galois** *and* **of degree a power of *p***.

(D) *The hyperbolic curve* U_{NF} (*cf. condition* (B)), *hence also* X_{NF}, *has* **good reduction** *at every nonarchimedean prime of* k_{NF} *whose residue characteristic is* $\neq p$.

(*For example, if* $p > 3$, *then the number field* $k_{\mathrm{NF}} = \mathbb{Q}(\zeta_p)$ *and the connected finite étale covering*

$$U_{\mathrm{NF}} = \mathrm{Spec}\,\mathbb{Q}(\zeta_p)[x_1^{\pm 1}, x_2^{\pm 1}]/(x_1^p + x_2^p - 1) \longrightarrow T_{\mathrm{NF}}$$

— *where* x_1 *and* x_2 *are indeterminates — given by "*$t \mapsto x_1^p$*" satisfy the above four conditions.*) *Then there exists a finite extension* $k'_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ *of* k_{NF} *contained in* $\mathbb{Q}^{\mathrm{unr}}$ *which satisfies the following condition:*

> *Let* $\square$ *be either "*NF*" or "*LF*",* $k''_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ *a finite extension of* k'_{NF} *contained in* $\mathbb{Q}^{\mathrm{unr}}$, *and* k''_{LF} *the completion of* k''_{NF} *at a nonarchimedean prime of* k''_{NF} *whose residue characteristic is* p. *Then there exists a* **nongeometric** (*cf. Definition 1.1,* (iii), *also Remark 1.1.3*) *pro-*p *Galois section* (*cf. Definition 1.1,* (i)) *of the hyperbolic curve* $X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_{\square}$ (*respectively,* $U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_{\square}$) *over* $k''_{\square}$.

If one's primary interest lies in *diophantine geometry*, one may take the point of view that the *finiteness* of the set $\mathrm{GS}^{\Sigma}(X/k)$ is more important than the *bijectivity* of the natural map $X(k) \to \mathrm{GS}^{\Sigma}(X/k)$ — where $\Sigma \subseteq \mathfrak{Primes}$ is a nonempty subset of $\mathfrak{Primes}$. Indeed, for example, even if the natural *injection* (cf. the above result (II)) $X(k) \hookrightarrow \mathrm{GS}^{\Sigma}(X/k)$ in the case where X is a *proper hyperbolic curve* over a *number field* k is *not bijective*, the *finiteness* of the set $\mathrm{GS}^{\Sigma}(X/k)$ *already implies* the *finiteness* of the set $X(k)$, i.e., an *affirmative answer* to the well-known conjecture of Mordell, which is now a theorem of Faltings.

On the other hand, it follows from the following result, which is the second main result of the present paper, that if one only considers the case where $\Sigma = \{p\}$, then this approach to the conjecture of Mordell *fails* (cf. §4):

Theorem B (**Existence of hyperbolic curves over number fields that admit infinitely many pro-*p* Galois sections**). *We continue to use the notation of Theorem A. Moreover, we take* $p > 7$ *and*

$$U_{\mathrm{NF}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}\, k_{\mathrm{NF}}[x_1^{\pm 1}, x_2^{\pm 1}]/(x_1^p + x_2^p - 1)$$

— *where* x_1 *and* x_2 *are indeterminates. Then there are* **infinitely many** *conjugacy classes of pro-*p *Galois sections* (*cf. Definition 1.1,* (i)) *of the hyperbolic curve* X_{NF} (*respectively,* U_{NF}) *over* k_{NF}.

The present paper is organized as follows: In §1, we discuss the notion of a pro-Σ Galois section. In §2, we consider the pro-p outer Galois representations associated to certain hyperbolic curves obtained as finite étale coverings of tripods. In §3, we consider pro-p Galois

sections of certain hyperbolic curves obtained as finite étale coverings of tripods. In §4, we prove Theorems A and B.

Acknowledgements

The author would like to thank Mamoru Asada, Shinichi Mochizuki, and Akio Tamagawa for helpful comments. This research was supported by Grant-in-Aid for Young Scientists (B) (No. 20740010).

0. Notations and Conventions

Numbers: The notation $\mathfrak{Primes}$ will be used to denote the set of all prime numbers. The notation $\mathbb{Z}$ will be used to denote the set, group, or ring of rational integers. The notation $\mathbb{Q}$ will be used to denote the set, group, or field of rational numbers. If p is a prime number, then the notation $\mathbb{Z}_p$ (respectively, $\mathbb{Q}_p$) will be used to denote the p-adic completion of $\mathbb{Z}$ (respectively, $\mathbb{Q}$).

A finite extension of $\mathbb{Q}$ will be referred to as a *number field*. If p is a prime number, then a finite extension of $\mathbb{Q}_p$ will be referred to as a *p-adic local field*.

Profinite groups: If G is a profinite group, then we shall write

$$\mathrm{Aut}(G)$$

for the group of (continuous) automorphisms of G,

$$\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$$

the group of inner automorphisms of G, and

$$\mathrm{Out}(G) \stackrel{\mathrm{def}}{=} \mathrm{Aut}(G)/\mathrm{Inn}(G)\,.$$

If, moreover, G is *topologically finitely generated*, then one verifies easily that the topology of G admits a basis of *characteristic open subgroups*, which thus induces a *profinite topology* on the groups $\mathrm{Aut}(G)$ and $\mathrm{Out}(G)$.

If G is a profinite group, and $H \subseteq G$ is a closed subgroup of G, then we shall write

$$[H, H] \subseteq G$$

for the closed subgroup of G topologically generated by $h_1 h_2 h_1^{-1} h_2^{-1} \in G$, where h_1, $h_2 \in H$. Note that if H is *normal* in G, then it follows from the fact that $[H, H] \subseteq H$ is a *characteristic subgroup* of H that the closed subgroup $[H, H]$ is *normal in* G.

Curves: We shall say that a scheme X over a field k is a *smooth curve* over k if there exist a scheme Y which is *of dimension* 1, *smooth*, *proper*, and *geometrically connected* over k and a closed subscheme $D \subseteq Y$ which is *finite* and *étale* over k such that X is *isomorphic to* the complement of D in Y over k. If, moreover, a geometric fiber of Y

over k is *of genus* g, and a finite étale covering D over k is *of degree* r, then we shall say that X is a *smooth curve of type* (g, r) over k.

