Hoshi, Y.
Osaka J. Math.
52 (2015), 647–675

ON THE KERNELS OF THE PRO-l OUTER GALOIS REPRESENTATIONS ASSOCIATED TO HYPERBOLIC CURVES OVER NUMBER FIELDS

YUICHIRO HOSHI

(Received May 28, 2013, revised March 10, 2014)

Abstract

In the present paper, we discuss the relationship between the Galois extension corresponding to the kernel of the pro-l outer Galois representation associated to a hyperbolic curve over a number field and l-moderate points of the hyperbolic curve. In particular, we prove that, for a certain hyperbolic curve, the Galois extension under consideration is generated by the coordinates of the l-moderate points of the hyperbolic curve. This may be regarded as an analogue of the fact that the Galois extension corresponding to the kernel of the l-adic Galois representation associated to an abelian variety is generated by the coordinates of the torsion points of the abelian variety of l-power order. Moreover, we discuss an application of the argument of the present paper to the study of the Fermat equation.

Contents

Introduction

Throughout the present paper, let l be a prime number, k a number field (i.e., a finite extension of the field of rational numbers), $\overline{k}$ an algebraic closure of k, and C a *hyperbolic curve* over k. Write $G_k \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{k}/k)$, Δ_C for the *pro-l geometric étale fundamental group* of C (i.e., the maximal pro-l quotient of the étale fundamental group $\pi_1(C \otimes_k \overline{k})$ of $C \otimes_k \overline{k}$), and

$$\rho_C \colon G_k \to \mathrm{Out}(\Delta_C)$$

2010 Mathematics Subject Classification. Primary 14H30; Secondary 14H25, 14K15, 11D41.

for the *pro-l outer Galois representation associated to C*. In the present paper, we study the Galois extension

$$\Omega_C \stackrel{\text{def}}{=} \overline{k}^{\mathrm{Ker}(\rho_C)}$$

of k corresponding to the kernel of ρ_C.

The notion for an abelian variety A/k naturally corresponding to the above pro-l outer Galois representation ρ_C is the *l-adic Galois representation on the l-adic Tate module* of A. Thus, the Galois extension Ω_A for the abelian variety A naturally corresponding to the above Galois extension Ω_C is the *Galois extension of k obtained by adjoining to k the coordinates of all torsion points of A of l-power order*, i.e.,

$$\Omega_A = k(\text{torsion points of } l\text{-power order of } A).$$

From this point of view, we have the following two questions:

- What is an analogue for a hyperbolic curve of a *torsion point of l-power order* of an abelian variety?
- If one has an analogue for a hyperbolic curve of a *torsion point of l-power order* of an abelian variety, then does the equality

$$\Omega_C = k(\text{“torsion points of } l\text{-power order” of } C)$$

hold?

Of course, to realize an analogue for a hyperbolic curve of a torsion point of l-power order of an abelian variety, one may consider a point that lies on the *intersection of a given hyperbolic curve and the set of torsion points of l-power order of the Jacobian variety of the curve* (by means of a suitable immersion from the curve into the Jacobian variety). On the other hand, however, since (one verifies easily that) the above Galois extension Ω_C of k is always *infinite*, it follows from the *finiteness result* of [20], Théorème 1, that this analogue for a hyperbolic curve of a torsion point of l-power order always does *not satisfy* the above equality

$$\Omega_C = k(\text{“torsion points of } l\text{-power order” of } C).$$

In §2 of the present paper, we define the notion of an *l-moderate point* of a hyperbolic curve and an abelian variety (cf. Definition 2.4). Typical examples of *l-moderate points* of hyperbolic curves are as follows:

- The closed point of the tripod $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$ corresponding to a *tripod l-unit* (cf. Definition 1.6; Proposition 2.8).
- The closed point of a hyperbolic curve of type (1, 1) corresponding to a *torsion point of l-power order* of the underlying elliptic curve of the hyperbolic curve (cf. Proposition 2.7).

In §2, we also prove that,

for a closed point of a hyperbolic curve, the closed point is *l-moderate* if and only if the closed point satisfies the condition "$E(C, x, l)$" introduced by Matsumoto in [13], Introduction (cf. the equivalence (1) $\Leftrightarrow$ (3) of Proposition 2.5).

Moreover, we prove that,

for a closed point of an abelian variety, the closed point is *l-moderate* if and only if the closed point is *torsion* (cf. Proposition 2.6).

In particular,

the notion of an *l-moderate point* of a hyperbolic curve may be regarded as an analogue of the notion of a *torsion point* of an abelian variety.

From this observation, one may pose the following question:

Does the equality

$$\Omega_C = k_C^{\text{mdr-}l} \stackrel{\text{def}}{=} k(l\text{-moderate points of } C)$$

hold?

Our first result concerning the above question is as follows (cf. Theorem 3.1).

Theorem A. *Every l-*moderate *point of C is* defined *over Ω_C, i.e.,*

$$k_C^{\text{mdr-}l} \subseteq \Omega_C.$$

Theorem A follows immediately from standard techniques that appear in the study of *Galois sections* (cf., e.g., [6], [9]).

At the time of writing, the author does not know whether or not the converse

$$\Omega_C \subseteq k_C^{\text{mdr-}l},$$

i.e., the *equality under consideration*, holds in general. However, Theorem A leads naturally to some examples of hyperbolic curves for which the equality under consideration holds. In particular, we verify the following result (cf. Corollary 3.3; Example 3.4).

Theorem B. *If one of the following five conditions is satisfied, then the* equality

$$\Omega_C = k_C^{\text{mdr-}l}$$

holds:

(i) *C is isomorphic to $\mathbb{P}^1_k \setminus S$ for some $S \in \mathbb{S}(\{0, 1, \infty\})$ (cf.* Definition 1.4, (iv)) *such that $S \setminus \{\infty\} \subseteq k$ (e.g., the* tripod $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$).

(ii) *l is odd, and there exists a positive integer n such that C is isomorphic to the (open)* Fermat curve *of degree l^n*

$$\mathrm{Spec}(k[s, t]/(s^{l^n} + t^{l^n} + 1))$$

—where s and t are indeterminates.
(iii) *l is odd, and there exists a positive integer n such that $(l, n) \neq (3, 1)$, and, moreover, C is isomorphic to the (compactified)* Fermat curve *of degree l^n*

$$\mathrm{Proj}(k[s, t, u]/(s^{l^n} + t^{l^n} + u^{l^n}))$$

—where s, t, and u are indeterminates.
(iv) *$l = 3$, and there exists a positive integer n such that a primitive 3^n-th root of unity is contained in k, and, moreover, C is isomorphic to the* modular curve *$Y(3^n)$ parametrizing elliptic curves with $\Gamma(3^n)$-structures (cf., e.g.,* [12]).
(v) *$l = 3$, and there exists an integer $n \geq 2$ such that a primitive 3^n-th root of unity is contained in k, and, moreover, C is isomorphic to the smooth compactification $X(3^n)$ of the modular curve $Y(3^n)$ (cf.* (iv)).

Theorem B in the case where condition (i) is satisfied is verified from Theorem A, together with the *explicit description* of $\Omega_{\mathbb{P}^1_k \setminus \{0,1,\infty\}}$ given in [1]. Theorem B in the case where one of conditions (ii), (iii), (iv), and (v) is satisfied is verified from Theorem A and Theorem B in the case where condition (i) is satisfied, together with some results given in [7].

Finally, we present an application of the discussion of the present paper to the *study of the Fermat equation* (cf. Corollary 3.6).

Theorem C. *Suppose that l is ≥ 5 and* regular. *Let $a, b \in \Omega_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\}} \setminus \{0, 1\}$ be elements of $\Omega_{\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\}} \setminus \{0, 1\}$ such that*

$$a^l + b^l = 1.$$

Then the hyperbolic curve of type $(0, 4)$ over $\mathbb{Q}(a^l)$

$$\mathbb{P}^1_{\mathbb{Q}(a^l)} \setminus \{0, 1, \infty, a^l\}$$

is not quasi-*l*-monodromically full (*cf.* [5], Definition 2.2, (iii)).

Let us observe that it follows immediately from (the discussion given in the proof of) Theorem C that

- a positive solution of a *problem of Ihara* concerning the kernel of the pro-l outer representation associated to $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ (cf., e.g., [11], Lecture I, §2; also Remark 1.8.1 of the present paper) and
- a positive solution of a *problem of Matsumoto and Tamagawa* concerning monodromic fullness for hyperbolic curves (cf. [14], Problem 4.1; also [8], Introduction)

imply *Fermat's last theorem* (cf. Remark 3.6.1). On the other hand, however, the author answered the problem of Matsumoto and Tamagawa given as [14], Problem 4.1, in the *negative* in [8] (cf. [8], Theorem A). The above implication is one of the main motivations of studying the problem of Matsumoto and Tamagawa in [8].

0. Notations and conventions

Numbers. The notation $\mathbb{Z}$ will be used to denote the ring of rational integers. The notation $\mathbb{Q}$ will be used to denote the field of rational numbers. If l is a prime number, then we shall write $\mathbb{F}_l \stackrel{\text{def}}{=} \mathbb{Z}/l\mathbb{Z}$ and $\mathbb{Z}_l$ for the l-adic completion of $\mathbb{Z}$. We shall refer to a finite extension of $\mathbb{Q}$ as a *number field*.

Profinite groups. Let G be a profinite group. Then we shall write $Z(G)$ for the *center* of G. We shall say that G is *slim* if $Z(H) = \{1\}$ for every open subgroup $H \subseteq G$ of G.

Let G be a profinite group and $\mathbb{P}$ a property for profinite groups. Then we shall say that G is *almost* $\mathbb{P}$ if an open subgroup of G is $\mathbb{P}$.

Let G be a profinite group. Then 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 G be a profinite group. Then we shall write $\text{Aut}(G)$ for the group of (continuous) automorphisms of G, $\text{Inn}(G) \subseteq \text{Aut}(G)$ for the group of inner automorphisms of G, and $\text{Out}(G) \stackrel{\text{def}}{=} \text{Aut}(G)/\text{Inn}(G)$ for the group of outer automorphisms of 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 group $\text{Aut}(G)$, hence also a *profinite topology* on the group $\text{Out}(G)$.

Curves. Let S be a scheme and X a scheme over S. Then we shall say that X is a *smooth curve* over S if there exist a scheme X^{cpt} which is smooth, proper, geometrically connected, and of relative dimension one over S and a closed subscheme $D \subseteq X^{\text{cpt}}$ of X^{cpt} which is finite and étale over S such that the complement $X^{\text{cpt}} \setminus D$ of D in X^{cpt} is isomorphic to X over S. Note that, as is well-known, if X is a smooth curve over (the spectrum of) a field k, then the pair "(X^{cpt}, D)" is *uniquely determined up to canonical isomorphism over* k; we shall refer to X^{cpt} as the *smooth compactification* of X over k and to a geometric point of X^{cpt} whose image lies on D as a *cusp* of X.

