RIMS-1876

Reconstruction of one-puctured elliptic curves in positive characteristic by their geometric fundamental groups

By

Akira SARASHINA

Aug 2017

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

Reconstruction of one-punctured elliptic curves in positive characteristic by their geometric fundamental groups

Akira Sarashina

1 Introduction

Let k be a field, G_k the absolute Galois group of k, U an algebraic variety over k (i.e. a geometrically connected separated scheme of finite type over k) and $\pi_1(U)$ the étale fundamental group of U.

When k is a number field or, more generally, a field finitely generated over the prime field, the following philosophy of anabelian geometry, which is sometimes called the Grothendieck conjecture, was advocated by A.Grothendieck.

When U is an"anabelian variety", the geometry of U is determined by $\pi_1(U) \twoheadrightarrow G_k$.

When k is an algebraically closed field of characteristic 0 and U is a curve (i.e. an integral separated regular scheme of finite type over k and of dimension 1), the isomorphism class of $\pi_1(U)$ as a topological group is determined by the cardinality of cusps of U and the genus of U. Therefore the isomorphism class of U as a scheme cannot be determined only by $\pi_1(U)$.

When k is an algebraically closed field of characteristic $p > 0$, the isomorphism class of $\pi_1(U)$ cannot be determined by easy invariants such as the cardinality of cusps or the genus. Thus, we can even consider the following problem.

Is the isomorphism class of U as a scheme determined only by $\pi_1(U)$?

Regarding this problem, the following theorem is known.

Theorem 1.1 ([7]Theorem 3.5)
Let k be an algebraically closed field of characteristic $p > 0$, U a curve over k, $F \subset k$ the algebraic closure of $\mathbb{F}_p$, U_0 a curve defined over F and X_0 a smooth compactification of U_0. Assume that the genus of X_0 is 0. Then

$$\pi_1(U) \simeq \pi_1(U_0) \Leftrightarrow U \simeq U_0 \times_F k \text{ (as a scheme)}$$

■

The main result of the present paper is the following generalization of Theorem 1.1.

Theorem 1.2 (Theorem 4.9)
Let k be an algebraically closed field of characteristic $p \neq 0, 2$, U a curve over k, $F \subset k$ the algebraic

closure of $\mathbb{F}_p$, U_0 a curve defined over F and X_0 a smooth compactification of U_0. Assume that the genus of X_0 is 1 and that the cardinality of $X_0 \backslash U_0$ is 1. Then

$$\pi_1(U) \simeq \pi_1(U_0) \Leftrightarrow U \simeq U_0 \times_F k \text{ (as a scheme)}$$

In the second section, we will review the reconstruction of various invariants by $\pi_1(U)$, which will be used in the later sections.

In the third section, U is assumed to be an open subscheme of an elliptic or hyperelliptic curve. We will prove that linear relations of the images of cusps in $\mathbb{P}^1$ are encoded in $\pi_1(U)$ and a certain closed subgroup $L_U \subset \pi_1(U)$ (see the third section for the definition of L_U).

In the fourth section, U is assumed to be a curve of (1,1)-type. At first we will prove that we can apply the main theorem of the third section to certain étale covers of U. Then we will prove that the isomorphism class of U as a scheme is determined only by $\pi_1(U)$.

2 The reconstruction of various invariants ([7]§1,§2)

In this section, we will review the reconstruction of various invariants that was shown in [7].

The theorems in the first section are about curves of genus 0 or 1, while the theorems in this section are about curves of arbitrary genus.

