Hokkaido Mathematical Journal Vol. 45 (2016) p. 271–291

Finiteness of the Moderate Rational Points of Once-punctured Elliptic Curves

Yuichiro Hoshi

(Received February 28, 2014; Revised June 12, 2014)

Abstract. In the present paper, we prove the *finiteness* of the set of *moderate* rational points of a once-punctured elliptic curve over a number field. This *finiteness* may be regarded as an analogue for a once-punctured elliptic curve of the well-known *finiteness* of the set of torsion rational points of an abelian variety over a number field. In order to obtain the *finiteness*, we discuss the *center* of the image of the pro-l outer Galois action associated to a hyperbolic curve. In particular, we give, under the assumption that l is *odd*, a *necessary and sufficient condition* for a certain hyperbolic curve over a generalized sub-l-adic field to have *trivial center*.

Key words: moderate point, once-punctured elliptic curve, hyperbolic curve, Galois-like automorphism.

Introduction

In the present paper, we discuss the *finiteness* of the set of *moderate* rational points of a hyperbolic curve over a number field. First, let us review the notion of a *moderate point* of a hyperbolic curve. Let l be a prime number, k a field of characteristic zero, $\overline{k}$ an algebraic closure of k, and X a *hyperbolic curve* over k. Write $G_k \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k)$, $\Delta_X^{(l)}$ for the pro-l geometric fundamental group of X [i.e., the maximal pro-l quotient of $\pi_1(X \otimes_k \overline{k})$], and

$$\rho_X^{(l)} \colon G_k \longrightarrow \mathrm{Out}(\Delta_X^{(l)})$$

for the *pro-l outer Galois action* associated to X. In [6], M. Matsumoto studied a k-rational point $x \in X(k)$ of X that satisfies the following condition $E(X, x, l)$ [cf. [6, Introduction]]:

> $E(X, x, l)$: If we write $s_x \colon G_k \to \pi_1(X)$ for the outer homomorphism induced by the k-rational point $x \in X(k)$, then the kernel of the composite

---

2000 Mathematics Subject Classification : 14H30.

$$G_k \xrightarrow{s_x} \pi_1(X) \longrightarrow \mathrm{Aut}(\Delta_X^{(l)})$$

— where the second arrow is the action obtained by conjugation — *coincides* with the kernel $\mathrm{Ker}(\rho_X^{(l)})$ of the outer action

$$\rho_X^{(l)} : G_k \longrightarrow \mathrm{Out}(\Delta_X^{(l)}).$$

For instance, Matsumoto proved that, roughly speaking, there are *many* hyperbolic curves over number fields which have *no* rational point that satisfies the above condition "$E(X, x, l)$" [cf. [6, Theorem 1]].

As in [5], in the case where k is a *number field*, we shall say that a k-rational point $x \in X(k)$ of X is *l-moderate* if the above condition $E(X, x, l)$ is satisfied [cf. [5, Definition 2.4, (i)]; the equivalence (1) $\Leftrightarrow$ (3) of [5, Proposition 2.5]]; moreover, we shall say that a k-rational point of X is *moderate* if it is p-moderate for some prime number p [cf. Definition 2.1]. Typical examples of moderate points of hyperbolic curves are as follows:

(a) A closed point of a *split tripod* [i.e., "$\mathbb{P}^1_k \setminus \{0, 1, \infty\}$"] corresponding to a *tripod p-unit* [cf. [5, Definition 1.6]] [that is a certain *higher circular p-unit* — cf. [5, Remark 1.6.1]] for some prime number p [cf. [5, Proposition 2.8]].
(b) A torsion point of [the underlying elliptic curve of] a *once-punctured elliptic curve* whose order is a [positive] power of a prime number [cf. [5, Proposition 2.7]].
(c) Every $\mathbb{Q}^{\text{un-}l}$-rational [cf. [5, Definition 1.8]] point of the [compactified] Fermat curve over $\mathbb{Q}$ of degree l [i.e., "$\mathrm{Proj}(\mathbb{Q}[s, t, u]/(s^l + t^l + u^l))$"] if l is ≥ 5 and *regular* [cf. [5, Remark 3.5.1]].

Let us recall from [5, Remark 2.6.1, (i)], that

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

On the other hand, it is well-known that the set of *torsion* rational points of an abelian variety over a number field is *finite.* Thus, we have the following natural question:

> Is the set of *moderate* rational points of a hyperbolic curve over a number field *finite*?

Observe that it follows from Faltings' work on the *Mordell conjecture* that if the hyperbolic curve under consideration is of genus ≥ 2, then the set of rational points, hence also *moderate* rational points, is *finite*.

The main result of the present paper is as follows [cf. Corollaries 2.6, 2.7]:

Theorem A *Let* k *be a* **number field** *and* $(G, o \in G(k))$ *an* **elliptic curve** (*respectively, a* **nonsplit torus** *of dimension one*) *over* k. *Write* $X \stackrel{\mathrm{def}}{=} G \setminus \{o\}$. [*Thus,* X *is a* **hyperbolic curve** *over* k *of type* $(1,1)$ (*respectively,* $(0,3)$).] *Then the set of* **moderate** k*-rational points of* X *is* **finite**.

In order to prove Theorem A, we discuss the *center* of the image of the pro-l outer Galois action $\rho_X^{(l)} : G_k \to \mathrm{Out}(\Delta_X^{(l)})$ associated to X. In particular, we prove the following result [cf. Theorem 1.13]:

Theorem B *Let* (g, r) *be a pair of nonnegative integers such that* $2g-2+r > 0$, l *an* **odd** *prime number,* k *a* **generalized sub-l-adic** *field* [*cf.* [7, Definition 4.11]], $\overline{k}$ *an algebraic closure of* k, *and* X *a* **split** [*cf. Definition* 1.3, (i); *Remark* 1.3.1, (i)] *hyperbolic curve of type* (g, r) *over* k *which has* **no special symmetry** [*cf. Definition* 1.3, (ii); *Remark* 1.3.1, (ii)]. *Write* $G_k \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k)$, $\Delta_X^{(l)}$ *for the pro-l geometric fundamental group of* X [*i.e., the maximal pro-l quotient of* $\pi_1(X \otimes_k \overline{k})$], $\rho_X^{(l)} : G_k \to \mathrm{Out}(\Delta_X^{(l)})$ *for the pro-l outer Galois action associated to* X, $\Gamma_X^{(l)} \stackrel{\mathrm{def}}{=} \mathrm{Im}(\rho_X^{(l)}) \subseteq \mathrm{Out}(\Delta_X^{(l)})$, *and* $M_X^{(l)} \stackrel{\mathrm{def}}{=} (\Delta_X^{(l)})^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l$. *Then the following three conditions are* **equivalent**:

(1) *It holds that* $(g, r) \in \{(1,1), (2,0)\}$, *and that* $-1 \in \mathrm{Aut}(M_X^{(l)})$ *is* **contained** *in the image of the action* $G_k \to \mathrm{Aut}(M_X^{(l)})$ *induced by* $\rho_X^{(l)}$.

(2) *The center* $Z(\Gamma_X^{(l)})$ *is* **isomorphic** *to* $\mathbb{Z}/2\mathbb{Z}$.