Let S be a scheme. Then we shall say that a smooth curve X over S is a *hyperbolic curve* (of type (g, r)) (respectively, *tripod*) over S if there exist a pair (X^{cpt}, D) satisfying the condition in the above definition of the term "smooth curve" and a pair (g, r) of nonnegative integers such that $2g - 2 + r > 0$ (respectively, $(g, r) = (0, 3)$), any geometric fiber of $X^{\text{cpt}} \to S$ is (a necessarily smooth proper connected curve) of genus g, and the degree of $D \subseteq X^{\text{cpt}}$ over S is r.

Let S be a scheme, $U \subseteq S$ an open subscheme of S, and X a hyperbolic curve over U. Then we shall say that X admits *good reduction* over S if there exists a hyperbolic curve X_S over S such that $X_S \times_S U$ is isomorphic to X over U.

1. Generalities on the kernels of pro-l outer Galois representations

Throughout the present paper, let l be a prime number, k a number field, $\overline{k}$ an algebraic closure of k, C a *hyperbolic curve* over k, A an *abelian variety* over k, and $V \in \{C, A\}$. Write $G_k \overset{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k)$ and C^{cpt} for the *smooth compactification* of C over k. In the present §1, we discuss generalities on the kernel of the pro-l outer Galois representation associated to V.

DEFINITION 1.1. (i) We shall write

$$\Delta_V$$

for the *pro-l geometric étale fundamental group* of V (i.e., the maximal pro-l quotient of the étale fundamental group $\pi_1(V \otimes_k \overline{k})$ of $V \otimes_k \overline{k}$);

$$\Pi_V$$

for the *geometrically pro-l étale fundamental group* of V (i.e., the quotient of the étale fundamental group $\pi_1(V)$ of V by the kernel of the natural surjection $\pi_1(V \otimes_k \overline{k}) \twoheadrightarrow \Delta_V$). Thus, we have a natural exact sequence of profinite groups

$$1 \to \Delta_V \to \Pi_V \to G_k \to 1$$

(cf. [25], Exposé IX, Théorème 6.1).
(ii) We shall write

$$\rho_V \colon G_k \to \mathrm{Out}(\Delta_V)$$

for the outer action determined by the exact sequence of (i). We shall refer to ρ_V as the *pro-l outer Galois representation associated to V*.
(iii) We shall write

$$G_k \twoheadrightarrow \Gamma_V \overset{\mathrm{def}}{=} G_k/\mathrm{Ker}(\rho_V) \quad (\subseteq \mathrm{Out}(\Delta_V))$$

for the quotient of G_k determined by ρ_V.
(iv) We shall write

$$\Omega_V \overset{\mathrm{def}}{=} \overline{k}^{\mathrm{Ker}(\rho_V)},$$

i.e.,

$$\Gamma_V = \mathrm{Gal}(\Omega_V/k).$$

REMARK 1.1.1. It follows immediately from the discussion given in [18], §18, that there exists a natural isomorphism of Δ_A with the *l-adic Tate module $T_l(A)$* of A. Moreover, one verifies easily that the Galois representation $\rho_A \colon G_k \to \mathrm{Out}(\Delta_A) = \mathrm{Aut}(\Delta_A)$

coincides, relative to this isomorphism $\Delta_A \xrightarrow{\sim} T_l(A)$, with the usual l-adic Galois representation $G_k \to \mathrm{Aut}(T_l(A))$ associated to A.

REMARK 1.1.2. Let $U \subseteq C$ be an open subscheme of C. Then one verifies easily that U is a *hyperbolic curve* over k. Moreover, it follows immediately from [25], Exposé V, Proposition 8.2, that the natural open immersion $U \hookrightarrow C$ induces an outer *surjection* $\Pi_U \twoheadrightarrow \Pi_C$. Thus, we have a natural factorization $G_k \twoheadrightarrow \Gamma_U \twoheadrightarrow \Gamma_C$.

REMARK 1.1.3. Suppose that $C^{\mathrm{cpt}}(k) \neq \emptyset$, and that C^{cpt} is of *genus* ≥ 1. Write J_C for the Jacobian variety of C^{cpt}. Then it follows immediately from [15], Proposition 9.1, together with [25], Exposé V, Proposition 8.2, that the morphism $C \hookrightarrow J_C$ determined by a k-rational point of C^{cpt} induces an outer *surjection* $\Pi_C \twoheadrightarrow \Pi_{J_C}$. Thus, we have a natural factorization $G_k \twoheadrightarrow \Gamma_C \twoheadrightarrow \Gamma_{J_C}$.

REMARK 1.1.4. Let $N \subseteq G_k$ be a normal closed subgroup of G_k. Then it follows from the *Shafarevich conjecture for abelian varieties over number fields* proven by Faltings, together with Proposition 1.2, (ii), below, that, for a fixed positive integer d,

the set of the isomorphism classes of abelian varieties A of dimension d over k such that $\mathrm{Ker}(\rho_A) = N$ is *finite*.

On the other hand, it follows from [5], Theorem C, that, for a fixed pair (g, r) of nonnegative integers such that $2g - 2 + r > 0$,

the set of the isomorphism classes of hyperbolic curves C of type (g, r) over k such that $\mathrm{Ker}(\rho_C) = N$ is *finite*.

Moreover, it follows from [5], Theorem A, that

the cardinality of the set of the isomorphism classes of hyperbolic curves C of genus zero over k such that C is *l-monodromically full* (cf. [5], Definition 2.2, (i)), every cusp of C is defined over k, and, moreover, it holds that $\mathrm{Ker}(\rho_C) = N$ is *at most one*.

REMARK 1.1.5. If one thinks the (not *pro-l*, as in the present paper, but) *profinite* outer Galois representation associated to C (i.e., the outer representation of G_k on $\pi_1(C \otimes_k \overline{k})$ determined by a similar exact sequence to the exact sequence of Definition 1.1, (i)), then the kernel is *trivial* (cf. [10], Theorem C).

Proposition 1.2. *The following hold*:

(i) *The profinite group Γ_V is* almost pro-l. *More precisely, if the composite*

$$G_k \xrightarrow{\rho_V} \mathrm{Out}(\Delta_V) \to \mathrm{Aut}(\Delta_V^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l)$$

factors through a pro-l quotient of G_k, then the profinite group Γ_V is pro-l.

(ii) *Let $\mathfrak{p}$ be a nonarchimedean prime of k whose residue characteristic is $\neq l$. Then it holds that V admits* good reduction *at $\mathfrak{p}$ if and only if the Galois extension Ω_V/k*

is unramified *at* $\mathfrak{p}$. *In particular, the Galois extension* Ω_V/k *is* unramified *for all but finitely many nonarchimedean primes of* k.
(iii) *The profinite group* Γ_V *is* topologically finitely generated.
(iv) *The center* $Z(\Gamma_A)$ *of* Γ_A *is* infinite.
(v) *The profinite group* Γ_C *is* almost slim.
(vi) *It holds that* $\Omega_{\mathrm{tpd}_{/k}} \overset{\mathrm{def}}{=} \Omega_{\mathbb{P}^1_k\setminus\{0,1,\infty\}} \subseteq \Omega_C$.

Proof. First, we verify assertion (i). Since Δ_V is *topologically finitely generated* and *pro-l*, it follows that the kernel of the natural homomorphism $\mathrm{Out}(\Delta_V) \to \mathrm{Aut}(\Delta_V^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l)$ is *pro-l*, which thus implies assertion (i). This completes the proof of assertion (i). Assertion (ii) in the case where $V = A$ (respectively, $V = C$) follows immediately from [21], Theorem 1 (respectively, [24], Theorem 0.8). Assertion (iii) is a formal consequence (cf., e.g., the proof of [14], Lemma 3.3) of *class field theory*, together with assertions (i), (ii). Assertion (iv) follows immediately from the fact that the image of ρ_A *contains infinitely many homotheties* in $\mathrm{Aut}(\Delta_A)$ (cf. [2], [3]). Assertion (v) is a formal consequence (cf., e.g., the proof of [5], Proposition 1.7, (ii)) of the *pro-l version of the Grothendieck conjecture for hyperbolic curves*, i.e., [16], Theorem A. Assertion (vi) follows from [10], Theorem C, (i) (cf. also [23], Remark 0.3; [23], Theorem 0.4; [23], Theorem 0.5). This completes the proof of Proposition 1.2. □

Corollary 1.3. Γ_C *is* not isomorphic *to* Γ_A. *In particular, in the situation of* Remark 1.1.3, *the natural surjection* $\Gamma_C \twoheadrightarrow \Gamma_{J_C}$ *is* not *an* isomorphism.

Proof. This follows immediately from Proposition 1.2, (iv), (v). □

REMARK 1.3.6. (i) In the case of abelian varieties, we have a "*tautological geometric description*" of the Galois extension Ω_A of k corresponding to the kernel of ρ_A

$$\Omega_A = k(\text{torsion points of } l\text{-power order of } A)$$

—where we write k(torsion points of l-power order of A) for the Galois extension of k obtained by adjoining to k the coordinates of all torsion points of A of l-power order.
(ii) On the other hand, in the case of hyperbolic curves, at the time of writing, the author does not know the existence of such a description of the Galois extension Ω_C of k corresponding to the kernel of ρ_C in general. Moreover, we already verified (cf. Corollary 1.3) that, in the situation of Remark 1.1.3, Ω_C does *not coincide* with Ω_{J_C}, i.e.,

$$\Omega_{J_C} = k(\text{torsion points of } l\text{-power order of } J_C) \subsetneq \Omega_C.$$

(iii) If the hyperbolic curve C is of *genus zero*, then we have an explicit "*geometric description*" of Ω_C given by Anderson and Ihara as follows (cf. Theorem 1.5 below).