Definition

Let k be an algebraically closed field of characteristic $p > 0$, U a curve over k (i.e. an integral separated regular scheme of finite type over k and of dimension 1), $\pi_1(U)$ the étale fundamental group of U, U_H the étale cover of U that corresponds to an open subgroup $H \subset \pi_1(U)$, $X = U^{cpt}$ the smooth compactification of U, $g(X)$ the genus of X, $S_U = X \backslash U$ the complement of U in X, n_U the cardinality of S_U, K the function field of U, K^{sep} a separable closure of K, $\tilde{K}$ the maximal Galois extension of K in K^{sep} that is unramified over U, $\tilde{X}$ the integral closure of X in $\tilde{K}$, $\tilde{S}_U$ the inverse image of S_U under $\tilde{X} \to X$, $I_{\tilde{P}}$ the inertia subgroup in $\pi_1(U)$ associated to $\tilde{P} \in \tilde{S}_U$, $I_{\tilde{P}}^{wild}$ the Sylow p-subgroup of $I_{\tilde{P}}$, $I_{\tilde{P}}^{tame} \stackrel{\text{def}}{=} I_{\tilde{P}}/I_{\tilde{P}}^{wild}$, $Sub(\pi_1(U)) \stackrel{\text{def}}{=} \{H \subset \pi_1(U) | \ H \text{ is a closed subgroup}\}$, F the algebraic closure of $\mathbb{F}_p$ in k, $(\mathbb{Q}/\mathbb{Z})' \stackrel{\text{def}}{=} \{a \in \mathbb{Q}/\mathbb{Z} \mid \text{ the order of } a \text{ is prime to } p\}$ and $F_{\tilde{P}} \stackrel{\text{def}}{=} (I_{\tilde{P}}^{tame} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})') \coprod \{*\}$ ($\{*\}$ means one point set, $\tilde{P} \in \tilde{S}_U$).

Theorem 2.1 ([7]§1,§2)

From $\pi_1(U)$

- $(g(X), n_U)$ can be recovered group-theoretically
- When $(g(X), n_U) \neq (0,0)$, p can be recovered group-theoretically
- $\pi_1(X)$ can be recovered group-theoretically as a quotient group of $\pi_1(U)$
- $\tilde{S}_U$ can be recovered group-theoretically as a subset of $Sub(\pi_1(U))$. More precisely, $\tilde{S}_U$ can be identified with a subset of $Sub(\pi_1(U))$ via $\tilde{S}_U \to Sub(\pi_1(U))$, $\tilde{P} \to I_{\tilde{P}}$, and this subset can be recovered group-theoretically.
- S_U can be recovered group-theoretically as a quotient set of $\tilde{S}_U$

- The field structure of $F_{\tilde{P}}$ obtained by identifying $F_{\tilde{P}}$ with F can be recovered group-thoretically

■

Definition

Set $I = I_{\tilde{P}}$. Let d be any positive integer. We define $\chi_{I,d}$ as follows

$$\chi_{I,d}\ :\ I \twoheadrightarrow I^{tame}/(p^d-1) = I^{tame} \otimes_{\mathbb{Z}} \frac{1}{p^d-1}\mathbb{Z}/\mathbb{Z} \hookrightarrow F_{\tilde{P}}^{\times}$$

Corollary 2.2 ([7]Corollary 2.11)

Let M be an $\mathbb{F}_p[\pi_1(U)]$-module that can be recovered group-theoretically from $\pi_1(U)$. Let $I = I_{\tilde{P}}$, $d \geq 1$ and $i \in \mathbb{Z}$. Then

$$M(\chi_{I,d}^i) \stackrel{\text{def}}{=} \{x \in M \otimes_{\mathbb{F}_p} F_{\tilde{P}} \mid \gamma x = \chi_{I,d}^i(\gamma) x\ (\gamma \in I)\}$$

can be recovered group-theoretically.

■

3 Linear relations of the images of cusps in $\mathbb{P}^1$

In this section, we will use the same symbols as in the previous sections, and we assume that $p \neq 0, 2$ and that X is an elliptic or hyperelliptic curve.

We will prove that linear relations of the images of cusps in $\mathbb{P}^1$ are encoded in $\pi_1(U)$ and a certain closed subgroup $L_U \subset \pi_1(U)$.