(3) *The center* $Z(\Gamma_X^{(l)})$ *is* **nontrivial**.

0. Notations and Conventions

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

Profinite Groups.— Let G be a profinite group, $H \subseteq G$ a closed subgroup of G, and $G \twoheadrightarrow Q$ a quotient of G. We shall say that H (respectively, Q) is *characteristic* if every [continuous] automorphism of G preserves H (respectively, $\mathrm{Ker}(G \twoheadrightarrow Q)$). 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], $N_G(H)$ for the *normalizer* of H in G, $Z_G(H)$ for the *centralizer* of H in G, and $Z(G) \stackrel{\mathrm{def}}{=} Z_G(G)$ for the *center* of G. We shall say that G is *slim* if $Z_G(J) = \{1\}$ for every open subgroup $J \subseteq G$ of G.

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

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 $D \subseteq X^{\mathrm{cpt}}$ of X^{cpt} which is finite and étale over S such that the complement $X^{\mathrm{cpt}} \setminus D$ 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 and to D as the *divisor at infinity* 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)] 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 $2g-2+r > 0$, each geometric fiber of $X^{\mathrm{cpt}} \to S$ is [a necessarily smooth proper connected curve] of genus g, and the degree of $D \subseteq X^{\mathrm{cpt}}$ over S is equal to r. We shall refer to a hyperbolic curve of type $(0, 3)$ as a *tripod*.

Tori.— Let S be a scheme and $(X, o \in X(S))$ an abelian group scheme over S. Then we shall write $\mathbb{G}_{m,S}$ for the [abelian] group scheme over S which represents the functor over S

$$(T \to S) \rightsquigarrow \Gamma(T, \mathcal{O}_T^{\times}).$$

We shall say that $(X, o \in X(S))$ is a *split torus* over S if $(X, o \in X(S))$ is isomorphic to a fiber product of finitely many copies of $\mathbb{G}_{m,S}$ over S. We shall say that $(X, o \in X(S))$ is a *torus* if, étale locally on S, $(X, o \in X(S))$ is a split torus. Thus, one verifies easily that if $(X, o \in X(S))$ is a torus of relative dimension d over S, then the assignment

$$(T \to S) \rightsquigarrow \mathrm{Hom}_{T\text{-ab.gr.}}((X \times_S T, o_T \in X(T)), \mathbb{G}_{m,T})$$

— where we write "$\mathrm{Hom}_{T\text{-ab.gr.}}$" for the module of homomorphisms of abelian group schemes over T — determines an *étale local system* in free $\mathbb{Z}$-modules of rank d on S. In particular, if, moreover, S is connected, then the above étale local system gives rise to a continuous outer homomorphism

$$\pi_1(S) \longrightarrow \mathrm{GL}_d(\mathbb{Z}).$$

Note that one verifies immediately that it holds that the torus $(X, o \in X(S))$ is *split* if and only if this outer homomorphism is *trivial*.

1. Center of the Outer Galois Image Associated to a Hyperbolic Curve

In the present Section 1, we discuss the *center* [which is necessarily a *finite* group — cf., e.g., [3, Proposition 1.7, (ii)], [3, Lemma 1.8]] of the image of the pro-l outer Galois action associated to a hyperbolic curve over a generalized sub-l-adic field [cf. [7, Definition 4.11]]. In particular, we give, under the assumption that l is *odd*, a *necessary and sufficient condition* [cf. Theorem 1.13] for a *split* [cf. Definition 1.3, (i); Remark 1.3.1, (i)] hyperbolic curve over a generalized sub-l-adic field which has *no special symmetry* [cf. Definition 1.3, (ii); Remark 1.3.1, (ii)] to have *trivial center*.

In the present Section 1, let (g, r) be a pair of nonnegative integers such that $2g - 2 + r > 0$, l a prime number, k a field of characteristic zero, $\overline{k}$ an algebraic closure of k, X a *hyperbolic curve* of type (g, r) over k, and V a *smooth variety* over k [i.e., a scheme which is smooth, of finite type, separated, and geometrically connected over k]. Write $G_k \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k)$, X^{cpt} for the *smooth compactification* of X, $\Delta_V \stackrel{\mathrm{def}}{=} \pi_1(V \otimes_k \overline{k})$ for the *geometric fundamental group* of V,

$$\rho_V : G_k \longrightarrow \mathrm{Out}(\Delta_V)$$

for the *outer Galois action* associated to V, $\Delta_V^{(l)}$ for the *pro-l geometric fundamental group* of V [i.e., the maximal pro-l quotient of Δ_V], and $M_V^{(l)} \overset{\mathrm{def}}{=} (\Delta_V^{(l)})^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l$. [Thus, $M_V^{(l)}$ is equipped with a natural structure of *vector space over* $\mathbb{F}_l$ *of finite dimension*.] If $\Delta_V \twoheadrightarrow Q$ is a *characteristic* quotient of Δ_V, then we shall write

$$\rho_V^Q : G_k \longrightarrow \mathrm{Out}(Q)$$

for the outer Galois action determined by ρ_V and

$$\Gamma_V[Q] \overset{\mathrm{def}}{=} \mathrm{Im}(\rho_V^Q) \subseteq \mathrm{Out}(Q).$$

Write, moreover,

$$\rho_V^{(l)} \overset{\mathrm{def}}{=} \rho_V^{\Delta_V^{(l)}} : G_k \longrightarrow \mathrm{Out}(\Delta_V^{(l)})$$

[i.e., the *pro-l outer Galois action* associated to V] and

$$\Gamma_V \overset{\mathrm{def}}{=} \Gamma_V[\Delta_V] = \mathrm{Im}(\rho_V) \subseteq \mathrm{Out}(\Delta_V),$$

$$\Gamma_V^{(l)} \overset{\mathrm{def}}{=} \Gamma_V[\Delta_V^{(l)}] = \mathrm{Im}(\rho_V^{(l)}) \subseteq \mathrm{Out}(\Delta_V^{(l)}),$$

$$\Gamma_V^{(\text{mod-}l)} \overset{\mathrm{def}}{=} \Gamma_V[M_V^{(l)}] \subseteq \mathrm{Out}(M_V^{(l)}) = \mathrm{Aut}(M_V^{(l)}).$$

Theorem 1.1 (Mochizuki) *Suppose that k is* **generalized sub-l-adic** [*cf.* [7, Definition 4.11]]. *Then the natural homomorphisms*

$$\mathrm{Aut}_k(X) \longrightarrow \mathrm{Out}(\Delta_X) \longrightarrow \mathrm{Out}(\Delta_X^{(l)})$$

determine **isomorphisms of finite groups**

$$\mathrm{Aut}_k(X) \xrightarrow{\sim} Z_{\mathrm{Out}(\Delta_X)}(\Gamma_X) \xrightarrow{\sim} Z_{\mathrm{Out}(\Delta_X^{(l)})}(\Gamma_X^{(l)}).$$

Proof. This follows immediately from [7, Theorem 4.12] [cf. also [8, Corollary 1.5.7]]. □

Definition 1.2 Let $\Delta_V \twoheadrightarrow Q$ be a *characteristic* quotient of Δ_V and $\alpha \in \mathrm{Aut}_k(V)$ an automorphism of V over k. Then we shall say that α is *Q-Galois-like* if the image of $\alpha \in \mathrm{Aut}_k(V)$ via the composite of natural homomorphisms $\mathrm{Aut}_k(V) \to \mathrm{Out}(\Delta_V) \to \mathrm{Out}(Q)$ is contained in $\Gamma_V[Q] \subseteq \mathrm{Out}(Q)$. We shall say that α is *l-Galois-like* (respectively, *$(\mathrm{mod}\, l)$-Galois-like*) if α is $\Delta_V^{(l)}$-Galois-like (respectively, $M_V^{(l)}$-Galois-like).