DEFINITION 1.4. For each algebraic extension $k' \subseteq \overline{k}$ of k, let us naturally identify $\mathbb{P}^1_k(k')$ with $k' \sqcup \{\infty\}$. Let $S, T \subseteq \mathbb{P}^1_k(\overline{k})$ be subsets of $\mathbb{P}^1_k(\overline{k})$.
(i) We shall write

$$S \overset{[l]}{\rightsquigarrow} T$$

if

$$T = \{x \in \mathbb{P}^1_k(\overline{k}) \mid x^l \in S\}$$

—where we write $\infty^l \overset{\text{def}}{=} \infty$.
(ii) Let $a, b, c \in S$ be distinct elements of S. Then we shall write

$$S \overset{[(a,b,c)]}{\rightsquigarrow} T$$

if the following condition is satisfied: If we write ϕ for the (*uniquely determined*) automorphism of $\mathbb{P}^1_{\overline{k}}$ over $\overline{k}$ such that $\phi(a) = 0$, $\phi(b) = 1$, $\phi(c) = \infty$, then

$$T = \{\phi(x) \in \mathbb{P}^1_k(\overline{k}) \mid x \in S\}.$$

(iii) Let n be a nonnegative integer. Then we shall refer to a finite chain

$$S = S_0 \overset{[*_1]}{\rightsquigarrow} S_1 \overset{[*_2]}{\rightsquigarrow} \cdots \overset{[*_{n-1}]}{\rightsquigarrow} S_{n-1} \overset{[*_n]}{\rightsquigarrow} S_n = T$$

—where, for each $i \in \{1, \dots, n\}$, "$*_i$" is either "l" (cf. (i)) or "(a, b, c)" (cf. (ii)) for distinct elements a, b, c of S_{i-1} — as a *cusp chain* (from S to T).
(iv) We shall write

$$\mathbb{S}(S)$$

for the family of subsets of $\mathbb{P}^1_k(\overline{k})$ that consists of subsets S' of $\mathbb{P}^1_k(\overline{k})$ such that there exists a cusp chain from S to S' (cf. (iii)).
(v) We shall write

$$\mathbb{U}(S) \subseteq \overline{k}^{\times}$$

for the subset of $\overline{k}^{\times}$ that consists of $a \in S' \setminus (S' \cap \{0, \infty\})$ for some $S' \in \mathbb{S}(S)$ (cf. (iv)).
(vi) We shall write

$$\mathbb{E}(S) \subseteq \overline{k}^{\times}$$

for the subgroup of $\overline{k}^{\times}$ generated by $\mathbb{U}(S) \subseteq \overline{k}^{\times}$ (cf. (v)).

Theorem 1.5 (Anderson–Ihara). *Let $S \subseteq \mathbb{P}^1_k(k)$ be a finite subset of $\mathbb{P}^1_k(k)$ such that $\{0, 1, \infty\} \subseteq S$. (Thus, one verifies easily that $\mathbb{P}^1_k \setminus S$ is a* hyperbolic curve *over k.) Then it holds that*

$$\Omega_{\mathbb{P}^1_k \setminus S} = k(\mathbb{E}(S)) = k(\mathbb{U}(S)).$$

Proof. This is a consequence of [1], Theorem B. □

DEFINITION 1.6. We shall refer to an element of $\mathbb{U}(\{0,1,\infty\})$ as a *tripod l-unit*. Thus, it follows from Theorem 1.5 that

$$\Omega_{\mathrm{tpd}_{/k}} \stackrel{\mathrm{def}}{=} \Omega_{\mathbb{P}^1_k \setminus \{0,1,\infty\}} = k(\text{tripod } l\text{-units}).$$

REMARK 1.6.1. An element of $\mathbb{E}(\{0, 1, \infty\})$ is called a *higher circular l-unit* (cf. [1], §2.6, Definition). That is to say, a higher circular l-unit is an element of $\overline{k}^{\times}$ obtained by forming a product of finitely many tripod l-units.

Lemma 1.7. *Let $S \subseteq \mathbb{P}^1_k(\overline{k})$ be a finite subset of $\mathbb{P}^1_k(\overline{k})$ such that $\{0, 1, \infty\} \subseteq S$. Then the following hold*:
(i) *Every element of $\mathbb{S}(S)$ contains $\{0, 1, \infty\}$.*
(ii) *Let $T \in \mathbb{S}(S)$ be an element of $\mathbb{S}(S)$. Then it holds that $\mathbb{S}(T) \subseteq \mathbb{S}(S)$. In particular, it holds that $\mathbb{U}(T) \subseteq \mathbb{U}(S)$, $\mathbb{E}(T) \subseteq \mathbb{E}(S)$.*
(iii) *Let $T \subseteq \mathbb{P}^1_k(\overline{k})$ be a finite subset of $\mathbb{P}^1_k(\overline{k})$ such that $S \subseteq T$. Then, for every $S' \in \mathbb{S}(S)$, there exists an element $T' \in \mathbb{S}(T)$ such that $S' \subseteq T'$. In particular, it holds that $\mathbb{U}(S) \subseteq \mathbb{U}(T)$, $\mathbb{E}(S) \subseteq \mathbb{E}(T)$.*
(iv) *For every pair $(a, T) \in \mathbb{U}(\{0, 1, \infty\}) \times \mathbb{S}(\{0, 1, \infty\})$ such that $a \notin \{0, 1, \infty\}$, there exists an element $T' \in \mathbb{S}(\{0, 1, \infty\})$ such that $T \subsetneq T'$, and, moreover, $a \in k(T' \setminus \{\infty\})$.*
(v) *Let T, $T' \in \mathbb{S}(S)$ be elements of $\mathbb{S}(S)$; $S' \subseteq \mathbb{P}^1_k(k)$ a finite subset of $\mathbb{P}^1_k(k)$ such that $T' \subseteq S' \subseteq T$. Suppose that $T \subseteq \mathbb{P}^1_k(k)$. Then it holds that $k(\mathbb{U}(S)) = k(\mathbb{U}(S'))$.*

Proof. Assertion (i) follows immediately from the various definitions involved. Next, we verify assertion (ii). Let $T' \in \mathbb{S}(T)$ be an element of $\mathbb{S}(T)$. Then, by considering the "composite" of a cusp chain from S to T and a cusp chain from T to T', it follows that $T' \in \mathbb{S}(S)$. This completes the proof of assertion (ii). Next, we verify assertion (iii). Since $S' \in \mathbb{S}(S)$, there exists a cusp chain from S to S'. Thus, since $S \subseteq T$, by considering a similar cusp chain from T to the cusp chain from S to S', we obtain an element $T' \in \mathbb{S}(T)$ such that $S' \subseteq T'$. This completes the proof of assertion (iii). Next, we verify assertion (iv). Since $a \in \mathbb{U}(\{0, 1, \infty\})$, there exists an element $S_a \in \mathbb{S}(\{0, 1, \infty\})$ such that $a \in S_a$. Moreover, since $T \in \mathbb{S}(\{0, 1, \infty\})$, there exists a cusp chain from $\{0,1,\infty\}$ to T. Thus, (since $\{0,1,\infty\} \subseteq S_a$—cf. assertion (i)), by considering a similar cusp chain from S_a to the cusp chain from $\{0,1,\infty\}$ to T, we obtain an element $T' \in \mathbb{S}(\{0, 1, \infty\})$ such that $T \subsetneq T'$ (cf. our assumption that $a \notin \{0, 1, \infty\}$, which thus implies that $\{0, 1, \infty\} \subsetneq S_a$). On the other hand, since T' is obtained by considering a cusp chain from S_a, it follows immediately from the definitions of "$\stackrel{[l]}{\rightsquigarrow}$" and "$\stackrel{[(a,b,c)]}{\rightsquigarrow}$" of Definition 1.4, (i), (ii), that $a \in S_a \subseteq k(T' \setminus \{\infty\})$. This completes the proof of assertion (iv).

Finally, we verify assertion (v). Now I claim that the following assertion holds:

Claim 1.7.A. *It holds that* $k(\mathbb{U}(S)) = k(\mathbb{U}(T))$.

Indeed, let us first observe that one verifies easily that the automorphism "ϕ" of $\mathbb{P}^1_{\overline{k}}$ in Definition 1.4, (ii), is defined over $k(a, b, c)$ (cf. also the discussion concerning "$T^{(a,b,c)}(x)$" given in [1], §2.3). Thus, it follows immediately from the *induction on the* "*length*" of a cusp chain from S to T that, to verify Claim 1.7.A, it suffices to verify Claim 1.7.A in the case where $S \overset{[l]}{\rightsquigarrow} T$. Write $\mathbb{P}^1_k \setminus T \to \mathbb{P}^1_k \setminus S$ for the connected finite étale covering given by mapping $u \mapsto u^l$, where we write u for the standard coordinate of $\mathbb{P}^1_k$. (Here, we note that it follows from assertion (i) that every element of $\mathbb{S}(S)$ contains $\{0, \infty\}$.) Then one verifies easily that this covering satisfies conditions (i), (ii), (iii), (iv), and (v) of [7], Lemma 28. Thus, it follows from [7], Lemma 28, that $\Omega_{\mathbb{P}^1_k \setminus S} = \Omega_{\mathbb{P}^1_k \setminus T}$, which implies (cf. Theorem 1.5) Claim 1.7.A. This completes the proof of Claim 1.7.A.

It follows from Claim 1.7.A that $\Omega_{\mathbb{P}^1_k \setminus S} = \Omega_{\mathbb{P}^1_k \setminus T} = \Omega_{\mathbb{P}^1_k \setminus T'}$. On the other hand, it follows from Remark 1.1.2 that $\Omega_{\mathbb{P}^1_k \setminus T'} \subseteq \Omega_{\mathbb{P}^1_k \setminus S'} \subseteq \Omega_{\mathbb{P}^1_k \setminus T}$. Thus, we conclude that $\Omega_{\mathbb{P}^1_k \setminus S} = \Omega_{\mathbb{P}^1_k \setminus S'}$, which thus implies (cf. Theorem 1.5) assertion (v). This completes the proof of assertion (v). $\square$

DEFINITION 1.8. We shall write

$$k^{\text{un-}l} \quad (\subseteq \overline{k})$$

(cf. the notation at the beginning of [6], §1) for the maximal Galois extension of k that satisfies the following conditions:

(1) The extension $k^{\text{un-}l}/k$ is *unramified* at every nonarchimedean prime of k whose residue characteristic is $\neq l$.

(2) If $\zeta_l \in \overline{k}$ is a primitive l-th root of unity, then $\zeta_l \in k^{\text{un-}l}$, and, moreover, the extension $k^{\text{un-}l}/k(\zeta_l)$ is *pro-l*.

REMARK 1.8.1. Ihara posed the following question concerning an "*arithmetic description*" of $\Omega_{\text{tpd}_{/\mathbb{Q}}}$ (cf., e.g., [11], Lecture I, §2):

(I_l): Does the equality

$$\Omega_{\text{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$$

hold?

Note that the inclusion $\Omega_{\text{tpd}_{/\mathbb{Q}}} \subseteq \mathbb{Q}^{\text{un-}l}$ was already verified. (In fact, one verifies easily from Proposition 1.2, (i), (ii), that this inclusion $\Omega_{\text{tpd}_{/\mathbb{Q}}} \subseteq \mathbb{Q}^{\text{un-}l}$ holds.) The problem (I_l) remains *unsolved* for general l. On the other hand, if l is a *regular* prime, then the problem (I_l) was answered in the *affirmative* as follows (cf. Theorem 1.9 below).