Definition

Let $x : X \to \mathbb{P}^1$ be a finite morphism of degree 2, $S \stackrel{\text{def}}{=} x(S_U)$, $\lambda_0, \lambda_\infty, \lambda_1, \lambda_2, \cdots, \lambda_m \in X$ ramified points of x and P_i the image of λ_i in $\mathbb{P}^1$ $(i = 0, \infty, 1, 2, \cdots, m)$. By Hurwitz's formula, m is an even number. In this section, we assume that $\lambda_0, \lambda_\infty, \lambda_1, \lambda_2, \cdots, \lambda_m \in S_U$, $S_U \backslash \{\lambda_0, \lambda_\infty, \lambda_1, \lambda_2, \cdots, \lambda_m\} \neq \emptyset$ and $x^{-1}(S) = S_U$. Let $\mu_{(1,1)}, \mu_{(1,2)}, \mu_{(2,1)}, \cdots, \mu_{(l,1)}, \mu_{(l,2)} \in S_U$ be unramified points ($\mu_{(i,1)}$ is conjugate with $\mu_{(i,2)}$), $R_1, R_2, \cdots, R_l$ the images of $\mu_{(1,1)}, \mu_{(1,2)}, \mu_{(2,1)}, \cdots, \mu_{(l,1)}, \mu_{(l,2)} \in S_U$ in $\mathbb{P}^1$.
Set $S_{U,unr} \stackrel{\text{def}}{=} \{\mu_{(1,1)}, \mu_{(1,2)}, \mu_{(2,1)}, \cdots, \mu_{(l,1)}, \mu_{(l,2)}\}$, $S_{U,ram} \stackrel{\text{def}}{=} \{\lambda_0, \lambda_\infty, \lambda_1, \lambda_2, \cdots, \lambda_m\}$,
$S_{unr} \stackrel{\text{def}}{=} \{R_1, R_2, \cdots, R_l\}$, $S_{ram} \stackrel{\text{def}}{=} \{P_0, P_\infty, P_1, P_2, \cdots, P_m\}$.
Let $I_{\tilde{\lambda}} \subset \pi_1(U)$ be the inertia group corresponding to $\tilde{\lambda} \in \tilde{X}$, $I_{\tilde{\lambda},\mathbb{P}^1} \subset \pi_1(\mathbb{P}^1 \backslash S)$ be the inertia group corresponding to $\tilde{\lambda} \in \tilde{\mathbb{P}}^1$ (Here, $\tilde{\mathbb{P}}^1$ stands for the integral closure of $\mathbb{P}^1$ in $\tilde{K}$. By definition, $\tilde{X} = \tilde{\mathbb{P}}^1$).
Set $Q \stackrel{\text{def}}{=} \pi_1(\mathbb{P}^1 \backslash S)^{ab,p'}$ (the maximal pro-prime-to-p abelian quotient of $\pi_1(\mathbb{P}^1 \backslash S)$), $L_U \stackrel{\text{def}}{=} ker(\pi_1(U) \to \pi_1(\mathbb{P}^1 \backslash S) \to Q)$ and $Q_U \stackrel{\text{def}}{=} \pi_1(U)/L_U$.
When X is a hyperelliptic curve, x is the unique finite morphism of degree 2 (up to isomorphism of $\mathbb{P}^1$, see [2]IV Propotition 5.3). When X is an elliptic curve, x is not unique (therefore, $S, Q, L_U, Q_U, S_{U,unr}, S_{unr}$, $\lambda_0, P_0, \mu_{(1,1)}, R_1$, etc., depend on the choice of x). In this section, we assume that x is fixed.

Proposition 3.1

$S_{U,ram}$, $S_{U,unr}$, S, S_{ram}, S_{unr}, Q and the natural injective map $Q_U \hookrightarrow Q$ can be recovered group-theoretically from $\pi_1(U)$ and L_U.

Proof

For each $\lambda \in S_U$, we fix $\tilde{\lambda} \in \tilde{S}_U$ above λ. We define an equivalence relation $\sim$ on S_U by saying $\nu \sim \lambda$ if $I_{\tilde{\nu}}/(I_{\tilde{\nu}} \cap L_U) = I_{\tilde{\lambda}}/(I_{\tilde{\lambda}} \cap L_U)$ (as subsets of Q_U). We can identify S with $S_U/\sim$ (see the proof of [7]Lemma 2.1). $S_{U,unr} = \{\lambda \in S_U |$ there exists $\nu \in S_U \backslash \{\lambda\}$ such that $\lambda \sim \nu$ $\}$, $S_{U,unr}$ and $S_{U,ram}$ are recovered from $\pi_1(U)$ and L_U. As S_{ram} (resp. S_{unr}) is the image of $S_{U,ram}$ (resp. $S_{U,unr}$), S_{ram} and S_{unr} are recovered from $\pi_1(U)$ and L_U.