Remark 1.2.1 One verifies immediately from the various definitions involved that the natural injection $\mathrm{Aut}_k(X) \hookrightarrow \mathrm{Out}(\Delta_X^{(l)})$ determines an injection

$$\{l\text{-}\textit{Galois-like} \text{ automorphisms of } X \text{ over } k\} \hookrightarrow Z(\Gamma_X^{(l)}).$$

If, moreover, k is *generalized sub-l-adic*, then it follows from Theorem 1.1 that this injection is, in fact, an *isomorphism*:

$$\{l\text{-}\textit{Galois-like} \text{ automorphisms of } X \text{ over } k\} \xrightarrow{\sim} Z(\Gamma_X^{(l)}).$$

Definition 1.3

(i) We shall say that the hyperbolic curve X is *split* [cf. [3, Definition 1.5, (i)]] if the divisor at infinity of X determines a trivial covering of $\mathrm{Spec}(k)$, or, equivalently, the natural action of G_k on the set of cusps of X is trivial.

(ii) We shall say that the hyperbolic curve X has *no special symmetry* [cf. [3, Definition 3.3]] if the following condition is satisfied: Write $\mathcal{M}_{g,r}$ for the moduli stack of r-pointed proper smooth curves of genus g over k whose r marked points are equipped with an ordering, $(\mathcal{C}_{g,r}^{\mathrm{cpt}} \to \mathcal{M}_{g,r}; s_1, \ldots, s_r \colon \mathcal{M}_{g,r} \to \mathcal{C}_{g,r}^{\mathrm{cpt}})$ for the universal family over $\mathcal{M}_{g,r}$, and $\mathcal{C}_{g,r} \stackrel{\mathrm{def}}{=} \mathcal{C}_{g,r}^{\mathrm{cpt}} \setminus \bigcup_{i=1}^{r} \mathrm{Im}(s_i)$. [Thus, $\mathcal{C}_{g,r} \to \mathcal{M}_{g,r}$ is a *split hyperbolic curve* of type (g,r) over $\mathcal{M}_{g,r}$.] Then the specialization homomorphism $\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r}) \to \mathrm{Aut}_{\overline{k}}(X \otimes_k \overline{k})$ [obtained by equipping the cusps of $X \otimes_k \overline{k}$ with some ordering] is an isomorphism.

Remark 1.3.1

(i) It follows from the definition of a hyperbolic curve that there exists a finite extension K of k such that $X \otimes_k K$ is *split*.

(ii) In the notation of Definition 1.3, (ii), it is well-known [cf., e.g., [2, Theorem 1.11]] that the functor over $\mathcal{M}_{g,r}$

$$(S \to \mathcal{M}_{g,r}) \rightsquigarrow \mathrm{Aut}_S(\mathcal{C}_{g,r} \times_{\mathcal{M}_{g,r}} S)$$

is *represented* by a *finite unramified* [relative] scheme $\mathcal{A} \to \mathcal{M}_{g,r}$ over $\mathcal{M}_{g,r}$. Thus, there exists a *dense open* substack $U \subseteq \mathcal{M}_{g,r}$ of $\mathcal{M}_{g,r}$ on which $\mathcal{A} \to \mathcal{M}_{g,r}$ is a *finite étale covering.* Thus, it follows immediately from the definition given in Definition 1.3, (ii), that each hyperbolic curve parametrized by a point of U has *no special symmetry.*

(iii) It follows immediately that the hyperbolic curve X has *no special symmetry* if and only if $\mathrm{Aut}_{\overline{k}}(X \otimes_k \overline{k})$ is isomorphic to the finite group

$$\begin{cases} \mathfrak{S}_3 & (\text{if } (g,r) = (0,3)) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & (\text{if } (g,r) = (0,4)) \\ \mathbb{Z}/2\mathbb{Z} & (\text{if } (g,r) \in \{(1,1),(1,2),(2,0)\}) \\ \{1\} & (\text{if } 2g-2+r \geq 3). \end{cases}$$

In this situation, if, moreover, X is *split*, then one verifies immediately that $\mathrm{Aut}_k(X)$ is isomorphic to the above finite group.

Lemma 1.4 *Suppose that X is* **split**. *Then the following hold:*

(i) *Let α be an* ***l*-Galois-like** *automorphism of X over k. Then α induces the* **identity** *automorphism on the set of cusps of X.*

(ii) *Suppose, moreover, that X is of* **genus zero**. *Then there is* **no nontrivial *l*-Galois-like** *automorphism of X over k.*

Proof. First, we verify assertion (i). Since X is *split*, one verifies immediately that the natural action of $\Gamma_X^{(l)}$, hence also α [cf. our assumption that α is *l-Galois-like*], on the set of conjugacy classes of cuspidal inertia subgroups of $\Delta_X^{(l)}$ is *trivial.* Thus, assertion (i) follows from the [well-known] *injectivity* of the natural map from the set of cusps of X to the set of conjugacy classes of cuspidal inertia subgroups of $\Delta_X^{(l)}$. This completes the proof of assertion (i). Assertion (ii) follows immediately from assertion (i), together with the [easily verified] fact that every nontrivial automorphism of X over k acts *nontrivially* on the set of cusps of X [cf. our assumption that X is of *genus* *zero*]. This completes the proof of assertion (ii), hence also of Lemma 1.4. $\square$

Proposition 1.5 *Suppose that k is* **generalized sub-$\boldsymbol{l}$-adic***, and that X is* **split** *and of* **genus zero***. Then the center $Z(\Gamma_X^{(l)})$ is* **trivial***.*

Proof. This follows immediately from Lemma 1.4, (ii), together with Remark 1.2.1. $\square$

Lemma 1.6 *Let O, A be profinite groups*; *$f\colon O \to A$ a homomorphism of profinite groups*; *$G \subseteq O$ a closed subgroup of O*; *$\alpha \in N_O(G)$. Suppose that the following three conditions are satisfied*:

(1) *The kernel of f is* **pro-$\boldsymbol{l}$***.*
(2) *There exists a positive integer n such that n is* **prime** *to l, and, moreover, $\alpha^n = 1$.*
(3) *It holds that $f(\alpha) \in f(G)$.*

Then it holds that $\alpha \in G$.