Theorem 1.9 (Brown, Sharifi). *Suppose that l is an* odd regular *prime. Then the equality*

$$\Omega_{\text{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$$

of the problem (I_l) *of* Remark 1.8.1 *holds.*

Proof. This follows immediately from the main result of [4], together with [22], Theorem 1.1. □

2. Moderate points

In the present §2, we maintain the notation of the preceding §1. In the present §2, we define and discuss the notion of an *l-moderate point* of V (cf. Definition 2.4). In particular, we prove that, for a closed point of a hyperbolic curve, the closed point is *l-moderate* if and only if the closed point satisfies the condition "$E(C,x,l)$" introduced by Matsumoto in [13], Introduction (cf. the equivalence (1) $\Leftrightarrow$ (3) of Proposition 2.5 below). Moreover, we also prove that, for a closed point of an abelian variety, the closed point is *l-moderate* if and only if the closed point is *torsion* (cf. Proposition 2.6 below). From this point of view, the notion of an *l-moderate point* of a hyperbolic curve may be regarded as an analogue of the notion of a *torsion point* of an abelian variety (cf. Remark 2.6.1, (i)).

Lemma 2.1. *There exists a* unique splitting s_V *of the natural surjection*

$$\Pi_V \times_{G_k} \mathrm{Ker}(\rho_V) \overset{\mathrm{pr}_2}{\twoheadrightarrow} \mathrm{Ker}(\rho_V)$$

that satisfies the following conditions:
(1) *The image of* s_V *is* normal *in* Π_V ($\supseteq \Pi_V \times_{G_k} \mathrm{Ker}(\rho_V)$).
(2) *If* $V = A$, *then the image of* s_A *is* contained *in the image of some* (*or*, *alternatively*, *every—cf.* (1)) *splitting of* $\Pi_A \twoheadrightarrow G_k$ *determined by the identity section of* A/k.

Proof. Lemma 2.1 in the case where $V = C$ follows immediately from [7], Lemma 4, (i), (ii), together with the well-known fact that Δ_C is *topologically finitely generated* and *center-free*. Next, we verify Lemma 2.1 in the case where $V = A$. Let us first observe that the *uniqueness* of such an s_A follows immediately from condition (2) of the statement of Lemma 2.1, together with the various definitions involved. Thus, we verify the *existence of* such an s_A. Now let us observe that the identity section of A/k gives rise to an isomorphism $\Pi_A \xrightarrow{\sim} \Delta_A \rtimes G_k$; moreover, one verifies easily that the closed subgroup $\{1\} \rtimes \mathrm{Ker}(\rho_A) \subseteq \Delta_A \rtimes G_k \xleftarrow{\sim} \Pi_A$ is *normal*. Thus, the closed subgroup $\{1\} \rtimes \mathrm{Ker}(\rho_A) \subseteq \Delta_A \rtimes G_k \xleftarrow{\sim} \Pi_A$ of Π_A gives rise to a splitting of the surjection of the statement of Lemma 2.1 that satisfies the condition in the statement of Lemma 2.1. This completes the proof of Lemma 2.1 in the case where $V = A$, hence also of Lemma 2.1. □

DEFINITION 2.2. We shall write

$$\Phi_V \overset{\mathrm{def}}{=} \Pi_V / \mathrm{Im}(s_V)$$

(cf. Lemma 2.1). Thus, we have a natural commutative diagram of profinite groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_V & \longrightarrow & \Pi_V & \longrightarrow & G_k & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_V & \longrightarrow & \Phi_V & \longrightarrow & \Gamma_V & \longrightarrow & 1 \end{array}$$

—where the horizontal sequences are *exact*, the vertical arrows are *surjective*, and the right-hand square is *cartesian*.

REMARK 2.2.1. If $V = C$, then it follows immediately from the proof of Lemma 2.1 that the quotient $\Pi_C \twoheadrightarrow \Phi_C$ defined in Definition 2.2 *coincides* with the quotient "$\Phi^{\{l\}}_{C/k}$" defined in [7], Definition 1, (iv). On the other hand, if $V = A$, then one verifies easily that the quotient $\Pi_A \twoheadrightarrow \Phi_A$ defined in Definition 2.2 does *not coincide* with the quotient "$\Phi^{\{l\}}_{A/k}$" defined in [7], Definition 1, (iv). (In fact, one verifies easily that the quotient "$\Phi^{\{l\}}_{A/k}$" defined in [7], Definition 1, (iv), *coincides* with the quotient $\Pi_A \twoheadrightarrow G_k \twoheadrightarrow \Gamma_A$.)

DEFINITION 2.3. Let $x \in V$ be a closed point of V. Then we shall write

$$\kappa(x) \subseteq \overline{k}$$

for the (necessarily *finite Galois*) extension of k obtained by forming the Galois closure over k of the residue field of V at x in $\overline{k}$.

DEFINITION 2.4. Let $x \in V$ be a closed point of V.
(1) Suppose that $x \in V$ is *k-rational*, i.e., $x \in V(k)$. Then we shall say that $x \in V$ is *l-moderate* if the splitting (that is well-defined, up to Δ_V-conjugation) of the upper exact sequence of the commutative diagram of Definition 2.2 induced by x (i.e., a pro-l Galois section of V/k arising from $x \in V(k)$—cf. [6], Definition 1.1, (ii)) arises from a splitting of the lower exact sequence of the commutative diagram of Definition 2.2.
(2) We shall say that $x \in V$ is *l-moderate* if every (necessarily *$\kappa(x)$-rational*) closed point of $V \otimes_k \kappa(x)$ arising from x is l-moderate (in the sense of (i)).

Proposition 2.5. *Let $x \in C(k)$ be a k-rational point of C. Write $U \stackrel{\text{def}}{=} C \setminus \{x\} \subseteq C$. (Thus, one verifies easily that U is a* hyperbolic curve *over k.) Then the following conditions are equivalent*:
(1) *The k-rational point $x \in C(k)$ is l*-moderate.
(2) *The natural surjection $\Gamma_U \twoheadrightarrow \Gamma_C$ (cf.* Remark 1.1.2) *is an* isomorphism, *i.e., $\Omega_C = \Omega_U$.*
(2′) *The kernel of the natural surjection $\Gamma_U \twoheadrightarrow \Gamma_C$ (cf.* Remark 1.1.2) *is* finite, *i.e., the Galois extension Ω_U/Ω_C is* finite.

(3) *The kernel of the composite*

$$G_k \to \Pi_C \to \mathrm{Aut}(\Delta_C)$$

of the splitting

$$G_k \to \Pi_C$$

(*that is well-defined, up to* Δ_C*-conjugation*) *of the upper exact sequence of the commutative diagram of* Definition 2.2 *induced by* x *and the action*

$$\Pi_C \to \mathrm{Aut}(\Delta_C)$$

obtained by conjugation coincides *with* $\mathrm{Ker}(\rho_C)$.

Proof. This follows immediately from [7], Proposition 33, (i), together with Remark 2.2.1. □

REMARK 2.5.1. In [13], Matsumoto studied a closed point of a proper hyperbolic curve over a number field that satisfies condition (3) of Proposition 2.5. The study of the present §2, as well as the study of [7], §4, is inspired by the study of [13].

Proposition 2.6. *Let* $x \in A(k)$ *be a* k*-rational point of* A*. Then the following conditions are equivalent*:
(1) *The* k*-rational point* $x \in A(k)$ *is* l-moderate.
(2) *The* k*-rational point* $x \in A(k)$ *is* torsion.

Proof. Write "H^1_{cont}" for the first continuous cohomology group and $\mathrm{Kum}\colon A(k) \to H^1_{\mathrm{cont}}(G_k, \Delta_A)$ for the pro-l Kummer homomorphism associated to A (cf., e.g., [6], Remark 1.1.4, (iii)). Consider the following condition:
(1′) The cohomology class $\mathrm{Kum}(x) \in H^1_{\mathrm{cont}}(G_k, \Delta_A)$ is *contained* in $H^1_{\mathrm{cont}}(\Gamma_A, \Delta_A) \subseteq H^1_{\mathrm{cont}}(G_k, \Delta_A)$ (cf. [19], the discussion following Corollary 2.4.2; [19], Corollary 2.7.6).
Then one verifies easily from the definition of the splitting s_A of Lemma 2.1 that the equivalence (1) $\Leftrightarrow$ (1′) holds.
Next, I claim that the following assertion holds:

Claim 2.6.A. *The cohomology group* $H^1_{\mathrm{cont}}(\Gamma_A, \Delta_A)$ *is torsion.*

Indeed, let us recall (cf. [2], [3]) that the image $\mathrm{Im}(\rho_A) \xrightarrow{\sim} \Gamma_A \subseteq \mathrm{Aut}(\Delta_A)$ of ρ_A *contains* a subgroup $J \subseteq \mathrm{Aut}(\Delta_A)$ of $\mathrm{Aut}(\Delta_A)$ that consists of *homotheties* and is isomorphic to $\mathbb{Z}_l$ as an abstract profinite group. (That is to say, J is *nontrivial* and *contained* in $1 + l\mathbb{Z}_l$ (respectively, $1 + l^2\mathbb{Z}_l$) $\subseteq \mathbb{Z}_l^\times \subseteq \mathrm{Aut}(\Delta_A)$ if l is odd (respectively, even).) Then one verifies easily that there exists a positive integer N such that, for each positive integer n, the invariant part $(\Delta_A/l^n\Delta_A)^J$ is *annihilated* by N, which implies that the kernel of the natural homomorphism $H^1_{\mathrm{cont}}(\Gamma_A, \Delta_A) \to H^1_{\mathrm{cont}}(J, \Delta_A)$ is *torsion* (cf. also [19], the discussion following Corollary 2.4.2; [19], Corollary 2.7.6). Thus, to complete the verification of Claim 2.6.A, it suffices to verify that $H^1_{\mathrm{cont}}(J, \Delta_A)$ is *torsion*. On the other hand, this follows immediately from a straightforward computation by means of the simple structure of $J \subseteq \mathrm{Aut}(\Delta_A)$. This completes the proof of Claim 2.6.A.

Next, we verify the implication (1) $\Rightarrow$ (2). Suppose that condition (1) is satisfied. Then it follows from the above equivalence (1) $\Leftrightarrow$ (1′), together with Claim 2.6.A, that $\mathrm{Kum}(x)$ is *torsion*. Thus, there exists a positive integer N such that $Nx \in \mathrm{Ker}(\mathrm{Kum})$. On the other hand, one verifies easily from the *Mordell–Weil theorem* (cf., e.g., [18], Appendix II) that the kernel $\mathrm{Ker}(\mathrm{Kum})$ is *finite*. Thus, we conclude that Nx, hence also x, is *torsion*. This completes the proof of the implication (1) $\Rightarrow$ (2).