We shall say that a scheme X over a field k is a *hyperbolic curve* (respectively, *tripod*) over k if there exists a pair of nonnegative integers (g, r) such that $2g - 2 + r > 0$ (respectively, $(g, r) = (0, 3)$), and, moreover, X is a smooth curve of type (g, r) over k.

1. Galois sections and their geometricity

Throughout the present paper, fix an odd prime number p and an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$; moreover, let $\zeta_p \in \overline{\mathbb{Q}}$ be a *primitive p-th root of unity*.

In the present §, we discuss the notion of a *pro-Σ Galois section*. In the present §, let k be a field of characteristic 0 and $\overline{k}$ an algebraic closure of k containing $\overline{\mathbb{Q}}$.

Definition 1.1. Let $\Sigma \subseteq \mathfrak{Primes}$ be a nonempty subset of $\mathfrak{Primes}$ (where we refer to the discussion entitled "Numbers" in §0 concerning the set $\mathfrak{Primes}$), X a scheme which is *geometrically connected* and *of finite type* over k, and $\overline{x}\colon \operatorname{Spec}\overline{k} \to X$ a geometric point of X. By abuse of notation, we shall write $\overline{x}$ for the geometric points of $X \otimes_k \overline{k}$ and $\operatorname{Spec} k$ determined by the geometric point $\overline{x}$ of X.

(i) If we write

$$\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$$

for the maximal pro-Σ quotient of $\pi_1(X \otimes_k \overline{k}, \overline{x})$ — i.e., the *pro-Σ geometric fundamental group* of X — and

$$\pi_1(X, \overline{x})^{\underline{\Sigma}}$$

for the quotient of $\pi_1(X, \overline{x})$ by the kernel of the natural surjection $\pi_1(X \otimes_k \overline{k}, \overline{x}) \twoheadrightarrow \pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$ — i.e., the *geometrically pro-Σ fundamental group* of X — then the natural isomorphism $\operatorname{Gal}(\overline{k}/k) \simeq \pi_1(\operatorname{Spec} k, \overline{x})$ (cf. [4], Exposé V, Proposition 8.1) and the natural morphisms $X \otimes_k \overline{k} \to X$, $X \to \operatorname{Spec} k$ determine a commutative diagram of profinite groups

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_1(X \otimes_k \overline{k}, \overline{x}) & \longrightarrow & \pi_1(X, \overline{x}) & \longrightarrow & \operatorname{Gal}(\overline{k}/k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma} & \longrightarrow & \pi_1(X, \overline{x})^{\underline{\Sigma}} & \longrightarrow & \operatorname{Gal}(\overline{k}/k) & \longrightarrow & 1
\end{array}$$

— where the horizontal sequences are *exact* (cf. [4], Exposé IX, Théorème 6.1), and the vertical arrows are *surjective*. Now we shall refer to a section of the lower exact sequence of the above commutative diagram as a *pro-Σ Galois section* of X. Moreover, the $\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$-conjugacy class of a pro-Σ Galois section of X as the *conjugacy class* of the pro-Σ Galois section.

(ii) It follows from the definition of the commutative diagram in (i) that a k-rational point of X (i.e., a section of the structure morphism $X \to \operatorname{Spec} k$ of X) gives rise to a conjugacy class of a pro-Σ Galois section of X. Now we shall say that a pro-Σ Galois section of X *arises from a k-rational point $x \in X(k)$ of* X if the conjugacy class of the pro-Σ Galois section coincides with the conjugacy class of a pro-Σ Galois section determined by the k-rational point $x \in X(k)$ of X.

(iii) Suppose that X is a *hyperbolic curve* over k (where we refer to the discussion entitled "Curves" in §0 concerning the term "hyperbolic curve"). Then we shall say that a pro-Σ Galois section is *geometric* if the image of the pro-Σ Galois section is contained in a decomposition subgroup of $\pi_1(X, \overline{x})^{\Sigma}$ associated to a k-rational point of the (uniquely determined) smooth compactification of X over k.

Remark 1.1.1. Let Y be a scheme which is geometrically connected and of finite type over k and $Y \to X$ a morphism over k. If a pro-Σ Galois section of Y *arises from a k-rational point of Y*, then it follows from the various definitions involved that the pro-Σ Galois section of X determined by the pro-Σ Galois section of Y and the morphism $Y \to X$ *arises from a k-rational point of X*. If, moreover, X and Y are *hyperbolic curves* over k, and a pro-Σ Galois section of Y is *geometric*, then it follows from the various definitions involved that the pro-Σ Galois section of X determined by the pro-Σ Galois section of Y and the morphism $Y \to X$ is *geometric*.

Remark 1.1.2. Suppose that X is a *hyperbolic curve* over k. Then it follows from the various definitions involved that the geometricity of a pro-Σ Galois section of X *depends only on* its conjugacy class.

Remark 1.1.3. Suppose that X is a *hyperbolic curve* over k. Let s be a pro-Σ Galois section of X. Then it follows from the various definitions involved that if s *arises from a k-rational point of X*, then s is *geometric*. If, moreover, the hyperbolic curve X is *proper*, then it follows from the various definitions involved that s is *geometric* if and only if s *arises from a k-rational point of X*.

Remark 1.1.4. Suppose that X is an *abelian variety* over k. Then it follows from the various definitions involved that the following hold:

(i) The pro-Σ geometric fundamental group $\pi_1(X \otimes_k \overline{k}, \overline{x})^{\Sigma}$ is *naturally isomorphic to* the *pro-Σ Tate module* $T_{\Sigma}(X)$ of X, and the geometrically pro-Σ fundamental group $\pi_1(X, \overline{x})^{\Sigma}$ is *naturally isomorphic to* the semi-direct product $T_{\Sigma}(X) \rtimes \operatorname{Gal}(\overline{k}/k)$.

(ii) There exists a *natural bijection* between the set of conjugacy classes of pro-Σ Galois sections of X and the Galois cohomology group $H^1(k, T_{\Sigma}(X))$.