Proof. Let us first observe that one verifies easily that, to verify Lemma 1.6, we may assume without loss of generality, by replacing O by the closed subgroup of O generated by G and α, that G is *normal* in O [cf. our assumption that α *normalizes* G]. Next, let us observe that one verifies immediately from condition (3) that, to verify Lemma 1.6, we may assume without loss of generality, by replacing (O, A) by $(f^{-1}(f(G)), f(G))$, that $f|_G$, hence also f, is *surjective.* In particular, the natural inclusion $N \stackrel{\mathrm{def}}{=} \mathrm{Ker}(f) \hookrightarrow O$ determines an *isomorphism* $N/(N \cap G) \xrightarrow{\sim} O/G$, which thus implies that O/G is *pro-l* [cf. condition (1)]. Thus, it follows immediately from condition (2) that the image of $\alpha \in O$ in O/G is *trivial*, i.e., that $\alpha \in G$. This completes the proof of Lemma 1.6. $\square$

Lemma 1.7 *Let $\alpha \in \mathrm{Aut}_k(V)$ be an automorphism of V over k of* **finite order***. Suppose that α is of order* **prime** *to l. Then it holds that α is* **$\boldsymbol{l}$-Galois-like** *if and only if α is* **$(\mathbf{mod}\,\boldsymbol{l})$-Galois-like***.*

Proof. Let us first observe that since the natural surjection $\Delta_V \twoheadrightarrow M_V^{(l)}$ factors through $\Delta_V \twoheadrightarrow \Delta_V^{(l)}$, the *necessity* follows from the definition given in Definition 1.2. To verify the *sufficiency*, suppose that α is $(\mathrm{mod}\, l)$-*Galois-like.* Write $\alpha[\Delta_V^{(l)}] \in \mathrm{Out}(\Delta_V^{(l)})$ for the image of α in $\mathrm{Out}(\Delta_V^{(l)})$. Then one verifies immediately that $\alpha[\Delta_V^{(l)}]$ *centralizes* $\Gamma_V^{(l)} \subseteq \mathrm{Out}(\Delta_V^{(l)})$. Thus, since the kernel of the natural homomorphism $\mathrm{Out}(\Delta_V^{(l)}) \twoheadrightarrow \mathrm{Aut}(M_V^{(l)})$ is *pro-l* [cf., e.g., [1, Theorem 6]], by applying Lemma 1.6 in the case where we take "(O, A, G, α)" in the statement of Lemma 1.6 to be $(\mathrm{Out}(\Delta_V^{(l)}), \mathrm{Aut}(M_V^{(l)}), \Gamma_V^{(l)}, \alpha[\Delta_V^{(l)}])$, we conclude that $\alpha[\Delta_V^{(l)}] \in \Gamma_V^{(l)}$, i.e., that α is *l-Galois-like*. This completes the proof of the *sufficiency*, hence also of Lemma 1.7. □

Lemma 1.8 *Let $(T, o \in T(k))$ be a* **nonsplit** *torus of dimension one over k. Suppose that $X = T \setminus \{o\}$. [Thus, X is a* **nonsplit tripod** *over k.] Suppose, moreover, that the following two conditions are satisfied:*

(1) *l is* **odd**.
(2) *k contains a* **primitive *l*-th root of unity**.

Then the automorphism $\alpha \in \mathrm{Aut}_k(X)$ of X over k induced by the automorphism of T given by "$a \mapsto a^{-1}$" [i.e., by multiplication by -1 if the group operation of T is written additively] is ***l*-Galois-like**.

Proof. Write $\chi\colon G_k \twoheadrightarrow \mathbb{Z}^{\times}$ for the [necessarily *nontrivial*] character determined by the *nonsplit* torus T. Let $\gamma \in G_k$ be such that $\chi(\gamma)$ is *nontrivial*. Write $I_o \subseteq M_X^{(l)}$ for the [uniquely determined] inertia subgroup of $M_X^{(l)}$ associated to the cusp [corresponding to] o of X. Then let us observe that one verifies easily that we have a natural exact sequence of finite G_k-modules

$$1 \longrightarrow I_o \longrightarrow M_X^{(l)} \longrightarrow M_T^{(l)} \longrightarrow 1.$$

Observe that I_o and $M_T^{(l)}$ are equipped with natural structures of *vector spaces over $\mathbb{F}_l$ of dimension one.*

Next, let us observe that it follows immediately from the definition of α that the actions of α on I_o, $M_T^{(l)}$ are given by multiplication by 1, -1, respectively. On the other hand, it follows immediately from our choice of $\gamma \in G_k$, together with condition (2), that the actions of γ on I_o, $M_T^{(l)}$ are given by multiplication by 1, -1, respectively. Thus, since γ *commutes* with α, we conclude from condition (1) that the action of α on $M_X^{(l)}$ *coincides* with the action of γ on $M_X^{(l)}$. In particular, α is $(\mathrm{mod}\, l)$-*Galois-like*, hence also [cf. condition (1), Lemma 1.7] *l-Galois-like*. This completes the proof of Lemma 1.8. □

Lemma 1.9 *Let $\alpha \in \mathrm{Aut}_k(X)$ be an automorphism of X over k of order* **prime** *to l. Write $\alpha^{\mathrm{cpt}} \in \mathrm{Aut}_k(X^{\mathrm{cpt}})$ for the automorphism of X^{cpt} determined by α. Then the following hold*:

(i) *If α is* ***l*-Galois-like** [*i.e.,* **(mod *l*)-Galois-like** — *cf. Lemma* 1.7], *then α^{cpt} is* ***l*-Galois-like** [*i.e.,* **(mod *l*)-Galois-like** — *cf. Lemma* 1.7].

(ii) *Suppose that one of the following two conditions is satisfied*:

(1) $r \leq 1$.

(2) *α induces the* **identity** *automorphism on the set of cusps of X, k contains a* **primitive *l*-th root of unity**, *and X is* **split**.

Then it holds that α is ***l*-Galois-like** *if and only if α^{cpt} is* ***l*-Galois-like**.

Proof. Assertion (i) follows immediately from the fact that the natural surjection $\Delta_X \twoheadrightarrow \Delta^{(l)}_{X^{\mathrm{cpt}}}$ factors through the natural surjection $\Delta_X \twoheadrightarrow \Delta^{(l)}_X$. Assertion (ii) in the case where condition (1) is satisfied follows immediately — in light of Lemma 1.7 — from the [easily verified] fact that the natural surjection $\Delta^{(l)}_X \twoheadrightarrow \Delta^{(l)}_{X^{\mathrm{cpt}}}$ determines an *isomorphism* $M^{(l)}_X \xrightarrow{\sim} M^{(l)}_{X^{\mathrm{cpt}}}$.

Finally, we verify assertion (ii) in the case where condition (2) is satisfied. Let us first observe that it follows — in light of Lemma 1.7 — from assertion (i) that it suffices to verify that if condition (2) is satisfied, and α^{cpt} is $(\mathrm{mod}\, l)$-*Galois-like*, then α is $(\mathrm{mod}\, l)$-*Galois-like*. Write $\alpha[M^{(l)}_X] \in \mathrm{Aut}(M^{(l)}_X)$ for the image of α in $\mathrm{Aut}(M^{(l)}_X)$ and $A \subseteq \mathrm{Aut}(M^{(l)}_X)$ for the subgroup of $\mathrm{Aut}(M^{(l)}_X)$ consisting of automorphisms of $M^{(l)}_X$ that induce the *identity automorphism* on $M^{\mathrm{csp}}_X \stackrel{\mathrm{def}}{=} \mathrm{Ker}(M^{(l)}_X \twoheadrightarrow M^{(l)}_{X^{\mathrm{cpt}}}) \subseteq M^{(l)}_X$. Here, let us observe that [since the module $\mathrm{Hom}_{\mathbb{F}_l}(M^{(l)}_{X^{\mathrm{cpt}}}, M^{\mathrm{csp}}_X)$ of $\mathbb{F}_l$-linear homomorphisms $M^{(l)}_{X^{\mathrm{cpt}}} \to M^{\mathrm{csp}}_X$ is of *order a power of l*] the kernel of the natural homomorphism $A \to \mathrm{Aut}(M^{(l)}_{X^{\mathrm{cpt}}})$ is an *l-group*. Moreover, it follows immediately from condition (2) that $\alpha[M^{(l)}_X]$ is *contained* in A.