Finally, we verify the implication (2) $\Rightarrow$ (1). Suppose that condition (2) is satisfied. Let $x_{=l}, x_{\neq l} \in A(k)$ be torsion elements of $A(k)$ such that $x_{=l}$ is of *l-power order*, $x_{\neq l}$ is of *prime-to-l order*, and $x = x_{=l} + x_{\neq l}$. Then it follows immediately that $\mathrm{Kum}(x) = \mathrm{Kum}(x_{=l})$. Moreover, since (one verifies easily that) $x_{=l}$ is *l^∞-divisible* in $A(\Omega_A)$, by considering the image of $x_{=l}$ via the pro-l Kummer homomorphism associated to $A \otimes_k \Omega_A$, we conclude that the image of $\mathrm{Kum}(x) = \mathrm{Kum}(x_{=l}) \in H^1_{\mathrm{cont}}(G_k, \Delta_A)$ in $H^1_{\mathrm{cont}}(\mathrm{Ker}(\rho_A), \Delta_A)$ *vanishes*, which implies that $\mathrm{Kum}(x) = \mathrm{Kum}(x_{=l}) \in H^1_{\mathrm{cont}}(G_k, \Delta_A)$ is *contained* in $H^1_{\mathrm{cont}}(\Gamma_A, \Delta_A) \subseteq H^1_{\mathrm{cont}}(G_k, \Delta_A)$ (cf. [19], the discussion following Corollary 2.4.2; [19], Corollary 2.7.6). Thus, it follows from the above equivalence (1) $\Leftrightarrow$ (1′) that x satisfies condition (1). This completes the proof of the implication (2) $\Rightarrow$ (1), hence also of Proposition 2.6. $\square$

REMARK 2.6.1. (i) By the equivalence given in Proposition 2.6, the notion of an *l-moderate point* of a hyperbolic curve may be regarded as an analogue of the notion of a *torsion point* of an abelian variety.

(ii) However, although (it is immediate that) the issue of whether or not a point of an abelian variety is *torsion* does *not depend* on the choice of l, the issue of whether or not a point of a hyperbolic curve is *l-moderate depends* on the choice of l (cf. Remark 2.8.1 below). A similar phenomenon to this phenomenon may be found in the analogy between the property of *not admitting complex multiplication* and the property of *being quasi-l-monodromically full* (cf. [5], Definition 2.2, (iii)). The property of *being quasi-l-monodromically full* for a hyperbolic curve may be regarded as an analogue of the property of *not admitting complex multiplication* for an elliptic curve (cf. [14], §4.1; [5], Introduction; [8], Introduction). On the other hand, in fact, although the issue of whether or not an elliptic curve admits *complex multiplication* does *not depend* on the choice of l, the issue of whether or not a hyperbolic curve is *quasi-l-monodromically full depends* on the choice of l (cf. [8], Theorem A).

REMARK 2.6.2. Let us recall from Remark 1.3.6, (i), that, in the case of abelian varieties, we have a "*tautological geometric description*" of the Galois extension Ω_A of k corresponding to the kernel of ρ_A:

$$\Omega_A = k(\text{torsion points of } l\text{-power order of } A).$$

On the other hand, as we discussed in Remark 2.6.1, (i), the notion of an *l-moderate point* of a hyperbolic curve may be regarded as an analogue of the notion of a *torsion point* of an abelian variety. Thus, one may pose the following question:

Is Ω_C generated by the coordinates of all *l-moderate points* of C? That is to say, does the equality

$$\Omega_C = k_C^{\text{mdr-}l} \stackrel{\text{def}}{=} \prod_{x \in C\,:\, l\text{-moderate}} \kappa(x)$$

hold?

The §3 focuses on the study of this question.

REMARK 2.6.3. One may expect, from the observation given in Remark 2.6.1, (i), that the following assertion holds:

Suppose that C is of *genus* ≥ 1. Let $x_1, x_2 \in C(k)$ be two k-rational *l-moderate* points of C. Write J_C for the Jacobian variety of C^{cpt}. Then the k-rational point of J_C obtained by forming the difference of x_1 and x_2 is *l-moderate*, i.e., *torsion* (cf. Proposition 2.6).

However, in general, the above assertion does *not hold* (cf. Remark 3.4.1 below).

REMARK 2.6.4. The observation given in the proof of Proposition 2.6 was related to the author by *Seidai Yasuda*.

Proposition 2.7. *Suppose that C is of* type $(1, 1)$. *Write E for the elliptic curve over k determined by the hyperbolic curve C. Then every nontrivial torsion point of E of l-power order is an l*-moderate *point of C.*

Proof. This follows immediately from [7], Proposition 40, together with the implication (3) $\Rightarrow$ (1) of Proposition 2.5. $\square$

Proposition 2.8. *Every closed point of $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$ corresponding to a* tripod l-unit *is* l-moderate.

Proof. Let $x \in \mathbb{P}^1_k \setminus \{0, 1, \infty\}$ be a closed point that corresponds to a *tripod l-unit*. Then it follows from the definition of a tripod l-unit, together with Lemma 1.7, (i), that there exists an element $T \in \mathbb{S}(\{0, 1, \infty\})$ of $\mathbb{S}(\{0, 1, \infty\})$ such that $(\{0, 1, \infty\} \subseteq)$

$\{0, 1, \infty, x\} \subseteq T$. Thus, it follows immediately from Lemma 1.7, (v), together with Theorem 1.5, that $\Omega_{\mathbb{P}^1_{k(T\setminus\{\infty\})}\setminus\{0,1,\infty\}} = \Omega_{\mathbb{P}^1_{k(T\setminus\{\infty\})}\setminus\{0,1,\infty,x\}} = \Omega_{\mathbb{P}^1_{k(T\setminus\{\infty\})}\setminus T}$. In particular, we conclude that the extension

$$\Omega_{\mathbb{P}^1_{\kappa(x)}\setminus\{0,1,\infty,x\}}/\Omega_{\mathbb{P}^1_{\kappa(x)}\setminus\{0,1,\infty\}}$$

is *finite*, which implies (cf. the implication $(2') \Rightarrow (1)$ of Proposition 2.5) that x is *l-moderate*. This completes the proof of Proposition 2.8. $\square$

REMARK 2.8.1. Let $\zeta_l \in \overline{\mathbb{Q}}$ be a primitive l-th root of unity. Then it follows from Proposition 2.8 that the ($\mathbb{Q}(\zeta_l)$-rational) closed point of $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0,1,\infty\}$ corresponding to ζ_l is *l-moderate*. On the other hand, the ($\mathbb{Q}(\zeta_l)$-rational) closed point of $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0,1,\infty\}$ corresponding to ζ_l is *not l'-moderate* for every prime number $l' \neq l$. Indeed, since (one verifies easily that) $1 - \zeta_l$ is *not a unit* at the (unique) nonarchimedean prime $\mathfrak{l}$ of $\mathbb{Q}(\zeta_l)$ whose residue characteristic is $= l$, one verifies easily that the hyperbolic curve $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0,1,\infty,\zeta_l\}$ of type $(0,4)$ over $\mathbb{Q}(\zeta_l)$ does *not admit good reduction* at $\mathfrak{l}$. Thus, it follows from Proposition 1.2, (ii), that the Galois extension "$\Omega_{\mathbb{P}^1_{\mathbb{Q}(\zeta_l)}\setminus\{0,1,\infty,\zeta_l\}}$" of $\mathbb{Q}(\zeta_l)$ that occurs in the case where we take "l" to be l' (i.e., the Galois extension of $\mathbb{Q}(\zeta_l)$ corresponding to the kernel of the *pro-l'* outer Galois representation associated to $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0, 1, \infty, \zeta_l\}$) is *ramified* at $\mathfrak{l}$. On the other hand, since (one verifies easily again from Proposition 1.2, (ii), that] the Galois extension "$\Omega_{\mathbb{P}^1_{\mathbb{Q}(\zeta_l)}\setminus\{0,1,\infty\}}$" of $\mathbb{Q}(\zeta_l)$ that occurs in the case where we take "l" to be l' (i.e., the Galois extension of $\mathbb{Q}(\zeta_l)$ corresponding to the kernel of the *pro-l'* outer Galois representation associated to $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0, 1, \infty\}$) is *unramified* at $\mathfrak{l}$, it follows from the equivalence $(1) \Leftrightarrow (2)$ of Proposition 2.5 that the ($\mathbb{Q}(\zeta_l)$-rational) closed point of $\mathbb{P}^1_{\mathbb{Q}(\zeta_l)} \setminus \{0,1,\infty\}$ corresponding to ζ_l is *not l'-moderate*. Thus, we conclude that

the issue of whether or not a given closed point of a hyperbolic curve is *l-moderate depends* on the choice of l.

REMARK 2.8.2. Let us observe that the examples of *moderate closed points* given in Proposition 2.7 (respectively, Proposition 2.8) arises from a sort of the *elliptic* (respectively, *Belyĭ*) *cuspidalization* discussed in [17], §3.

3. Kernels of pro-l outer Galois representations and moderate points

In the present §3, we maintain the notation of the preceding §2. In the present §3, we discuss the relationship between the Galois extension of k corresponding to the *kernel of the pro-l outer Galois representation* associated to C and *l-moderate points* of C. More concretely, we study the question posed in Remark 2.6.2: Does the equality

$$\Omega_C = k_C^{\text{mdr-}l} \stackrel{\text{def}}{=} \prod_{x\in C:\ l\text{-moderate}} \kappa(x)$$

hold?

Theorem 3.1. *Every l*-moderate *point of C is* defined *over Ω_C, i.e.,*

$$k_C^{\text{mdr-}l} \subseteq \Omega_C.$$

Proof. Let $x \in C$ be an *l-moderate* closed point of C. Let us first observe that, by replacing k by the (necessarily *finite Galois*) extension of k corresponding to the image of the composite $G_{\kappa(x)} \hookrightarrow G_k \twoheadrightarrow \Gamma_C$ (note that this extension of k is *contained* in Ω_C), we may assume without loss of generality that the composite $G_{\kappa(x)} \hookrightarrow G_k \twoheadrightarrow \Gamma_C$ is *surjective*. Then one verifies easily that the natural morphism $C \otimes_k \kappa(x) \stackrel{\text{pr}_1}{\to} C$ induces a commutative diagram of profinite groups

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \Delta_{C\otimes_k\kappa(x)} & \longrightarrow & \Phi_{C\otimes_k\kappa(x)} & \longrightarrow & \Gamma_{C\otimes_k\kappa(x)} & \longrightarrow & 1 \\
 & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\
1 & \longrightarrow & \Delta_C & \longrightarrow & \Phi_C & \longrightarrow & \Gamma_C & \longrightarrow & 1
\end{array}$$

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

Next, let us observe that it follows immediately from the definition of an l-moderate point that the l-moderate closed point x of C induces a splitting of the upper horizontal sequence of the above commutative diagram. Thus, since the vertical arrows of the above commutative diagram are *isomorphisms*, we obtain a splitting of the lower horizontal sequence of the above commutative diagram. In particular, since the right-hand square of the commutative diagram of Definition 2.2 is *cartesian*, we obtain a splitting s of the upper horizontal sequence of the commutative diagram of Definition 2.2 in the case where $V = C$, i.e., a *pro-l Galois section s* of C/k (cf. [6], Definition 1.1, (i)).