Moreover, it follows from a similar argument to the argument used in the proof of [9], Theorem 2.1 (cf. also [9], Claim 2.2), that the following holds.:

(iii) Under the bijection in (ii), the natural map from $X(k)$ to the set of conjugacy classes of pro-Σ Galois sections of X obtained by sending $x \in X(k)$ to the conjugacy class of a pro-Σ Galois section of X arising from $x \in X(k)$ *coincides with* the *pro-Σ Kummer homomorphism* for X

$$X(k) \longrightarrow H^1(k, T_\Sigma(X)) .$$

2. Pro-p outer Galois representations associated to certain coverings of tripods

In the present §, we consider the pro-p outer Galois representations associated to certain hyperbolic curves obtained as finite étale coverings of tripods (where we refer to the discussion entitled "Curves" in §0 concerning the term "tripod"). In the present §, let

$$k_{\mathrm{NF}} \subseteq \overline{\mathbb{Q}}$$

be a *number field* (where we refer to the discussion entitled "Numbers" in §0 concerning the term "number field"). Write

$$G_{\mathrm{NF}} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathrm{NF}})$$

for the absolute Galois group of k_{NF} and

$$T_{\mathrm{NF}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}\, k_{\mathrm{NF}}[t^{\pm 1}, 1/(t-1)]$$

— where t is an indeterminate — i.e., T_{NF} is a *split tripod* $\mathbb{P}^1_{k_{\mathrm{NF}}} \setminus \{0, 1, \infty\}$ over k_{NF}. Let

$$U_{\mathrm{NF}} \longrightarrow T_{\mathrm{NF}}$$

be a *connected finite étale covering* of T_{NF},

$$(U_{\mathrm{NF}} \subseteq)\ X_{\mathrm{NF}}$$

the (uniquely determined) *smooth compactification* of U_{NF} over (a finite extension of) k_{NF}, and

$$\overline{x} \colon \mathrm{Spec}\, \overline{\mathbb{Q}} \longrightarrow U_{\mathrm{NF}}$$

a geometric point of U_{NF}. Suppose that the following four conditions are satisfied:

(A) X_{NF} is *of genus* ≥ 2.
(B) X_{NF} has a *k_{NF}-rational point* $O \in X_{\mathrm{NF}}(k_{\mathrm{NF}})$. (In particular, X_{NF}, hence also U_{NF}, is *geometrically connected* over k_{NF}; thus, X_{NF} and U_{NF} are *hyperbolic curves* over k_{NF} [cf. condition (A)].)
(C) The finite étale covering $U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}} \to T_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}$ is *Galois* and *of degree a power of p*.

(D) The hyperbolic curve U_{NF} (cf. condition (B)), hence also X_{NF}, has *good reduction* at every nonarchimedean prime of k_{NF} whose residue characteristic is $\neq p$.

We shall write

$$J_{\mathrm{NF}}$$

for the Jacobian variety of X_{NF} (cf. condition (A)) and

$$\iota_O \colon X_{\mathrm{NF}} \longrightarrow J_{\mathrm{NF}}$$

for the closed immersion determined by $O \in X_{\mathrm{NF}}(k_{\mathrm{NF}})$ (cf. condition (B)); moreover, write

$$\Delta_{T_{\mathrm{NF}}} \ \text{(respectively, } \Delta_{U_{\mathrm{NF}}};\ \Delta_{X_{\mathrm{NF}}};\ \Delta_{J_{\mathrm{NF}}})$$

for the maximal pro-p quotient of the geometric fundamental group $\pi_1(T_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x})$ (respectively, $\pi_1(U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x})$; $\pi_1(X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x})$; $\pi_1(J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x})$) — here, by abuse of notation, we write $\overline{x}$ for the geometric points of T_{NF}, X_{NF}, and J_{NF} determined by the geometric point $\overline{x}$ of U_{NF} — and

$$\Pi_{T_{\mathrm{NF}}} \ \text{(respectively, } \Pi_{U_{\mathrm{NF}}};\ \Pi_{X_{\mathrm{NF}}};\ \Pi_{J_{\mathrm{NF}}})$$

for the quotient of the fundamental group $\pi_1(T_{\mathrm{NF}}, \overline{x})$ (respectively, $\pi_1(U_{\mathrm{NF}}, \overline{x})$; $\pi_1(X_{\mathrm{NF}}, \overline{x})$; $\pi_1(J_{\mathrm{NF}}, \overline{x})$) by the kernel of the natural surjection $\pi_1(T_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x}) \twoheadrightarrow \Delta_{T_{\mathrm{NF}}}$ (respectively, $\pi_1(U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x}) \twoheadrightarrow \Delta_{U_{\mathrm{NF}}}$; $\pi_1(X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x}) \twoheadrightarrow \Delta_{X_{\mathrm{NF}}}$; $\pi_1(J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} \overline{\mathbb{Q}}, \overline{x}) \twoheadrightarrow \Delta_{J_{\mathrm{NF}}}$). Then the finite étale covering $U_{\mathrm{NF}} \to T_{\mathrm{NF}}$, the open immersion $U_{\mathrm{NF}} \hookrightarrow X_{\mathrm{NF}}$, and the closed immersion $\iota_O \colon X_{\mathrm{NF}} \hookrightarrow J_{\mathrm{NF}}$ induce a commutative diagram of profinite groups

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \Delta_{T_{\mathrm{NF}}} & \longrightarrow & \Pi_{T_{\mathrm{NF}}} & \longrightarrow & G_{\mathrm{NF}} & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \| & & \\
1 & \longrightarrow & \Delta_{U_{\mathrm{NF}}} & \longrightarrow & \Pi_{U_{\mathrm{NF}}} & \longrightarrow & G_{\mathrm{NF}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \Delta_{X_{\mathrm{NF}}} & \longrightarrow & \Pi_{X_{\mathrm{NF}}} & \longrightarrow & G_{\mathrm{NF}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \Delta_{J_{\mathrm{NF}}} & \longrightarrow & \Pi_{J_{\mathrm{NF}}} & \longrightarrow & G_{\mathrm{NF}} & \longrightarrow & 1
\end{array}$$

— where the horizontal sequences are *exact* — and an isomorphism of profinite groups

$$\Pi_{X_{\mathrm{NF}}}/[\Delta_{X_{\mathrm{NF}}}, \Delta_{X_{\mathrm{NF}}}] \xrightarrow{\sim} \Pi_{J_{\mathrm{NF}}}$$

— where we refer to the discussion entitled "Profinite groups" in §0 concerning the notation "$[-,-]$". Finally, we shall write

$$\rho_{T_{\mathrm{NF}}} \colon G_{\mathrm{NF}} \longrightarrow \mathrm{Out}(\Delta_{T_{\mathrm{NF}}})$$

$$(\text{respectively, } \rho_{U_{\mathrm{NF}}} \colon G_{\mathrm{NF}} \longrightarrow \mathrm{Out}(\Delta_{U_{\mathrm{NF}}});$$

$$\rho_{X_{\mathrm{NF}}} : G_{\mathrm{NF}} \longrightarrow \mathrm{Out}(\Delta_{X_{\mathrm{NF}}});$$
$$\rho_{J_{\mathrm{NF}}} : G_{\mathrm{NF}} \longrightarrow \mathrm{Aut}(\Delta_{J_{\mathrm{NF}}}))$$