Via the exact sequence $0 \to Q_U \to Q \to \mathbb{Z}/2\mathbb{Z}$, we can regard Q as subset of $\frac{1}{2}Q_U$. By G.A.G.A theorems ([1]Exposé 12 , Exposé 13)

$$Q \simeq (\oplus_{P\in S} I^{tame}_{\tilde{P},\mathbb{P}^1})/\Delta \ , \ I^{tame}_{\tilde{P},\mathbb{P}^1} \simeq \hat{\mathbb{Z}}^{p'} \ , \ \Delta \simeq \hat{\mathbb{Z}}^{p'}$$
$$I^{tame}_{\tilde{\lambda},\mathbb{P}^1}/I^{tame}_{\tilde{\lambda}} \simeq \mathbb{Z}/2\mathbb{Z} \ (\lambda \in S_{U,ram}) \ , \ I^{tame}_{\tilde{\lambda},\mathbb{P}^1}/I^{tame}_{\tilde{\lambda}} = 0 \ (\lambda \in S_{U,unr})$$

and

$$Q_U \simeq ((\oplus_{P\in S_{ram}} I^{tame}_{\tilde{P},\mathbb{P}^1})^* + (\sum_{P\in S_{unr}} I^{tame}_{\tilde{P},\mathbb{P}^1}))$$
$$(\ (\oplus_{\lambda\in S_{ram}} I^{tame}_{\tilde{P},\mathbb{P}^1})^* \stackrel{\text{def}}{=} ker((\oplus_{\lambda\in S_{ram}} I^{tame}_{\tilde{P},\mathbb{P}^1}) \twoheadrightarrow \oplus\mathbb{Z}/2\mathbb{Z} \stackrel{\text{sum}}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z})\ )$$

therefore

$$Q \simeq (\sum_{P\in S_{ram}} \frac{1}{2} I^{tame}_{\tilde{P}}) + (\sum_{P\in S_{unr}} I^{tame}_{\tilde{P}}) \subset \frac{1}{2}Q_U$$

By identifying Q with the right-hand side of this isomorphism, we obtain $Q_U \hookrightarrow Q$.

■

We will use the following lemma in the proof of Theorem 3.3.

Lemma 3.2

Let p be an odd prime number. For any $a_1, \cdots, a_m, b_1, \cdots, b_l \in \{0, 1, \cdots, p-1\}$ ($m \in 2\mathbb{Z}_{\geq 0}$, $l \in \mathbb{Z}_{\geq 0}$ and $(m, l) \neq (0, 0)$), $e_1, \cdots, e_m, f_1, \cdots, f_l \in \mathbb{Z}_{>0}$ with $p \nmid (\prod_{i=1}^m e_i)(\prod_{j=1}^l f_j)$ and $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_l \in \mathbb{Z}$, there exist $d_0, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l \in \mathbb{Z}_{>0}$ such that, for any $d \in \mathbb{Z}$ such that $d \geq d_0$, we have $(i) \sim (iii)$

(i) $\tilde{c} \equiv c \ mod \ p$ $\ (c = a_1, \cdots, a_m, b_1, \cdots, b_l)$

(ii) $\tilde{a}_i \equiv \alpha_i \ mod \ e_i$, $\tilde{b}_j \equiv \beta_j \ mod \ f_j$ $\ (1 \leq i \leq m \ , \ 1 \leq j \leq l)$

(iii) For all $q, t, \delta_1, \cdots, \delta_m, \epsilon_1, \cdots, \epsilon_l \in \mathbb{Z}$ $s.t.$ $0 \leq q \leq \dfrac{m}{2}$, $0 \leq t \leq \dfrac{m}{2}$,

$$0 \leq \delta_i \leq \tilde{a}_i + \frac{p^d - 1}{2} \ , \ 0 \leq \epsilon_j \leq \tilde{b}_j \text{ and } \sum_i \delta_i + \sum_j \epsilon_j = \frac{p^d - 1}{2} + s - q + tp^d \ ,$$

we have $\displaystyle\prod_{i,j} \binom{\tilde{a}_i + \frac{p^d-1}{2}}{\delta_i} \binom{\tilde{b}_j}{\epsilon_j} \equiv 0 \ mod \ p$