Next, let us observe that it follows immediately from the definition of s that the restriction of s to $G_{\kappa(x)} \subseteq G_k$ *coincides* with a pro-l Galois section of $C \otimes_k \kappa(x)/\kappa(x)$ arising from a $\kappa(x)$-rational closed point of $C \otimes_k \kappa(x)$ (that arises from x), i.e., the restriction of s to $G_{\kappa(x)} \subseteq G_k$ is *geometric* (cf. [6], Definition 1.1, (iii)). Thus, it follows from the implication (2) $\Rightarrow$ (1) of [9], Lemma 1.5, that s is *geometric*. Let $y \in C^{\text{cpt}}(k)$ be a k-rational point of C^{cpt} such that the image of s is contained in a decomposition subgroup of Π_C associated to $y \in C^{\text{cpt}}(k)$. Then it follows from [9], Lemma 1.4, together with the definitions of s and y, that $x = y$. In particular, we conclude that $\kappa(x) = k \subseteq \Omega_C$. This completes the proof of Theorem 3.1. $\square$

REMARK 3.1.1. (i) Consider the following conditions:
(1) The equality $\Omega_C = k_C^{\text{mdr-}l}$ holds.
(1′) The inclusion $\Omega_C \subseteq k_C^{\text{mdr-}l}$ holds.
(2) The extension Ω_C of $k_C^{\text{mdr-}l}$ (cf. Theorem 3.1) is *finite*.
(3) There are *infinitely many l-moderate* points of C.
(4) There is an *l-moderate* point of C.

Then we have an equivalence and implications

$$(1) \Longleftrightarrow (1') \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (4).$$

Indeed, the equivalence (1) $\Leftrightarrow$ (1′) follows from Theorem 3.1. The implication (1) $\Rightarrow$ (2) is immediate. The implication (2) $\Rightarrow$ (3) follows immediately from the (easily verified) fact that the Galois extension Ω_C/k is *infinite*. The implication (3) $\Rightarrow$ (4) is immediate.

(ii) The discussion given in (i) leads naturally to the following observation concerning the study of *rational points of hyperbolic curves*:

Suppose that condition (4) of (i) holds (e.g., condition (1) of (i) holds). Write k_C^0 ($\subseteq \overline{k}$) for the finite Galois extension of k corresponding to the kernel of the composite

$$G_k \stackrel{\rho_C}{\to} \mathrm{Out}(\Delta_C) \to \mathrm{Aut}(\Delta_C^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l)$$

and ($k_C^0 \subseteq$) $(k_C^0)^{\text{pro-}l} \subseteq (k_C^0)^{\mathrm{nilp}} \subseteq (k_C^0)^{\mathrm{solv}}$ ($\subseteq \overline{k}$) for the maximal pro-l, nilpotent, solvable Galois extensions of k_C^0, respectively. Then

$$C((k_C^0)^{\text{pro-}l}),$$

hence also

$$C((k_C^0)^{\mathrm{nilp}}) \quad \text{and} \quad C((k_C^0)^{\mathrm{solv}}),$$

is *nonempty*. In particular, if the above displayed composite is *trivial*, then it holds that

$$C(k^{\text{pro-}l}), C(k^{\mathrm{nilp}}), C(k^{\mathrm{solv}}) \neq \emptyset.$$

Indeed, this follows immediately from Theorem 3.1, together with Proposition 1.2, (i).

REMARK 3.1.2. The observation given in the discussion of Remark 3.1.1 was related to the author by *Akio Tamagawa*.

Corollary 3.2. *Let $X \to C$ be a connected finite étale covering of C that arises from an open subgroup of Π_C. Suppose that X is a* hyperbolic curve *over k (i.e., X is* geometrically connected *over k). Then the following hold*:

(i) *Let $x \in X$ be a closed point of X. Write $c \in C$ for the closed point of C obtained by forming the image of x via the covering $X \to C$. Then it holds that x is l-*moderate *if and only if c is l-*moderate. *Moreover, in this case, it holds that*

$$\Omega_C \cdot \kappa(x) = \Omega_X.$$

*In particular, if there exists an l-*moderate *closed point of X* defined *over Ω_C, then it holds that*

$$\Omega_C = \Omega_X.$$

(ii) *We have natural inclusions of fields*

$$\begin{array}{ccc} k_C^{\text{mdr-}l} & \subset & k_X^{\text{mdr-}l} \\ \cap & & \cap \\ \Omega_C & \subset & \Omega_X. \end{array}$$

Moreover, the extension Ω_X/Ω_C (*determined by the lower horizontal inclusion*) *is* finite.
(iii) *Suppose that the extension*

$$\Omega_C/k_C^{\text{mdr-}l}$$

(*cf.* Theorem 3.1) *is* finite (*e.g., C is isomorphic to* $\mathbb{P}_k^1 \setminus \{0, 1, \infty\}$—*cf.* Corollary 3.3 *below*). *Then the two extensions*

$$\Omega_X/k_X^{\text{mdr-}l},$$
$$k_X^{\text{mdr-}l}/k_C^{\text{mdr-}l}$$

(*cf.* (ii)) *are* finite.

Proof. First, we verify assertion (i). Let us first observe that it follows immediately from the equivalence (1) $\Leftrightarrow$ (2$'$) of Proposition 2.5, together with Theorem 3.1, that, to verify assertion (i), by replacing k by $\kappa(x)$, we may assume without loss of generality that $x \in X(k)$, $c \in C(k)$. Thus, assertion (i) follows from [7], Proposition 35, together with the implication (3) $\Rightarrow$ (1) of Proposition 2.5. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us first observe that, by considering the closed points of X that lie over the *l-moderate* closed points of C, we conclude immediately from assertion (i) that

$$k_C^{\text{mdr-}l} \subseteq k_X^{\text{mdr-}l}.$$

On the other hand, it follows from [7], Proposition 25, (i), that we have an inclusion $\Omega_C \subseteq \Omega_X$, and, moreover, the extension Ω_X/Ω_C is *finite*. Thus, assertion (ii) follows immediately from Theorem 3.1. This completes the proof of assertion (ii). Assertion (iii) follows immediately from the various definitions involved, together with assertion (ii). This completes the proof of Corollary 3.2. $\square$

Corollary 3.3. *Let* $S \in \mathbb{S}(\{0, 1, \infty\})$ *be an element of* $\mathbb{S}(\{0, 1, \infty\})$ *such that* $S \setminus \{\infty\} \subseteq k$. *Then it holds that*

$$\Omega_{\mathbb{P}_k^1 \setminus S} = k_{\mathbb{P}_k^1 \setminus S}^{\text{mdr-}l}.$$

In particular, the equality

$$\Omega_{\text{tpd}_{/k}} \stackrel{\text{def}}{=} \Omega_{\mathbb{P}_k^1 \setminus \{0,1,\infty\}} = k_{\mathbb{P}_k^1 \setminus \{0,1,\infty\}}^{\text{mdr-}l}$$

holds.

Proof. It follows from Theorem 3.1 that, to verify Corollary 3.3, it suffices to verify that $\Omega_{\mathbb{P}^1_k \setminus S} \subseteq k^{\text{mdr-}l}_{\mathbb{P}^1_k \setminus S}$. On the other hand, it follows immediately from Lemma 1.7, (v), together with Theorem 1.5 and the equality of Definition 1.6, that $\Omega_{\mathbb{P}^1_k \setminus S}$ is *generated by the tripod l-units*. Thus, to verify Corollary 3.3, it suffices to verify that, for each tripod l-unit $a \in \overline{k} \setminus \{0, 1\}$, it holds that $a \in k^{\text{mdr-}l}_{\mathbb{P}^1_k \setminus S}$. To this end, let us recall from Lemma 1.7, (iv), that there exists an element $T \in \mathbb{S}(\{0, 1, \infty\})$ such that $S \subsetneq T$, and, moreover, $a \in k(T \setminus \{\infty\})$. Let $a' \in T \setminus S$. Then since $S \subseteq S \sqcup \{a'\} \subseteq T$, it follows immediately from Lemma 1.7, (v), that $k(T \setminus \{\infty\}, \mathbb{U}(S)) = k(T \setminus \{\infty\}, \mathbb{U}(S \sqcup \{a'\}))$. Thus, it follows from Theorem 1.5, together with the equivalence (1) $\Leftrightarrow$ (2$'$) of Proposition 2.5, that the closed point of $\mathbb{P}^1_k \setminus S$ corresponding to $a' \in \overline{k}$ is *l-moderate*. In particular, since $a \in k(T \setminus \{\infty\}) = k(T \setminus S)$ (cf. our assumption that $S \setminus \{\infty\} \subseteq k$), we conclude that $a \in k^{\text{mdr-}l}_{\mathbb{P}^1_k \setminus S}$. This completes the proof of Corollary 3.3. $\square$

EXAMPLE 3.4. Theorem 3.1 and Corollary 3.2 give us other examples of hyperbolic curves X over k for which the equality

$$\Omega_X = k^{\text{mdr-}l}_X$$

holds as follows:

(i) Suppose that l is *odd*. Let n be a positive integer. Write

$$X \stackrel{\text{def}}{=} \operatorname{Spec}(k[s, t]/(s^{l^n} + t^{l^n} + 1))$$

—where s and t are indeterminates. Then the equalities

$$\Omega_{\text{tpd}_{/k}} = \Omega_X = k^{\text{mdr-}l}_X$$

hold. Indeed, let us consider the connected finite étale covering $X \to \mathbb{P}^1_k \setminus \{0, 1, \infty\}$ given by mapping $u \mapsto s^{l^n}$ (where we write u for the standard coordinate of $\mathbb{P}^1_k$). Then one verifies easily that this covering arises from an open subgroup of $\Pi_{\mathbb{P}^1_k \setminus \{0,1,\infty\}}$. Moreover, one verifies immediately that every closed point of X that lies (relative to this covering) over the closed point of $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$ corresponding to a *tripod l-unit* is *defined over k*(tripod l-units). Thus, since such a closed point of $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$ is *l-moderate* (cf. Proposition 2.8), and

$$k(\text{tripod } l\text{-units}) = \Omega_{\text{tpd}_{/k}}$$

(cf. Definition 1.6), it follows immediately from Corollary 3.2, (i), (ii), that the equality

$$\Omega_{\text{tpd}_{/k}} = \Omega_X$$

and the inclusion

$$\Omega_{\text{tpd}_{/k}} \subseteq k^{\text{mdr-}l}_X$$

hold. In particular, it follows from Theorem 3.1 that the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-}l}$$

hold.
(ii) Let n be a positive integer. Suppose that l is *odd*, and that $(l, n) \neq (3, 1)$. Write

$$X \stackrel{\mathrm{def}}{=} \mathrm{Proj}(k[s, t, u]/(s^{l^n} + t^{l^n} + u^{l^n}))$$