— where we refer to the discussion entitled "Profinite groups" in §0 concerning the notation "Out", "Aut" — for the homomorphism determined by the corresponding horizontal sequence in the above commutative diagram,

$$G_{\mathrm{NF}}[T] \ \text{(respectively, } G_{\mathrm{NF}}[U];\ G_{\mathrm{NF}}[X];\ G_{\mathrm{NF}}[J])$$

for the quotient of G_{NF} obtained as the image of $\rho_{T_{\mathrm{NF}}}$ (respectively, $\rho_{U_{\mathrm{NF}}}$; $\rho_{X_{\mathrm{NF}}}$; $\rho_{J_{\mathrm{NF}}}$), and

$$\mathbb{Q}^{\mathrm{unr}} \subseteq \overline{\mathbb{Q}}$$

for the maximal Galois extension of $\mathbb{Q}(\zeta_p)$ that is *pro-p* and *unramified* over every nonarchimedean prime of $\mathbb{Q}(\zeta_p)$ whose residue characteristic is $\neq p$.

Lemma 2.1 (**Quotients determined by the pro-p outer Galois representations associated to certain coverings of tripods).**

(i) *If $\zeta_p \in k_{\mathrm{NF}}$, then the quotient $G_{\mathrm{NF}}[T]$ of G_{NF} is* **pro-p**.
(ii) *If $k_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$, then the natural surjections $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[T]$, $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$, $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[X]$, and $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[J]$* **factor through** *the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/k_{\mathrm{NF}})$.*

Proof. Assertion (i) follows immediately from [1], Theorems A, B. Next, we verify assertion (ii). It follows from [5], Theorem C, (i), that we have natural surjections

$$G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U] \twoheadrightarrow G_{\mathrm{NF}}[T]\,;$$

moreover, it follows from the fact that the natural open (respectively, closed) immersion $U_{\mathrm{NF}} \hookrightarrow X_{\mathrm{NF}}$ (respectively, $\iota_O : X_{\mathrm{NF}} \hookrightarrow J_{\mathrm{NF}}$) *induces* a *surjection* $\Delta_{U_{\mathrm{NF}}} \twoheadrightarrow \Delta_{X_{\mathrm{NF}}}$ (respectively, $\Delta_{X_{\mathrm{NF}}} \twoheadrightarrow \Delta_{J_{\mathrm{NF}}}$) that we have natural surjections

$$G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U] \twoheadrightarrow G_{\mathrm{NF}}[X] \twoheadrightarrow G_{\mathrm{NF}}[J]\,.$$

Thus, to prove assertion (ii), it suffices to verify the fact that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$ *factors through* the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/k_{\mathrm{NF}})$. Moreover, since one may easily verify that the kernel of $\rho_{U_{\mathrm{NF}}}$ is *contained in* the open subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathrm{NF}}(\zeta_p)) \subseteq G_{\mathrm{NF}}$ of G_{NF} — to verify the fact that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$ *factors through* the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/k_{\mathrm{NF}})$ — we may assume without loss of generality that $\zeta_p \in k_{\mathrm{NF}}$. On the other hand, it follows from the condition (D) that — to prove the fact that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$ *factors through* the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/k_{\mathrm{NF}})$ — it suffices to verify the fact that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$ *factors through* a *pro-p quotient* of G_{NF}. On the other hand, if we write

$$\rho_{U_{\mathrm{NF}}/T_{\mathrm{NF}}} : \Delta_{T_{\mathrm{NF}}}/\Delta_{U_{\mathrm{NF}}} \longrightarrow \mathrm{Out}(\Delta_{U_{\mathrm{NF}}})$$

for the homomorphism arising from the exact sequence of profinite groups

$$1 \longrightarrow \Delta_{U_{\mathrm{NF}}} \longrightarrow \Delta_{T_{\mathrm{NF}}} \longrightarrow \Delta_{T_{\mathrm{NF}}}/\Delta_{U_{\mathrm{NF}}} \longrightarrow 1$$

(cf. condition (C)), then it follows immediately that we have inclusions

$$\rho_{U_{\mathrm{NF}}}(\mathrm{Ker}(\rho_{T_{\mathrm{NF}}})) \subseteq \mathrm{Im}(\rho_{U_{\mathrm{NF}}/T_{\mathrm{NF}}}) \subseteq \mathrm{Out}(\Delta_{U_{\mathrm{NF}}})\,;$$

in particular, $\rho_{U_{\mathrm{NF}}}(\mathrm{Ker}(\rho_{T_{\mathrm{NF}}}))$ is a *p-group*. Thus, the fact that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[U]$ *factors through* a *pro-p quotient* of G_{NF} follows immediately from assertion (i). This completes the proof of assertion (ii). □

3. Pro-p Galois sections of certain coverings of tripods

In the present §, we consider pro-p Galois sections of certain hyperbolic curves obtained as finite étale coverings of tripods. The purpose of the present § is to show that a certain pro-p Galois section of the Jacobian variety of a hyperbolic curve *arises from* a pro-p Galois section of the original hyperbolic curve (cf. Theorem 3.5 below). The main results of the present paper, i.e., Theorems A and B in Introduction, may be derived from this result (cf. §4).

We maintain the notation of the preceding §. In the present §, suppose that

$$\mathbb{Q}(\zeta_p) \subseteq k_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}\,.$$