Next, let us observe that the natural action of $\Gamma^{(\text{mod-}l)}_X$ on $M^{(l)}_X$ *preserves* the subspace $M^{\mathrm{csp}}_X \subseteq M^{(l)}_X$. Moreover, it follows immediately from condition (2) that the resulting action of $\Gamma^{(\text{mod-}l)}_X$ on M^{csp}_X is *trivial*, i.e., that $\Gamma^{(\text{mod-}l)}_X \subseteq A$. Thus, by applying Lemma 1.6 in the case where we take "(O, A, G, α)" in the statement of Lemma 1.6 to be $(A, \mathrm{Aut}(M^{(l)}_{X^{\mathrm{cpt}}}), \Gamma^{(\text{mod-}l)}_X, \alpha[M^{(l)}_X])$, we conclude that $\alpha[M^{(l)}_X] \in \Gamma^{(\text{mod-}l)}_X$, i.e., that α is $(\mathrm{mod}\, l)$-*Galois-like*. This completes the proof of assertion (ii) in the case where condition (2) is satisfied. $\square$

Definition 1.10 Let $\alpha \in \mathrm{Aut}_k(X)$ be an automorphism of X over k. Then we shall say that α is a *hyperelliptic involution* if $g \geq 1$, and, moreover, there exist a proper smooth curve C over k of genus zero and a finite morphism $X^{\mathrm{cpt}} \to C$ of degree two over k such that $\mathrm{Aut}_C(X^{\mathrm{cpt}})$ is generated by [the automorphism of X^{cpt} determined by] α. In particular, a *hyperelliptic involution* is of *order two*.

Remark 1.10.1 If $(g, r) \in \{(1,1), (2,0)\}$, then it is well-known that, in the notation of Definition 1.3, (ii), the image of the unique nontrivial [cf. Remark 1.3.1, (iii)] element of $\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r})$ in $\mathrm{Aut}_k(X)$ [cf. the fact that X is *split*] is a *hyperelliptic involution*.

Lemma 1.11 *Let $\alpha \in \mathrm{Aut}_k(X)$ be a* **hyperelliptic involution** *of X. Then α acts on $\Delta^{\mathrm{ab}}_{X^{\mathrm{cpt}}}$, hence also $M^{(l)}_{X^{\mathrm{cpt}}}$, via* **multiplication by -1**.

Proof. Let us first observe that it follows immediately that we may assume without loss of generality, by replacing k by $\overline{k}$, that k is *algebraically closed*. Write J_X for the Jacobian variety of X^{cpt}. Then one verifies immediately from the various definitions involved that, to verify Lemma 1.11, it suffices to verify that α acts on J_X via *multiplication by* -1. Write $j\colon X^{\mathrm{cpt}} \hookrightarrow J_X$ for the closed immersion associated to a k-rational closed point of X^{cpt} that is preserved by α. [Note that since $g \geq 1$, there exists a k-rational point of X^{cpt} that is preserved by α.] Then since J_X is *generated* by the image of j, and [one verifies easily that] the morphism "$X^{\mathrm{cpt}} \to C$" of Definition 1.10 *factors* through the composite

$$X^{\mathrm{cpt}} \xrightarrow{j \times j} J_X \times_k J_X \xrightarrow{(\mathrm{id}_{J_X}, \alpha_{J_X})} J_X \times_k J_X \longrightarrow J_X$$

— where we write α_{J_X} for the automorphism of J_X induced by α, and the third arrow is the group operation of J_X — Lemma 1.11 follows immediately from the [well-known] fact that *any morphism from a smooth curve of genus zero to an abelian variety is constant.* This completes the proof of Lemma 1.11. $\square$

Lemma 1.12 *Let $\alpha \in \mathrm{Aut}_k(X)$ be a* **hyperelliptic involution** *of X. Suppose that the following two conditions are satisfied*:

(1) *l is* **odd**.
(2) $-1 \in \Gamma^{(\text{mod-}l)}_{X^{\text{cpt}}} \subseteq \text{Aut}(M^{(l)}_{X^{\text{cpt}}})$.

Suppose, moreover, that one of the following two conditions is satisfied:

(3) $r \leq 1$.
(4) $g = 1$, *X is* **split**, *and α induces the* **identity** *automorphism on the set of cusps of X*.

Then α is ***l*-Galois-like**.

Proof. First, I claim that the following assertion holds:

> Claim 1.12.A: If $g = 1$, then condition (2) implies condition (2) in the case where we take "X" to be $X \otimes_k k(\zeta_l)$ — where $\zeta_l \in \overline{k}$ is a *primitive l-th root of unity.*

Indeed, Claim 1.12.A follows immediately from the [well-known] fact that $\wedge^2 M^{(l)}_{X^{\text{cpt}}}$ is isomorphic, as a G_k-module, to the *group of l-th roots of unity* of $\overline{k}$ [cf. our assumption that $g = 1$], together with the [easily verified] fact that $-1 \in \text{Aut}(M^{(l)}_{X^{\text{cpt}}})$ acts *trivially* on $\wedge^2 M^{(l)}_{X^{\text{cpt}}}$. This completes the proof of Claim 1.12.A.

Now since α acts on $M^{(l)}_{X^{\text{cpt}}}$ via *multiplication by* -1 [cf. Lemma 1.11], Lemma 1.12 in the case where condition (3) (respectively, (4)) is satisfied follows immediately from Lemma 1.9, (ii) (respectively, Lemma 1.9, (ii), together with Claim 1.12.A). This completes the proof of Lemma 1.12. $\square$

Theorem 1.13 *Let (g, r) be a pair of nonnegative integers such that $2g - 2 + r > 0$, l an* **odd** *prime number, k a* **generalized sub-*l*-adic** *field* [*cf.* [7, Definition 4.11]], *$\overline{k}$ an algebraic closure of k, and X a* **split** [*cf. Definition* 1.3, (i); *Remark* 1.3.1, (i)] *hyperbolic curve of type (g, r) over k which has* **no special symmetry** [*cf. Definition* 1.3, (ii); *Remark* 1.3.1, (ii)]. *Write $G_k \stackrel{\text{def}}{=} \text{Gal}(\overline{k}/k)$, $\Delta^{(l)}_X$ for the pro-l geometric fundamental group of X [i.e., the maximal pro-l quotient of $\pi_1(X \otimes_k \overline{k})$], $\rho^{(l)}_X \colon G_k \to \text{Out}(\Delta^{(l)}_X)$ for the pro-l outer Galois action associated to X, $\Gamma^{(l)}_X \stackrel{\text{def}}{=} \text{Im}(\rho^{(l)}_X) \subseteq \text{Out}(\Delta^{(l)}_X)$, and $M^{(l)}_X \stackrel{\text{def}}{=} (\Delta^{(l)}_X)^{\text{ab}} \otimes_{\mathbb{Z}_l} \mathbb{F}_l$. Then the following three conditions are* **equivalent**:

(1) *It holds that $(g, r) \in \{(1, 1), (2, 0)\}$, and that $-1 \in \text{Aut}(M^{(l)}_X)$ is* **contained** *in the image of the action $G_k \to \text{Aut}(M^{(l)}_X)$ induced by $\rho^{(l)}_X$.*
(2) *The center $Z(\Gamma^{(l)}_X)$ is* **isomorphic** *to $\mathbb{Z}/2\mathbb{Z}$.*

(3) *The center* $Z(\Gamma_X^{(l)})$ *is* **nontrivial**.

Proof. First, we verify the implication (1) $\Rightarrow$ (2). Suppose that condition (1) is satisfied. Then since [we have assumed that] X is *split* and has *no special symmetry*, it follows from Remark 1.3.1, (iii), that $\mathrm{Aut}_k(X) \simeq \mathbb{Z}/2\mathbb{Z}$. Write $\alpha \in \mathrm{Aut}_k(X) \xrightarrow{\sim} Z_{\mathrm{Out}(\Delta_X^{(l)})}(\Gamma_X^{(l)})$ [cf. Theorem 1.1] for the *unique nontrivial* element of $\mathrm{Aut}_k(X)$. Then it follows from Lemma 1.12, together with Remark 1.10.1, that $\alpha \in \Gamma_X^{(l)}$, i.e., that $\alpha \in Z(\Gamma_X^{(l)})$. In particular, it follows that

$$\mathbb{Z}/2\mathbb{Z} \simeq \langle \alpha \rangle \subseteq Z(\Gamma_X^{(l)}) \subseteq Z_{\mathrm{Out}(\Delta_X^{(l)})}(\Gamma_X^{(l)}) \xleftarrow{\sim} \mathrm{Aut}_k(X) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Thus, condition (2) is satisfied. This completes the proof of the implication (1) $\Rightarrow$ (2).

The implication (2) $\Rightarrow$ (3) is immediate. Finally, we verify the implication (3) $\Rightarrow$ (1). Suppose that condition (3) is satisfied. Let us first observe that it follows from Proposition 1.5 that $g \geq 1$. Next, let us observe that since [we have assumed that] X has *no special symmetry*, if $(g, r) \notin \{(1, 1), (1, 2), (2, 0)\}$, then it follows from Remark 1.3.1, (iii), together with Remark 1.2.1, that condition (3) is *not satisfied*. Thus, we conclude that $(g, r) \in \{(1, 1), (1, 2), (2, 0)\}$.

Assume that $(g, r) = (1, 2)$. Then one verifies immediately [cf., e.g., the proof of [3, Proposition 3.2, (i)]] that the unique nontrivial automorphism of X over k [cf. Remark 1.3.1, (iii)] acts *nontrivially* on the set of cusps of X. Thus, it follows immediately from Lemma 1.4, (i), together with Remark 1.2.1, that condition (3) is *not satisfied*. In particular, we conclude that $(g, r) \in \{(1, 1), (2, 0)\}$.

Next, let us observe that since $(g, r) \in \{(1, 1), (2, 0)\}$, it follows immediately from Remark 1.3.1, (iii), together with Remark 1.10.1, that $\mathrm{Aut}_k(X)$ is generated by a *hyperelliptic involution* α of X, i.e., $(\mathbb{Z}/2\mathbb{Z} \simeq)$ $\langle \alpha \rangle = \mathrm{Aut}_k(X) \xrightarrow{\sim} Z_{\mathrm{Out}(\Delta_X^{(l)})}(\Gamma_X^{(l)})$. Thus, since $Z(\Gamma_X^{(l)})$ $(\subseteq Z_{\mathrm{Out}(\Delta_X^{(l)})}(\Gamma_X^{(l)}))$ is *nontrivial* [cf. condition (3)], it holds that $\alpha \in Z(\Gamma_X^{(l)}) \subseteq \Gamma_X^{(l)}$. In particular, condition (1) follows immediately from Lemma 1.11. This completes the proof of the implication (3) $\Rightarrow$ (1), hence also of Theorem 1.13. $\square$

Proposition 1.14 *Let* $Y \to X$ *be a finite étale Galois covering over* k *such that* Y *is* **geometrically connected** *over* k*, i.e., that* Y *is a*

hyperbolic curve *over* k. *Write* $\Pi_X^{(l)}$, $\Pi_Y^{(l)}$ *for the respective geometrically pro-l fundamental groups of* X, Y [*i.e., the respective quotients of* $\pi_1(X)$, $\pi_1(Y)$ *by the normal closed subgroups* $\mathrm{Ker}(\Delta_X \twoheadrightarrow \Delta_X^{(l)}) \subseteq \pi_1(X)$, $\mathrm{Ker}(\Delta_Y \twoheadrightarrow \Delta_Y^{(l)}) \subseteq \pi_1(Y)$]. *Suppose that* $Y \to X$ *induces an outer open injection* $\Pi_Y^{(l)} \hookrightarrow \Pi_X^{(l)}$. *Consider the following three conditions*:

(1) *It holds that* $\mathrm{Ker}(\rho_X^{(l)}) \neq \mathrm{Ker}(\rho_Y^{(l)})$, *or, equivalently* [*cf.* [4, Proposition 25, (i)]], $\mathrm{Ker}(\rho_X^{(l)}) \not\subseteq \mathrm{Ker}(\rho_Y^{(l)})$.
(2) *There exists an automorphism* $\alpha \in \mathrm{Aut}_X(Y) \subseteq \mathrm{Aut}_k(Y)$ *of* Y *over* X, *hence also over* k, *which is* **nontrivial** *and* ***l*-Galois-like**.
(3) *The hyperbolic curve* $Y \otimes_k \overline{k}^{\mathrm{Ker}(\rho_X^{(l)})}$ *over* $\overline{k}^{\mathrm{Ker}(\rho_X^{(l)})}$ *is* **not split**.

Then we have implications

$$(1) \Longleftrightarrow (2) \Longleftarrow (3).$$

If, moreover, Y, *hence also* X, *is of* **genus zero**, *then we have equivalences*

$$(1) \Longleftrightarrow (2) \Longleftrightarrow (3).$$

Proof. First, we verify the equivalence (1) $\Leftrightarrow$ (2). Write $Q_X \stackrel{\mathrm{def}}{=} \Pi_X^{(l)}/Z_{\Pi_Y^{(l)}}(\Delta_Y^{(l)})$, $Q_Y \stackrel{\mathrm{def}}{=} \Pi_Y^{(l)}/Z_{\Pi_Y^{(l)}}(\Delta_Y^{(l)})$. [Thus, Q_Y *coincides* with the quotient "$\Phi_{Y/k}^{\{l\}}$" defined in [4, Definition 1, (iv)] — cf. also [4, Lemma 4, (i)].] Then it follows immediately that one obtains a commutative diagram of profinite groups [cf. also [4, Lemma 4, (i)]]

$$\begin{tikzcd}
1 \arrow[r] & \Delta_Y^{(l)} \arrow[r] \arrow[d] & Q_Y \arrow[r] \arrow[d] & \Gamma_Y^{(l)} \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \Delta_X^{(l)} \arrow[r] & Q_X \arrow[r] & \Gamma_Y^{(l)} \arrow[r] & 1
\end{tikzcd}$$

— where the horizontal sequences are *exact*, and the vertical arrows are outer *injections* whose images are *open* and *normal*.