—where s, t, and u are indeterminates. Then the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-}l}$$

hold. Indeed, by considering the open subscheme $U \subseteq X$ of X given by "X" of (i), we conclude from (i), together with Remark 1.1.2; Proposition 1.2, (vi), that the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = \Omega_U$$

hold. Moreover, let us observe that if a closed point $x \in X$ of X lies on the open subscheme $U \subseteq X$ (i.e., given by "X" of (i)) and is *l-moderate* as a closed point of U, then it follows from the equivalence (1) $\Leftrightarrow$ (2) of Proposition 2.5 that $\Omega_U = \Omega_{U\setminus\{x\}}$; thus, it follows immediately from Remark 1.1.2 that $\Omega_X = \Omega_{X\setminus\{x\}}$, i.e., $x \in X$ is *l-moderate* as a closed point of X (cf. the equivalence (1) $\Leftrightarrow$ (2) of Proposition 2.5). In particular, it follows that the inclusion

$$k_U^{\text{mdr-}l} \subseteq k_X^{\text{mdr-}l},$$

hence (cf. (i); Theorem 3.1) also the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-}l}$$

hold.
(iii) Suppose that $l = 3$, and that a primitive cube root of unity is contained in k. Write X for the *modular curve* $Y(3)$ *parametrizing elliptic curves with* $\Gamma(3)$*-structures* (cf., e.g., [12]) over k. Then the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-}3}$$

hold. Indeed, as is well-known, if $\zeta_3 \in k$ is a primitive cube root of unity, then there exists an isomorphism over k

$$X \simeq \mathbb{P}_k^1 \setminus \{1, \zeta_3, \zeta_3^2, \infty\}.$$

Thus, since (one verifies easily that) $\{0, 1, \zeta_3, \zeta_3^2, \infty\} \in \mathbb{S}(\{0, 1, \infty\})$, it follows immediately from Lemma 1.7, (v), together with Remark 1.1.2; Proposition 1.2, (vi); Theorem 1.5, that the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = \Omega_{\mathbb{P}_k^1\setminus\{0,1,\zeta_3,\zeta_3^2,\infty\}}$$

hold. Let $a \in \overline{k} \setminus \{0, 1\}$ be a *tripod* 3-*unit*; write $x \in X \simeq \mathbb{P}^1_k \setminus \{1, \zeta_3, \zeta_3^2, \infty\}$ for the closed point of X corresponding to $a^{1/3}$. (Note that it follows immediately from the definition of a tripod l-unit that $a^{1/3}$ is a tripod 3-unit.) Then, by considering the connected finite étale covering $\mathbb{P}^1_k \setminus \{0, 1, \zeta_3, \zeta_3^2, \infty\} \to \mathbb{P}^1_k \setminus \{0, 1, \infty\}$ given by mapping $u \mapsto u^3$ (where we write u for the standard coordinate of $\mathbb{P}^1_k$), we conclude from Corollary 3.2, (i), together with Proposition 2.8, that $x \in X \simeq \mathbb{P}^1_k \setminus \{1, \zeta_3, \zeta_3^2, \infty\}$ is 3-*moderate* as a closed point of $\mathbb{P}^1_k \setminus \{0, 1, \zeta_3, \zeta_3^2, \infty\}$. In particular, it follows immediately from a similar argument to the argument applied in (ii) (concerning "$x \in X$" of (ii)) that x is 3-*moderate* as a closed point of X. Thus, it follows that

$$a^{1/3} \in k_X^{\text{mdr-3}},$$

which thus implies (cf. the equality of Definition 1.6) that

$$\Omega_{\text{tpd}_{/k}} \subseteq k_X^{\text{mdr-3}}.$$

In particular, it follows from Theorem 3.1 that the equalities

$$\Omega_{\text{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-3}}$$

hold.

(iv) Let n be a positive integer. Suppose that $l = 3$, and that a primitive 3^n-th root of unity is contained in k. Write X for the *modular curve* $Y(3^n)$ *parametrizing elliptic curves with* $\Gamma(3^n)$-*structures* (cf., e.g., [12]) over k. Then the equalities

$$\Omega_{\text{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-3}}$$

hold. Indeed, let us first observe that it is immediate that, to verify the equalities under consideration, we may assume without loss of generality that $k = \mathbb{Q}(\zeta_{3^n})$, where $\zeta_{3^n} \in \overline{k}$ is a primitive 3^n-th root of unity. Let $a \in \overline{k} \setminus \{0, 1\}$ be a *tripod* 3-*unit*. Write $x \in Y(3) \simeq \mathbb{P}^1_k \setminus \{1, \zeta_3, \zeta_3^2, \infty\}$ (cf. (iii)) for the closed point of $Y(3)$ corresponding to $a^{1/3}$ and E_x for the elliptic curve over $k(a^{1/3})$ determined by the closed point $x \in Y(3)$. Then it follows from the discussion given in (iii) that the closed point $x \in Y(3)$ is 3-*moderate*. In particular, it follows immediately from the equivalence (1) $\Leftrightarrow$ (2) of Proposition 2.5, together with Proposition 1.2, (ii), that the elliptic curve E_x admits *good reduction* at every nonarchimedean prime of $k(a^{1/3})$ whose residue characteristic is $\neq 3$. Thus, in light of $k(a^{1/3}) \subseteq \Omega_{\text{tpd}_{/k}} = k^{\text{un-3}}$ (cf. Definition 1.6; Theorem 1.9), since every torsion point of E_x of order 3 is $k(a^{1/3})$-*rational*, and the kernel of the natural homomorphism $\mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{F}_3)$ is *pro*-3, it follows immediately from the definition of $k^{\text{un-3}}$, together with Proposition 1.2, (i), (ii), that every torsion point of E_x of 3-power order is *defined over* $\Omega_{\text{tpd}_{/k}} = k^{\text{un-3}}$. In particular, every closed point of X that lies, relative to the finite étale covering $X \to Y(3)$ arising from the natural inclusion $\Gamma(3^n) \hookrightarrow \Gamma(3)$ (which corresponds to an open subgroup of $\Pi_{Y(3)}$), over $x \in$

$Y(3)$ is *defined over* $\Omega_{\mathrm{tpd}_{/k}} = k^{\text{un-3}}$. Thus, it follows immediately from Corollary 3.2, (i), together with (iii), that the equality

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X$$

and (by allowing to *vary* a) the inclusion

$$\Omega_{\mathrm{tpd}_{/k}} \subseteq k_X^{\text{mdr-3}}$$

hold. Thus, it follows from Theorem 3.1 that the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-3}}$$

hold.
(v) Let $n \geq 2$ be an integer. Suppose that $l = 3$, and that a primitive 3^n-th root of unity is contained in k. Write X for the smooth compactification $X(3^n)$ of the modular curve $Y(3^n)$ of (iv). Then the equalities

$$\Omega_{\mathrm{tpd}_{/k}} = \Omega_X = k_X^{\text{mdr-3}}$$

hold. Indeed, in light of (iv), this follows immediately from a similar argument to the argument applied in (ii) (by replacing (i) by (iv)).

REMARK 3.4.1. It follows from Example 3.4, (ii), that if $l \geq 5$, then the proper hyperbolic curve X over $\mathbb{Q}$ defined by the homogeneous equation "$x^l + y^l + z^l$" satisfies condition (1) of Remark 3.1.1, (i). In particular, it follows from the implication (1) $\Rightarrow$ (3) of Remark 3.1.1, (i), that X admits *infinitely many l-moderate points*. Thus, it follows immediately from the *finiteness result* of [20], Théorème 1, that the assertion given in Remark 2.6.3 does *not hold*.

Lemma 3.5. *Suppose that the following two conditions are satisfied*:
(1) *The equality*

$$\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$$

of the problem (I_l) *of* Remark 1.8.1 *holds* (*e.g.*, l *is an* odd regular *prime—cf.* Theorem 1.9).
(2) $k \subseteq \Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$.
Then the following hold:
(i) *The equality*

$$\Omega_C = \Omega_{\mathrm{tpd}_{/\mathbb{Q}}}$$

holds if and only if the following condition is satisfied:

($\dagger$): *The hyperbolic curve C admits* good reduction *at every nonarchimedean prime of k whose residue characteristic is $\neq l$, and, moreover, if $\zeta_l \in \overline{k}$ is a primitive l-th root of unity, then the restriction to $G_{k(\zeta_l)} \subseteq G_k$ of the composite*

$$G_k \stackrel{\rho_C}{\to} \mathrm{Out}(\Delta_C) \to \mathrm{Aut}(\Delta_C^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l)$$

factors *through a pro-l quotient of $G_{k(\zeta_l)}$.*

(ii) *Suppose, moreover, that the equality*

$$\Omega_C = \Omega_{\mathrm{tpd}_{/\mathbb{Q}}}$$

holds, and that the hyperbolic curve C is proper *over k. Let $x \in C(k)$ be a k-rational point of C. Then the equalities*

$$\Omega_C = \Omega_{C \setminus \{x\}} = \Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$$

hold.

(iii) *In the situation of* (ii), *for a closed point of C, it holds that the closed point is* l-moderate *if and only if the closed point is* defined *over $\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$. In particular, it holds that*

$$\{l\text{-}\textit{moderate closed points of } C\} = C(\mathbb{Q}^{\text{un-}l}).$$

Proof. First, we verify assertion (i). The *necessity* follows immediately from Proposition 1.2, (ii), together with the definition of $\mathbb{Q}^{\text{un-}l}$. To verify the *sufficiency*, let us observe that if the condition ($\dagger$) holds, then it follows immediately from Proposition 1.2, (i), (ii), together with the definition of $\mathbb{Q}^{\text{un-}l}$, that the inclusion $\Omega_C \subseteq \mathbb{Q}^{\text{un-}l}$ holds, which thus implies (cf. condition (1)) that $\Omega_C \subseteq \Omega_{\mathrm{tpd}_{/k}}$. Thus, the *sufficiency* follows from Proposition 1.2, (vi). This completes the proof of assertion (i).