In the present §, let

$$k_{\mathrm{LF}}$$

be the completion of k_{NF} at a nonarchimedean prime whose residue characteristic is p and $\overline{k}_{\mathrm{LF}}$ an algebraic closure of k_{LF} containing $\overline{\mathbb{Q}}$; write, moreover,

$$G_{\mathrm{LF}} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}_{\mathrm{LF}}/k_{\mathrm{LF}})$$

for the absolute Galois group of k_{LF}. Then we have a proper hyperbolic curve

$$X_{\mathrm{LF}} \stackrel{\mathrm{def}}{=} X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k_{\mathrm{LF}}\,,$$

an affine hyperbolic curve

$$U_{\mathrm{LF}} \stackrel{\mathrm{def}}{=} U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k_{\mathrm{LF}}\,,$$

whose smooth compactification is naturally isomorphic to X_{LF}, and an abelian variety

$$J_{\mathrm{LF}} \stackrel{\mathrm{def}}{=} J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k_{\mathrm{LF}}\,,$$

which is naturally isomorphic to the Jacobian variety of X_{LF}, over k_{LF}. Moreover, we shall write

$$\Delta_{X_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Delta_{X_{\mathrm{NF}}}\ ;\ \Delta_{U_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Delta_{U_{\mathrm{NF}}}\ ;\ \Delta_{J_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Delta_{J_{\mathrm{NF}}}\ ;$$

$$\Pi_{X_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Pi_{X_{\mathrm{NF}}} \times_{G_{\mathrm{NF}}} G_{\mathrm{LF}}\ ;\ \Pi_{U_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Pi_{U_{\mathrm{NF}}} \times_{G_{\mathrm{NF}}} G_{\mathrm{LF}}\ ;$$

$$\Pi_{J_{\mathrm{LF}}} \stackrel{\mathrm{def}}{=} \Pi_{J_{\mathrm{NF}}} \times_{G_{\mathrm{NF}}} G_{\mathrm{LF}}\,.$$

Note that "$\Delta_{(-)}$" is naturally isomorphic to the *pro-p geometric fundamental group* of "$(-)$" — i.e., the maximal pro-p quotient of the fundamental group of "$(-) \otimes_{k_{\mathrm{LF}}} \overline{k}_{\mathrm{LF}}$" — and "$\Pi_{(-)}$" is naturally isomorphic to the *geometrically pro-p fundamental group* of "$(-)$" — i.e., the quotient of the fundamental group of "$(-)$" by the kernel of the natural surjection from the fundamental group of "$(-) \otimes_{k_{\mathrm{LF}}} \overline{k}_{\mathrm{LF}}$" to its maximal pro-$p$ quotient.

Definition 3.1. Let $\square$ be either "NF" or "LF".

(i) We shall write

$$G_\square \twoheadrightarrow Q_\square \stackrel{\text{def}}{=} \mathrm{Im}(G_\square \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/\mathbb{Q}))$$

— where the arrow "$G_\square \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$" is the homomorphism determined by the natural inclusions $\mathbb{Q} \hookrightarrow k_\square$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{k}_\square$.

(ii) It follows from Lemma 2.1, (ii), that the outer pro-p Galois representation $G_\square \to \mathrm{Out}(\Delta_{X_\square})$ (respectively, $G_\square \to \mathrm{Out}(\Delta_{U_\square})$) associated to $X_\square$ (respectively, $U_\square$) *factors through* $G_\square \twoheadrightarrow Q_\square$. We shall write

$$\Pi^Q_{X_\square} \ \ (\text{respectively, } \Pi^Q_{U_\square})$$

for the profinite group obtained by pulling back the natural exact sequence of profinite groups

$$1 \longrightarrow \Delta_{X_\square} \longrightarrow \mathrm{Aut}(\Delta_{X_\square}) \longrightarrow \mathrm{Out}(\Delta_{X_\square}) \longrightarrow 1$$

(respectively,

$$1 \longrightarrow \Delta_{U_\square} \longrightarrow \mathrm{Aut}(\Delta_{U_\square}) \longrightarrow \mathrm{Out}(\Delta_{U_\square}) \longrightarrow 1)$$

— where we refer to the discussion entitled "Profinite groups" in §0 concerning the topologies of "Aut" and "Out" — via the resulting (continuous) homomorphism $Q_\square \to \mathrm{Out}(\Delta_{X_\square})$ (respectively, $Q_\square \to \mathrm{Out}(\Delta_{U_\square})$). Note that it follows from the definition of $\Pi^Q_{X_\square}$ (respectively, $\Pi^Q_{U_\square}$) that we have a commutative diagram of profinite groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{X_\square} & \longrightarrow & \Pi_{X_\square} & \longrightarrow & G_\square & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_{X_\square} & \longrightarrow & \Pi^Q_{X_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \end{array}$$

(respectively,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{U_\square} & \longrightarrow & \Pi_{U_\square} & \longrightarrow & G_\square & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_{U_\square} & \longrightarrow & \Pi^Q_{U_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \end{array})$$

— where the horizontal sequences are *exact*, and the vertical arrows are *surjective*.

(iii) We shall write

$$\Pi^Q_{J_\square} \stackrel{\text{def}}{=} \Pi^Q_{X_\square}/[\Delta_{X_\square}, \Delta_{X_\square}]$$

— where we refer to the discussion entitled "Profinite groups" in §0 concerning the notation "$[-,-]$". Thus, the isomorphism

$$\Pi_{X_\square}/[\Delta_{X_\square}, \Delta_{X_\square}] \xrightarrow{\sim} \Pi_{J_\square}$$

induced by ι_O determines a commutative diagram of profinite groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{J_\square} & \longrightarrow & \Pi_{J_\square} & \longrightarrow & G_\square & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_{J_\square} & \longrightarrow & \Pi^Q_{J_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \end{array}$$

— where the horizontal sequences are *exact*, and the vertical arrows are *surjective*.

Remark 3.1.1. It follows from the various definitions involved that the open immersion $U_\square \hookrightarrow X_\square$ and the closed immersion $\iota_O\colon X_\square \hookrightarrow J_\square$ determine a commutative diagram of profinite groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{U_\square} & \longrightarrow & \Pi^Q_{U_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_{X_\square} & \longrightarrow & \Pi^Q_{X_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_{J_\square} & \longrightarrow & \Pi^Q_{J_\square} & \longrightarrow & Q_\square & \longrightarrow & 1 \end{array}$$

— where the horizontal sequences are *exact*, and the vertical arrows are *surjective*.