Now let us observe that one verifies immediately that condition (2) is *equivalent* to the following condition:

(a) There exist elements $\gamma_{Q_Y} \in Q_Y$, $\gamma_{\Delta_X^{(l)}} \in \Delta_X^{(l)} \setminus \Delta_Y^{(l)}$ such that the [necessarily *nontrivial* — cf. our assumption that $\gamma_{\Delta_X^{(l)}} \notin \Delta_Y^{(l)}$] *outer action* of $\gamma_{\Delta_X^{(l)}}$ on $\Delta_Y^{(l)}$ obtained by conjugation *coincides* with the *outer action* of γ_{Q_Y} on $\Delta_Y^{(l)}$ obtained by conjugation.

In particular, by multiplying "γ_{Q_Y}" in (a) with a suitable element of $\Delta_Y^{(l)}$ if necessary, it follows that condition (2) is *equivalent* to the following condition:

(b) There exist elements $\gamma_{Q_Y} \in Q_Y$, $\gamma_{\Delta_X^{(l)}} \in \Delta_X^{(l)} \setminus \Delta_Y^{(l)}$ such that $\gamma_{Q_Y} \cdot \gamma_{\Delta_X^{(l)}}^{-1} \in Z_{Q_X}(\Delta_Y^{(l)})$.

Now since $\Delta_Y^{(l)} = \Delta_X^{(l)} \cap Q_Y$, one verifies immediately that condition (b) is *equivalent* to the following condition:

(c) It holds that $Z_{Q_X}(\Delta_Y^{(l)}) \not\subseteq Q_Y$.

Moreover, since $Z_{Q_Y}(\Delta_Y^{(l)}) = \{1\}$ [cf. [4, Lemma 4, (i)]], condition (c) is *equivalent* to the following condition:

(d) It holds that $Z_{Q_X}(\Delta_Y^{(l)}) \neq \{1\}$, or, equivalently [cf. [4, Lemma 5]], $Z_{Q_X}(\Delta_X^{(l)}) \neq \{1\}$.

On the other hand, one verifies immediately that condition (d) is *equivalent* to condition (1). This completes the proof of the equivalence (1) $\Leftrightarrow$ (2).

Next, we verify the implication (3) $\Rightarrow$ (1). Suppose that condition (3) is satisfied. Let us first observe that since $\mathrm{Ker}(\rho_Y^{(l)}) \subseteq \mathrm{Ker}(\rho_X^{(l)})$ [cf. [4, Proposition 25, (i)]], we may assume without loss of generality, by replacing k by $\overline{k}^{\mathrm{Ker}(\rho_X^{(l)})}$, that $\rho_X^{(l)}$ is *trivial*. On the other hand, by considering the natural action of G_k on the set of cusps of Y, we conclude that condition (3) implies that $\rho_Y^{(l)}$ is *nontrivial*. In particular, condition (1) is satisfied. This completes the proof of the implication (3) $\Rightarrow$ (1). Finally, the implication (2) $\Rightarrow$ (3) in the case where Y is of *genus zero* follows immediately — in light of the inclusion $\mathrm{Ker}(\rho_Y^{(l)}) \subseteq \mathrm{Ker}(\rho_X^{(l)})$ [cf. [4, Proposition 25, (i)]], together with the equivalence (1) $\Leftrightarrow$ (2) — from Lemma 1.4, (ii). This completes the proof of Proposition 1.14. $\square$

2. Finiteness of the Moderate Points of Certain Hyperbolic Curves

In the present Section 2, we discuss the *finiteness* of the set of moderate rational points of a hyperbolic curve over a number field. In particular, we prove that the set of moderate rational points of the hyperbolic curve obtained by forming the complement of the origin in an *elliptic curve*, as well as a *nonsplit torus* of dimension one, over a number field is *finite* [cf. Corollaries 2.6, 2.7].

In the present Section 2, we maintain the notation of the preceding Section 1. Suppose, moreover, that k is a *number field*, which thus implies that k is *generalized sub-p-adic* for every prime number p.

Definition 2.1 Let $x \in X$ be a closed point of X. Then we shall say that x is *moderate* if there exists a prime number p such that x is p-moderate [cf. [5, Definition 2.4, (ii)]].

Proposition 2.2 *The set of* ***l*-moderate** [*cf.* [5, Definition 2.4, (ii)]] *k-rational points of X is* **finite**.

Proof. This follows immediately — in light of the equivalence (1) $\Leftrightarrow$ (3) of [5, Proposition 2.5] — from the final portion of [4, Theorem A]. $\square$

Lemma 2.3 *Let $x \in X(k)$ be a k-rational point of X and $\alpha \in \mathrm{Aut}_k(X)$ an automorphism of X over k. Suppose that x is* ***l*-moderate**, *and that α is* ***l*-Galois-like**. *Then $x \in X(k)$ is* **preserved** *by α.*

Proof. Write $U \subseteq X$ for the open subscheme of X obtained by forming the complement of [the image of] x in X and $\mathrm{Out}^x(\Delta_U^{(l)}) \subseteq \mathrm{Out}(\Delta_U^{(l)})$ for the group of outer automorphisms of $\Delta_U^{(l)}$ that preserve the conjugacy class of a cuspidal inertia subgroup associated to $x \in X(k)$. Then one verifies immediately from the various definitions involved that the natural open immersion $U \hookrightarrow X$ induces a commutative diagram of profinite groups

$$\begin{tikzcd}
\Gamma_U^{(l)} \arrow[r] \arrow[d, hook, "\cap"'] & \Gamma_X^{(l)} \arrow[d, hook, "\cap"] \\
\mathrm{Out}^x(\Delta_U^{(l)}) \arrow[r] & \mathrm{Out}(\Delta_X^{(l)})
\end{tikzcd}$$

— where the vertical arrows are the natural inclusions. Now since x is *l-moderate*, it follows immediately from the equivalence (1) $\Leftrightarrow$ (2) of [5, Proposition 2.5], that the upper horizontal arrow $\Gamma_U^{(l)} \twoheadrightarrow \Gamma_X^{(l)}$ of the above diagram is an *isomorphism*.