Next, we verify assertion (ii). It follows from assertion (i) that, to verify assertion (ii), it suffices to verify that the hyperbolic curve $C \setminus \{x\}$ satisfies the condition ($\dagger$). On the other hand, again by assertion (i), the hyperbolic curve C satisfies the condition ($\dagger$). Thus, one verifies easily that the hyperbolic curve $C \setminus \{x\}$ satisfies the condition ($\dagger$). This completes the proof of assertion (ii). Assertion (iii) follows immediately from Theorem 3.1, together with assertion (ii). This completes the proof of Lemma 3.5. $\square$

REMARK 3.5.1. Suppose that conditions (1) and (2) in the statement of Lemma 3.5 hold. Then it follows from Lemma 3.5, (iii), together with Example 3.4, (ii) (respectively, Example 3.4, (v)), that the proper hyperbolic curve "X" of Example 3.4, (ii) (respectively, Example 3.4, (v)), satisfies the equality

$$\{l\text{-moderate closed points of } X\} = X(\mathbb{Q}^{\text{un-}l}).$$

Corollary 3.6. *Suppose that* $l \geq 5$, *and that the equality*

$$\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$$

of the problem (I_l) *of* Remark 1.8.1 *holds* (*e.g.*, l *is a* regular *prime—cf.* Theorem 1.9). *Let* a, $b \in \Omega_{\mathrm{tpd}_{/\mathbb{Q}}} \setminus \{0, 1\} = \mathbb{Q}^{\text{un-}l} \setminus \{0, 1\}$ *be elements of* $\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} \setminus \{0, 1\} = \mathbb{Q}^{\text{un-}l} \setminus \{0, 1\}$ *such that*

$$a^l + b^l = 1.$$

Then the hyperbolic curve of type $(0, 4)$ *over* $\mathbb{Q}(a^l)$

$$\mathbb{P}^1_{\mathbb{Q}(a^l)} \setminus \{0, 1, \infty, a^l\}$$

is not quasi-l-monodromically full (*cf.* [5], Definition 2.2, (iii)), *i.e.*, *if we write* $k \stackrel{\text{def}}{=} \mathbb{Q}(a^l)$ *and* $C \stackrel{\text{def}}{=} \mathbb{P}^1_{\mathbb{Q}(a^l)} \setminus \{0, 1, \infty\}$, *then the image of the composite*

$$G_k \to \Pi_C \twoheadrightarrow \Phi_C$$

—where the first arrow is the splitting (*that is well-defined, up to* Δ_C*-conjugation*) *of the upper exact sequence of the commutative diagram of* Definition 2.2 *induced by the* k*-rational point of* C *determined by* a^l, *and the second arrow is the natural surjection defined in* Definition 2.2*—is* not open (*cf.* Remark 2.2.1; [7], Remark 11, (ii); [7], Proposition 19, (iv)).

Proof. Write X for the proper hyperbolic curve of Example 3.4, (ii), in the case where $(k, n) = (\mathbb{Q}, 1)$; $U \subseteq X$ for the open subscheme of X given by "X" of Example 3.4, (i), in the case where $(k, n) = (\mathbb{Q}, 1)$; $x \in U$ for the ($\Omega_{\mathrm{tpd}_{/\mathbb{Q}}}$-rational) closed point of U corresponding to the pair (a, b) in the statement of Corollary 3.6. Then it follows from Remark 3.5.1 that x is *l-moderate* as a closed point of X. In particular, it follows immediately from the equivalence (1) $\Leftrightarrow$ (3) of Proposition 2.5, together with [7], Proposition 33, (ii), that x is *not quasi-l-monodromically full* (cf. [7], Definition 8) as a closed point of X, hence (cf. [7], Proposition 24, (i)) also U. Thus, by considering the connected finite étale covering $U \to \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ given by mapping $u \mapsto s^l$ (where we write u for the standard coordinate of $\mathbb{P}^1_{\mathbb{Q}}$), we conclude from [7], Proposition 27, (ii), that the closed point of $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ corresponding to a^l is *not quasi-l-monodromically full*. In particular, it follows immediately from [7], Remark 11, (ii), that the hyperbolic curve $\mathbb{P}^1_{\mathbb{Q}(a^l)} \setminus \{0, 1, \infty, a^l\}$ of type $(0, 4)$ over $\mathbb{Q}(a^l)$ is *not quasi-l-monodromically full*. This completes the proof of Corollary 3.6. $\square$

REMARK 3.6.1. Corollary 3.6 leads naturally to the following observation which may be regarded as a "*conditional proof*" of *Fermat's last theorem*:

Suppose that the following two assertions hold:

(1) The equality $\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} = \mathbb{Q}^{\text{un-}l}$ of the problem (I_l) of Remark 1.8.1 holds for every prime number l.

(2) The problem of Matsumoto and Tamagawa given as [14], Problem 4.1, is answered in the *affirmative*. (In particular, the equivalence $(\mathrm{MT}_1) \Leftrightarrow (\mathrm{MT}_2)$ of [8], Introduction, holds.)

Let $l \geq 5$ be a prime number and $a, b \in \Omega_{\mathrm{tpd}_{/\mathbb{Q}}} \setminus \{0,1\} = \mathbb{Q}^{\text{un-}l} \setminus \{0,1\}$ elements of $\Omega_{\mathrm{tpd}_{/\mathbb{Q}}} \setminus \{0, 1\} = \mathbb{Q}^{\text{un-}l} \setminus \{0, 1\}$ such that

$$a^l + b^l = 1.$$

Then it follows from Corollary 3.6 that the hyperbolic curve of type (0, 4) over $\mathbb{Q}(a^l)$

$$X \stackrel{\text{def}}{=} \mathbb{P}^1_{\mathbb{Q}(a^l)} \setminus \{0, 1, \infty, a^l\}$$

is *not quasi-l-monodromically full*. Thus, it follows from our assumption that the equivalence $(\mathrm{MT}_1) \Leftrightarrow (\mathrm{MT}_2)$ of [8], Introduction, holds that X is *not quasi-l'-monodromically full* for every prime number l'. In particular, it follows immediately from [5], Corollary 7.11, that one of the elements of the set

$$\{a^l, b^l, -(a/b)^l, a^{-l}, b^{-l}, -(a/b)^{-l}\},$$

hence also one of the elements of the set

$$\{a, b, a/b\},$$

is a *unit* (in the ring of integers of $\overline{\mathbb{Q}}$).

Thus, one verifies easily that, for instance, every pair (a, b) of *nonzero rational numbers* does *not satisfy* the equality

$$a^l + b^l = 1.$$

On the other hand, however, the author answered the problem of Matsumoto and Tamagawa given as [14], Problem 4.1, in the *negative* in [8] (cf. [8], Theorem A). The above observation is one of the main motivations of studying the problem of Matsumoto and Tamagawa in [8].

ACKNOWLEDGMENTS. The author would like to thank *Naotake Takao*, *Akio Tamagawa*, and *Seidai Yasuda* for helpful comments and discussions. In particular, the author would like to thank *Akio Tamagawa* for a comment concerning the content of Remark 3.1.1; *Seidai Yasuda* for a discussion concerning the proof of Proposition 2.6. The present paper is based on talks by the author given at Research Institute for Mathematical Sciences in Kyoto University (May, 2011), Osaka University (November, 2011), and

Waseda University (January, 2012). The author would like to thank the organizers for giving me the opportunity for the talks. This research was supported by Grant-in-Aid for Scientific Research (C), No. 24540016, Japan Society for the Promotion of Science.

References

[1] G. Anderson and Y. Ihara: *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), 271–293.

[2] F.A. Bogomolov: *Sur l'algébricité des représentations l-adiques*, C.R. Acad. Sci. Paris Sér. A-B **290** (1980), A701–A703.

[3] F.A. Bogomolov: *Points of finite order on abelian varieties*, Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), 782–804, 973.

[4] F. Brown: *Mixed Tate motives over* $\mathbb{Z}$, Ann. of Math. (2) **175** (2012), 949–976.

[5] Y. Hoshi: *Galois-theoretic characterization of isomorphism classes of monodromically full hyperbolic curves of genus zero*, Nagoya Math. J. **203** (2011), 47–100.

[6] Y. Hoshi: *Existence of nongeometric pro-p Galois sections of hyperbolic curves*, Publ. Res. Inst. Math. Sci. **46** (2010), 829–848.

[7] Y. Hoshi: *On monodromically full points of configuration spaces of hyperbolic curves*; in The Arithmetic of Fundamental Groups—PIA 2010, Contrib. Math. Comput. Sci. **2**, Springer, Heidelberg, 2012, 167–207.

[8] Y. Hoshi: *On a problem of Matsumoto and Tamagawa concerning monodromic fullness of hyperbolic curves*: *genus zero case*, Tohoku Math. J. (2) **65** (2013), 231–242.

[9] Y. Hoshi: *Conditional results on the birational section conjecture over small number fields*, to appear in the Proceedings for Symposium in Durham (July 2011) "Automorphic Forms and Galois Representations".

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

[11] Y. Ihara: *Some arithmetic aspects of Galois actions in the pro-p fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$; in Arithmetic Fundamental Groups and Noncommutative Algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, RI, 2002, 247–273.

[12] N.M. Katz and B. Mazur: Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies **108**, Princeton Univ. Press, Princeton, NJ, 1985.

[13] M. Matsumoto: *Difference between Galois representations in automorphism and outer-automorphism groups of a fundamental group*, Proc. Amer. Math. Soc. **139** (2011), 1215–1220.

[14] M. Matsumoto and A. Tamagawa: *Mapping-class-group action versus Galois action on profinite fundamental groups*, Amer. J. Math. **122** (2000), 1017–1026.

[15] J.S. Milne: *Jacobian varieties*; in Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, 167–212.

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

[17] S. Mochizuki: *Topics in absolute anabelian geometry* II: *decomposition groups and endomorphisms*, J. Math. Sci. Univ. Tokyo **20** (2013), 171–269.

[18] D. Mumford: Abelian Varieties, corrected reprint of the second (1974) edition, Tata Institute of Fundamental Research Studies in Mathematics **5**, Published for the Tata Institute of Fundamental Research, Bombay, 2008.

[19] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of Number Fields, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2008.

[20] M. Raynaud: *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207–233.

[21] J.-P. Serre and J. Tate: *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[22] R.T. Sharifi: *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*; in Arithmetic Fundamental Groups and Noncommutative Algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, RI, 2002, 275–284.

[23] N. Takao: *Braid monodromies on proper curves and pro-l Galois representations*, J. Inst. Math. Jussieu **11** (2012), 161–181.

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

[25] Revêtements étales et Groupe Fondamental (SGA 1), Documents Mathématiques (Paris) **3**, Soc. Math. France, Paris, 2003.

Research Institute for Mathematical Sciences
Kyoto University
Kyoto 606-8502
Japan
e-mail: yuichiro@kurims.kyoto-u.ac.jp