Lemma 3.2 (**Freeness of certain Galois groups**). *Suppose that p is* **regular**. *Then the profinite groups Q_{NF} and Q_{LF} are* **free pro-p** *groups.*

Proof. Since a closed subgroup of a *free pro-p* group is a *free pro-p* group (cf. [13], Corollary 7.7.5), to prove Lemma 3.2, it suffices to verify the fact that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{unr}}/\mathbb{Q}(\zeta_p))$ is *free pro-p*. On the other hand, this follows from [12], the first example following Theorem 5. □

Lemma 3.3 (**Factorization of certain pro-p Galois sections**). *Let $\square$ be either "*NF*" or "*LF*", s_{NF} a pro-p Galois section of J_{NF} (cf. Definition 1.1,* (i)*), and s_{LF} the pro-p Galois section of J_{LF} obtained as the restriction of s_{NF}. Then the composite*

$$G_\square \stackrel{s_\square}{\hookrightarrow} \Pi_{J_\square} \twoheadrightarrow \Pi^Q_{J_\square}$$

factors through $G_\square \twoheadrightarrow Q_\square$, *i.e., the composite determines a* **section** *of the natural surjection $\Pi^Q_{J_\square} \twoheadrightarrow Q_\square$.*

Proof. First, we verify Lemma 3.3 in the case where $\square$ = "NF". It follows from the definition of the quotient Q_{NF} of G_{NF} that, to prove Lemma 3.3 in the case where $\square$ = "NF", it suffices to show that the following two assertions hold:

(i) The composite $G_{\mathrm{NF}} \overset{s_{\mathrm{NF}}}{\hookrightarrow} \Pi_{J_{\mathrm{NF}}} \twoheadrightarrow \Pi^{Q}_{J_{\mathrm{NF}}}$ *factors through* a pro-p quotient of G_{NF}.

(ii) If $\mathfrak{l}$ is a nonarchimedean prime of k_{NF} whose residue characteristic is $\neq p$, and $I_{\mathfrak{l}} \subseteq G_{\mathrm{NF}}$ is an inertia subgroup of G_{NF} associated to $\mathfrak{l}$, then the image of the composite

$$I_{\mathfrak{l}} \hookrightarrow G_{\mathrm{NF}} \overset{s_{\mathrm{NF}}}{\hookrightarrow} \Pi_{J_{\mathrm{NF}}} \twoheadrightarrow \Pi^{Q}_{J_{\mathrm{NF}}}$$

is $\{1\}$.

Now assertion (i) follows from the fact that $\Pi^{Q}_{J_{\mathrm{NF}}}$ is *pro-p*. Next, we verify assertion (ii). It follows immediately from the definition of Q_{NF} that the image of the composite $I_{\mathfrak{l}} \hookrightarrow G_{\mathrm{NF}} \overset{s_{\mathrm{NF}}}{\hookrightarrow} \Pi_{J_{\mathrm{NF}}} \twoheadrightarrow \Pi^{Q}_{J_{\mathrm{NF}}}$ is *contained in* $\Delta_{J_{\mathrm{NF}}} \subseteq \Pi^{Q}_{J_{\mathrm{NF}}}$; in particular, if we write $D_{\mathfrak{l}} \subseteq G_{\mathrm{NF}}$ for the decomposition subgroup of G_{NF} associated to $\mathfrak{l}$ containing $I_{\mathfrak{l}} \subseteq G_{\mathrm{NF}}$, then we obtain a $D_{\mathfrak{l}}/I_{\mathfrak{l}}$-equivariant homomorphism $I_{\mathfrak{l}} \to \Delta_{J_{\mathrm{NF}}}$, which *factors through* the abelianization of the maximal pro-p quotient of $I_{\mathfrak{l}}$ (cf. assertion (i)). On the other hand, since J_{NF} has *good reduction* at $\mathfrak{l}$ (cf. condition (D) in §2) (respectively, the residue characteristic of $\mathfrak{l}$ is $\neq p$), the weight of the action of the Frobenius element in $D_{\mathfrak{l}}/I_{\mathfrak{l}}$ on $\Delta_{J_{\mathrm{NF}}}$ (respectively, on the abelianization of the maximal pro-p quotient of $I_{\mathfrak{l}}$) is 1 (respectively, 2). Thus, it follows that the image of the $D_{\mathfrak{l}}/I_{\mathfrak{l}}$-equivariant homomorphism $I_{\mathfrak{l}} \to \Delta_{J_{\mathrm{NF}}}$ is $\{1\}$. This completes the proof of assertion (ii) hence also of Lemma 3.3 in the case where $\square$ = "NF".

Next, we verify Lemma 3.3 in the case where $\square$ = "LF". It follows from the various definitions involved that we have a commutative diagram of profinite groups

$$\begin{array}{ccccccc}
G_{\mathrm{LF}} & \xrightarrow{s_{\mathrm{LF}}} & \Pi_{J_{\mathrm{LF}}} & \longrightarrow & \Pi^{Q}_{J_{\mathrm{LF}}} & \longrightarrow & Q_{\mathrm{LF}} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
G_{\mathrm{NF}} & \xrightarrow[s_{\mathrm{NF}}]{} & \Pi_{J_{\mathrm{NF}}} & \longrightarrow & \Pi^{Q}_{J_{\mathrm{NF}}} & \longrightarrow & Q_{\mathrm{NF}}
\end{array}$$

— where the vertical arrows are *injective*. Therefore, Lemma 3.3 in the case where $\square$ = "LF" follows immediately from Lemma 3.3 in the case where $\square$ = "NF", together with the definition of the quotient $Q_{\square}$ of $G_{\square}$. $\square$

Lemma 3.4 (Uniqueness of certain pro-p Galois sections). *Let $\square$ be either "NF" or "LF", $i = 1$ or 2, s^{i}_{NF} a pro-p Galois section of J_{NF} (cf. Definition 1.1,* (i)*), and s^{i}_{LF} the pro-p Galois section of J_{LF} obtained as the restriction of s^{i}_{NF}. If the $\Delta_{J_{\square}}$-conjugacy classes of the*

composites

$$G_\square \overset{s^1_\square}{\hookrightarrow} \Pi_{J_\square} \twoheadrightarrow \Pi^Q_{J_\square} \ ; \ G_\square \overset{s^2_\square}{\hookrightarrow} \Pi_{J_\square} \twoheadrightarrow \Pi^Q_{J_\square}$$

coincide, *then the conjugacy classes of the pro-p Galois sections* $s^1_\square$, $s^2_\square$ **coincide**.