On the other hand, since α is *l-Galois-like*, it follows immediately from Remark 1.2.1 that α determines an element of $Z(\Gamma_X^{(l)})$. Thus, by means of the isomorphism $\Gamma_U^{(l)} \xrightarrow{\sim} \Gamma_X^{(l)}$, we obtain an element of $Z(\Gamma_U^{(l)})$. Write $\beta \in \mathrm{Aut}_k(U)$ for the automorphism of U over k that corresponds — relative to the *isomorphism* in the second display of Remark 1.2.1— to this element of $Z(\Gamma_U^{(l)})$. Then one verifies immediately from the *injectivity* of the composite

$$\mathrm{Aut}_k^x(U) \hookrightarrow \mathrm{Aut}_k(X) \hookrightarrow \mathrm{Out}(\Delta_X^{(l)})$$

— where we write $\mathrm{Aut}_k^x(U) \subseteq \mathrm{Aut}_k(U)$ for the group of automorphisms of U over k that preserve the cusp of U corresponding to $x \in X$ — that $\beta = \alpha|_U$, which thus implies that α *preserves* the k-rational point $x \in X(k)$. This completes the proof of Lemma 2.3. $\square$

Proposition 2.4 *In the notation of Proposition* 1.14*, suppose that k is a* **number field***. Then any of the three conditions* (1)*,* (2)*, and* (3) *implies the following condition: Y has* **no *l*-moderate** *k-rational point.*

Proof. Since [one verifies immediately that] every k-rational point of Y is *not preserved* by the "α" in condition (2), this follows immediately from Lemma 2.3. $\square$

Theorem 2.5 *Let X be a* **hyperbolic curve** *over a* **number field** *k. Suppose that there exists a nontrivial automorphism $\alpha \in \mathrm{Aut}_k(X)$ of X over k such that, for all but finitely many prime numbers p, the automorphism α is* ***p*-Galois-like** *[cf. Definition* 1.2*]. Then the set of* **moderate** *[cf. Definition* 2.1*] k-rational points of X is* **finite***.*

Proof. Write S for the set of prime numbers p such that the automorphism α is *p-Galois-like* and $Z_S \subseteq X(k)$ for the set of k-rational points of X which are *p-moderate* for some $p \in S$. Then let us observe that since [we have assumed that] the complement of S in the set of all prime numbers is *finite*, it follows immediately from Proposition 2.2 that, to complete the verification of Theorem 2.5, it suffices to verify that Z_S is *finite*. On the other hand, it follows immediately from Lemma 2.3 that every element of Z_S is *preserved* by α. Thus, the *finiteness* of Z_S follows immediately from the [well-known] *finiteness* of the set of fixed points of a nontrivial automorphism of a hyperbolic curve. This completes the proof of Theorem 2.5. $\square$

Corollary 2.6 *Let* $(T, o \in T(k))$ *be a* **nonsplit** *torus of dimension one over a* **number field** k. *Write* $X \stackrel{\text{def}}{=} T \setminus \{o\}$. [*Thus,* X *is a* **nonsplit** *— cf. Definition* 1.3, (i) *—* **tripod** *over* k.] *Then the set of* **moderate** [*cf. Definition* 2.1] k*-rational points of* X *is* **finite**.

Proof. Write $\alpha \in \mathrm{Aut}_k(X)$ for the automorphism of X over k induced by the automorphism of T given by "$a \mapsto a^{-1}$" [i.e., by multiplication by -1 if the group operation of T is written additively]. Then it follows from Theorem 2.5 that, to complete the verification of Corollary 2.6, it suffices to verify that α is *p-Galois-like* for all but finitely many prime numbers p. On the other hand, this follows immediately from Lemma 1.8, together with the [easily verified] fact that $\mathrm{Gal}(\overline{k}/k(\zeta_p)) \not\subseteq \mathrm{Ker}(\chi)$, where we write $\chi \colon G_k \twoheadrightarrow \mathbb{Z}^\times$ for the — necessarily *nontrivial* — character determined by the *nonsplit* torus T and use the notation $\zeta_p \in \overline{k}$ to denote a *primitive p-th root of unity*, for all but finitely many prime numbers p. This completes the proof of Corollary 2.6. $\square$

Corollary 2.7 *Let* $(E, o \in E(k))$ *be an elliptic curve over a* **number field** k. *For a positive integer* n, *write* $E[n] \subseteq E$ *for the subgroup scheme of* E *obtained by forming the kernel of the endomorphism of* E *given by multiplication by* n. *Let* $D \subseteq E$ *be a closed subscheme of* E *such that* $E[1]$ $(=$"$\{o\}$"$) \subseteq D \subseteq E[2]$. *Write* $X \stackrel{\text{def}}{=} E \setminus D$ *for the* **hyperbolic curve** *over* k *obtained by forming the complement of* D *in* E. [*Thus,* X *is of type* $(1,1)$, $(1,2)$, $(1,3)$, *or* $(1,4)$.] *Then the set of* **moderate** [*cf. Definition* 2.1] k*-rational points of* X *is* **finite**.

In particular, the set of **moderate** *rational points of a* **hyperbolic curve of type $(1,1)$** *over a* **number field** *is* **finite**.

Proof. Let us first observe that it follows immediately from the equivalence (1) $\Leftrightarrow$ (2′) of [5, Proposition 2.5], that, to verify Corollary 2.7, we may assume without loss of generality, by replacing k by a suitable finite extension of k, that X is *split* [cf. Remark 1.3.1, (i)]. Write $\alpha \in \mathrm{Aut}_k(X)$ for the automorphism of X over k determined by the automorphism of E

given by multiplication by -1. Now it follows immediately from Theorem 2.5 that, to complete the verification of Corollary 2.7, it suffices to verify that α is *p-Galois-like* for all but finitely many prime numbers p.

Next, let us observe that one verifies easily that α is a *hyperelliptic involution* of X and induces the *identity* automorphism on the set of cusps of X. Thus, it follows immediately from Lemma 1.12 [in the case where condition (4) is satisfied] that, to verify the assertion that α is *p-Galois-like* for all but finitely many prime numbers p, it suffices to verify that $-1 \in \mathrm{Aut}(M_E^{(p)})$ $(= \mathrm{Aut}(E[p](\overline{k})))$ is *contained* in $\Gamma_E^{(\mathrm{mod}\, p)} \subseteq \mathrm{Aut}(M_E^{(p)})$ $(= \mathrm{Aut}(E[p](\overline{k})))$ for all but finitely many prime numbers p. On the other hand, this follows from [9, Section 4.4, Théorème 3]; [9, Section 4.5, Corollaire to Théorème 5]. This completes the proof of Corollary 2.7. □

Acknowledgments The author would like to thank *Akio Tamagawa* for helpful discussions concerning Lemma 1.8 and Corollary 2.6. This research was supported by Grant-in-Aid for Scientific Research (C), No. 24540016, Japan Society for the Promotion of Science.

References

[1] Anderson M. P., *Exactness properties of profinite completion functors.* Topology **13** (1974), 229–239.

[2] Deligne P. and Mumford D., *The irreducibility of the space of curves of given genus.* Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

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

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

[5] Hoshi Y., *On the kernels of the pro-l outer Galois representations associated to hyperbolic curves over number fields.* Osaka J. Math. **52** (2015), 647–677.

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

[7] Mochizuki S., *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.

[8] Nakamura H., *Galois rigidity of pure sphere braid groups and profinite cal-*

culus. J. Math. Sci. Univ. Tokyo **1** (1994), 71–136.
[9] Serre J. P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), 259–331.

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