Proof. This follows immediately from Lemma 3.3, together with the existence of the *exact sequence* of Galois cohomology groups

$$0 \longrightarrow H^1(Q_\square, \Delta_{J_\square}) \longrightarrow H^1(G_\square, \Delta_{J_\square}) \longrightarrow H^1(N_\square, \Delta_{J_\square})^{Q_\square}$$

— where $N_\square$ is the kernel of the natural surjection $G_\square \twoheadrightarrow Q_\square$. □

Theorem 3.5 (**Lifting of certain pro-p Galois sections**). *Let* □ *be either "*NF*" or "*LF*", s_{NF} a pro-p Galois section of J_{NF} (cf. Definition 1.1,* (i)*), and s_{LF} the pro-p Galois section of J_{LF} obtained as the restriction of s_{NF}. Suppose that p is* **regular**. *Then there exists a pro-p Galois section $\widetilde{s}_\square$ of $X_\square$ (respectively, $U_\square$) such that the pro-p Galois section of $J_\square$ obtained as the composite*

$$G_\square \overset{\widetilde{s}_\square}{\hookrightarrow} \Pi_{X_\square} \twoheadrightarrow \Pi_{J_\square} \ \ (\textit{respectively}, \ G_\square \overset{\widetilde{s}_\square}{\hookrightarrow} \Pi_{U_\square} \twoheadrightarrow \Pi_{J_\square})$$

— where the second arrow is the surjection induced by ι_O — **coincides with** $s_\square$.

Proof. It follows from Lemma 3.3 that the composite $G_\square \overset{s_\square}{\hookrightarrow} \Pi_{J_\square} \twoheadrightarrow \Pi^Q_{J_\square}$ *determines* a section $s^Q_\square$ of the natural surjection $\Pi^Q_{J_\square} \twoheadrightarrow Q_\square$. On the other hand, since $Q_\square$ is a *free pro-p* group, (cf. Lemma 3.2), and $\Pi^Q_{X_\square}$ (respectively, $\Pi^Q_{U_\square}$) is a *pro-p* group, there exists a section $\widetilde{s}^Q_\square$ of the natural surjection $\Pi^Q_{X_\square} \twoheadrightarrow Q_\square$ (respectively, $\Pi^Q_{U_\square} \twoheadrightarrow Q_\square$) such that the composite $Q_\square \overset{\widetilde{s}^Q_\square}{\hookrightarrow} \Pi^Q_{X_\square} \twoheadrightarrow \Pi^Q_{J_\square}$ (respectively, $Q_\square \overset{\widetilde{s}^Q_\square}{\hookrightarrow} \Pi^Q_{U_\square} \twoheadrightarrow \Pi^Q_{J_\square}$) *coincides with* $s^Q_\square$. Therefore, by pulling back the section $\widetilde{s}^Q_\square$ via $G_\square \twoheadrightarrow Q_\square$, we obtain a section $\widetilde{s}_\square$ of the natural surjection $\Pi_{X_\square} \simeq \Pi^Q_{X_\square} \times_{Q_\square} G_\square \twoheadrightarrow G_\square \simeq Q_\square \times_{Q_\square} G_\square$ (respectively, $\Pi_{U_\square} \simeq \Pi^Q_{U_\square} \times_{Q_\square} G_\square \twoheadrightarrow G_\square \simeq Q_\square \times_{Q_\square} G_\square$). Now it follows from Lemma 3.4, together with the definition of $\widetilde{s}_\square$, that — by replacing $\widetilde{s}_\square$ by a suitable $\Delta_{X_\square}$ (respectively, $\Delta_{U_\square}$)-conjugate of $\widetilde{s}_\square$ — the pro-p Galois section $\widetilde{s}_\square$ of $X_\square$ (respectively, $U_\square$) satisfies the condition in the statement of Theorem 3.5. This completes the proof of Theorem 3.5. □

Corollary 3.6 (**Existence of certain pro-p Galois sections**). *Let* □ *be either "*NF*" or "*LF*". Suppose that p is* **regular**. *Then for any $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(k_{\mathrm{NF}})$, there exists a pro-$p$ Galois section $s_\square$ of $X_\square$ (respectively, $U_\square$) — cf. Definition 1.1,* (i) *— such that the conjugacy class of the pro-p Galois section of $J_\square$ obtained as the composite*

$$G_\square \overset{s_\square}{\hookrightarrow} \Pi_{X_\square} \twoheadrightarrow \Pi_{J_\square} \ \ (\textit{respectively}, \ G_\square \overset{s_\square}{\hookrightarrow} \Pi_{U_\square} \twoheadrightarrow \Pi_{J_\square})$$

— *where the second arrow is the surjection induced by* ι_O — **coincides with** *the conjugacy class of a pro-*p *Galois section of* $J_\square$ *which* **arises from** *the* k_{NF}*-rational point* $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(k_{\mathrm{NF}}) \subseteq J_{\mathrm{LF}}(k_{\mathrm{LF}})$ — *cf. Definition 1.1,* (ii).

Proof. This follows immediately from Theorem 3.5. □

4. Existence of nongeometric pro-p Galois sections

Proof of Theorem A. First, I *claim* that there exists a finite extension $k'_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ of k_{NF} contained in $\mathbb{Q}^{\mathrm{unr}}$ which satisfies the following condition (†):

> (†) : There exists a k'_{NF}-rational point $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(k'_{\mathrm{NF}})[p^\infty]$ of the Jacobian variety J_{NF} of X_{NF} which is *annihilated by a power of* p such that
>
> $$v_p(\mathrm{ord}(y)) < v_p(\mathrm{ord}(x_{\mathrm{NF}}))$$
>
> for any $y \in J_{\mathrm{NF}}(\overline{\mathbb{Q}})[\mathrm{tor}] \cap \iota_O(X_{\mathrm{NF}}(\overline{\mathbb{Q}}))$ — where v_p is the p-adic valuation on $\mathbb{Z}$ such that $v_p(p) = 1$, and $J_{\mathrm{NF}}(\overline{\mathbb{Q}})[\mathrm{tor}] \subseteq J_{\mathrm{NF}}(\overline{\mathbb{Q}})$ is the *maximal torsion subgroup* of $J_{\mathrm{NF}}(\overline{\mathbb{Q}})$.

Indeed, it follows from Lemma 2.1, (ii), that the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow G_{\mathrm{NF}}[J]$ *factors through* the natural surjection $G_{\mathrm{NF}} \twoheadrightarrow Q_{\mathrm{NF}}$; thus, the above *claim* follows immediately from the fact that the intersection

$$J_{\mathrm{NF}}(\overline{\mathbb{Q}})[\mathrm{tor}] \cap \iota_O(X_{\mathrm{NF}}(\overline{\mathbb{Q}}))$$

is *finite* (cf. [11], Théorème 1). This completes the proof of the above *claim*.

The rest of this proof is devoted to verifying the fact that this finite extension $k'_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ of k_{NF} satisfies the condition in the statement of Theorem A. Let $\square$ be either "NF" or "LF", $k''_{\mathrm{NF}} \subseteq \mathbb{Q}^{\mathrm{unr}}$ a finite extension of k'_{NF} contained in $\mathbb{Q}^{\mathrm{unr}}$, and k''_{LF} the completion of k''_{NF} at a nonarchimedean prime of k''_{NF} whose residue characteristic is p. Moreover, let $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(k''_{\mathrm{NF}})[p^\infty]$ be a k''_{NF}-rational point which satisfies the condition in (†) in the above *claim*, i.e., a k''_{NF}-rational point of J_{NF} which is *annihilated by a power of* p such that

$$v_p(\mathrm{ord}(y)) < v_p(\mathrm{ord}(x_{\mathrm{NF}}))$$

for any $y \in J_{\mathrm{NF}}(\overline{\mathbb{Q}})[\mathrm{tor}] \cap \iota_O(X_{\mathrm{NF}}(\overline{\mathbb{Q}}))$. Then it follows from Corollary 3.6 that there exists a pro-p Galois section $s_\square$ of the hyperbolic curve $X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_\square$ (respectively, $U_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_\square$) over $k''_\square$ such that the conjugacy class of the pro-p Galois section of $J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_\square$ determined by $s_\square$ *coincides with* the conjugacy class of a pro-p Galois section of $J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_\square$ which *arises from* the k''_{NF}-rational point $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(k''_{\mathrm{NF}}) \subseteq J_{\mathrm{NF}}(k''_{\mathrm{LF}})$.

Assume that the pro-p Galois section of $X_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_{\square}$ determined by $s_{\square}$ *arises from* a $k''_{\square}$-rational point $x \in X_{\mathrm{NF}}(k''_{\square})$ (cf. Remarks 1.1.1, 1.1.3). Now it follows from the well-known theorem of Mordell-Weil if $\square =$ "NF" or [6], Theorem 7, if $\square =$ "LF" that the kernel of the pro-p Kummer homomorphism for $J_{\mathrm{NF}} \otimes_{k_{\mathrm{NF}}} k''_{\square}$

$$\kappa\colon J_{\mathrm{NF}}(k''_{\square}) \longrightarrow H^1(k''_{\square}, \Delta_{J_{\mathrm{NF}}})$$

coincides with the *subgroup* $J_{\mathrm{NF}}(k''_{\square})_{\neq p}$ *of* $J_{\mathrm{NF}}(k''_{\square})$ *consisting of torsion elements* $a \in J_{\mathrm{NF}}(k''_{\square})$ *of* $J_{\mathrm{NF}}(k''_{\square})$ *such that every prime divisor of the order* $\mathrm{ord}(a)$ *of* a *is* $\neq p$. In particular, it follows from Remark 1.1.4, together with the various definitions involved, that the images of x_{NF} and $\iota_O(x)$ in $J_{\mathrm{NF}}(k''_{\square})/J_{\mathrm{NF}}(k''_{\square})_{\neq p}$ *coincide*; thus, since $x_{\mathrm{NF}} \in J_{\mathrm{NF}}(\overline{\mathbb{Q}})[\mathrm{tor}]$, it follows that $\iota_O(x) \in J_{\mathrm{NF}}(k''_{\mathrm{LF}})[\mathrm{tor}] \cap \iota_O(X_{\mathrm{NF}}(k''_{\mathrm{LF}}))$ — in contradiction to the assumption that x_{NF} satisfies the condition in (†) in the above *claim*. This completes the proof of the fact that the finite extension k'_{NF} of k_{NF} satisfies the condition in the statement of Theorem A. □

Proof of Theorem B. Since the set of k_{NF}-rational points of the Jacobian variety of X_{NF} is *infinite* (cf. [2], Theorem 2.1), it follows immediately from the well-known theorem of Mordell-Weil that the set consisting of conjugacy classes of pro-p Galois sections of the Jacobian variety of X_{NF} is *infinite* (cf. the discussion concerning the kernel of the pro-p Kummer homomorphism "κ" in the proof of Theorem A, also Remark 1.1.4). Therefore, Theorem B follows immediately from Corollary 3.6. This completes the proof of Theorem B. □

References

[1] G. Anderson and Y. Ihara, Pro-l branched coverings of $\mathbb{P}^1$ and higher circular l-units, *Ann. of Math.* (**2**) **128** (1988), no. **2**, 271–293.

[2] B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, *Invent. Math.* **44** (1978), no. **3**, 201–224.

[3] A. Grothendieck, letter to G. Faltings (June 1983) in P. Lochak, L. Schneps, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, London Math. Soc. Lect. Note Ser. **242**, Cambridge Univ. Press (1997).

[4] A. Grothendieck et al., *Revêtements étales et groupe fondamental* (SGA 1), Séminaire de géométrie algébrique du Bois Marie 1960–61, Documents Mathématiques, **3**. Société Mathématique de France, Paris, 2003.

[5] Y. Hoshi and S. Mochizuki, *On the combinatorial anabelian geometry of nodally nondegenerate outer representations*, RIMS preprint **1677**.

[6] A. Mattuck, Abelian varieties over p-adic ground fields, *Ann. of Math.* (**2**) **62**, (1955). 92–119.

[7] S. Mochizuki, The local pro-p anabelian geometry of curves, *Invent. Math.* **138** (1999), no. **2**, 319–423.

[8] S. Mochizuki, Topics surrounding the anabelian geometry of hyperbolic curves, *Galois groups and fundamental groups*, 119–165, Math. Sci. Res. Inst. Publ., **41**, Cambridge Univ. Press, Cambridge, 2003.

[9] H. Nakamura, Galois rigidity of algebraic mappings into some hyperbolic varieties, *Internat. J. Math.* **4** (1993), no. **3**, 421–438.

[10] F. Pop, On the birational p-adic section conjecture, to appear in *Compositio Math.*

[11] M. Raynaud, Courbes sur une variété abélienne et points de torsion, *Invent. Math.* **71** (1983), no. **1**, 207–233.

[12] I. R. Šafarevič, Extensions with given points of ramification, *Inst. Hautes Études Sci. Publ. Math.* **18** (1964), 295–319; English transl. in *Amer. Math. Soc. Transl.* Ser. **2 59** (1966), 128–149.

[13] L. Ribes and P. Zalesskii, *Profinite groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, **3**. Folge, A Series of Modern Surveys in Mathematics, **40**, Springer-Verlag, Berlin, 2000.

(Yuichiro Hoshi) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, JAPAN

E-mail address: yuichiro@kurims.kyoto-u.ac.jp