In particular, when $l \neq 0$ and $(m, l) \neq (0, 1)$, for any $a_1, \cdots, a_m, b_1, \cdots, b_l \in \{0, 1, \cdots, p-1\}$, there exist

$d, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l \in \mathbb{Z}_{>0}$ which satisfy $(i), (iii), (iv), (v), (vi)$.

$$(iv)\ p^d > 4s \ \ (s \overset{\text{def}}{=} \sum_{c=a_1,\cdots,a_m,b_1,\cdots,b_l} \tilde{c})$$

$$(v)\ 2|\frac{p^d-1}{(p^d-1,\tilde{c})}\ ,\ 2|\frac{p^d-1}{(p^d-1,s-1)} \ \ (c = a_1,\cdots,a_m,b_1,\cdots,b_l)$$

$$(vi)\ (p^d-1,\tilde{b_1}) = 1$$

Proof

We take any $u \in \mathbb{Z}$ such that

$$p^u > 2(\sum_i a_i + \sum_j b_j + \frac{m}{2}p + (\sum_i e_i + \sum_j f_j)p) - 1$$

$$(\iff p^u > (\sum_i a_i + \sum_j b_j + \frac{m}{2}p + (\sum_i e_i + \sum_j f_j)p) + (\sum_{h=0}^{u-1} \frac{p-1}{2}p^h)\ )$$

and set $d_0 \overset{\text{def}}{=} u+3$. We define $\tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$ to be the unique integers that satisfy (ii) and the following condition.

$$\tilde{a}_i = a_i + \frac{p+1}{2}p + \sum_{h=2}^{u} \frac{p-1}{2}p^h + A_i p \ \ (1 \le A_i \le e_i)$$

$$\tilde{b}_j = b_j + B_j p \ \ (1 \le B_j \le f_j)$$

Then for any $d \ge d_0$, we have

$$s = \sum_i a_i + \sum_j b_j + \frac{m}{2}p + \frac{m}{2}p^{u+1} + D \ \ ((m+l)p \le D \overset{\text{def}}{=} (\sum_i A_i p) + (\sum_j B_j p) \le (\sum_i e_i + \sum_j f_j)p)$$

$$\tilde{a}_i + \frac{p^d-1}{2} = a_i + \frac{p-1}{2} + \frac{p+1}{2}p^{u+1} + (\sum_{h=u+2}^{d-1} \frac{p-1}{2}p^h) + A_i p$$

$$\frac{p^d-1}{2} + s - q + tp^d = (\sum_i a_i + \sum_j b_j + \frac{m}{2}p + D - q) + (\sum_{h=0}^{d-1} \frac{p-1}{2}p^h) + \frac{m}{2}p^{u+1} + tp^d$$

Let $\sum_g a_{(i,g)}p^g\ ,\ \sum_g b_{(j,g)}p^g\ ,\ \sum_g \delta_{(i,g)}p^g\ ,\ \sum_g \epsilon_{(j,g)}p^g\ \ (a_{(i,g)}, b_{(j,g)}, \delta_{(i,g)}, \epsilon_{(j,g)} \in \{0,1,\cdots,p-1\})$ be the p-adic expansions of $\tilde{a}_i + \frac{p^d-1}{2},\ \tilde{b}_j,\ \delta_i,\ \epsilon_j$, respectively.

At first, suppose either that there exist $i \in \{1,2,\cdots,m\}, g \in \{0,1,\cdots,u-1\}$ such that $b_{(j,g)} < \epsilon_{(j,g)}$, or that there exist $j \in \{1,2,\cdots,l\}, g \in \{0,1,\cdots,u-1\}$ such that $b_{(j,g)} < \epsilon_{(j,g)}$. By Lucas' theorem ([3]),

$$\binom{\tilde{a}_i + \frac{p^d-1}{2}}{\delta_i} \equiv 0 \ mod\ p \ \ \text{or} \ \ \binom{\tilde{b}_j}{\epsilon_j} \equiv 0 \ mod\ p$$

therefore we have (iii).

Next, suppose that $a_{(i,g)} \ge \delta_{(i,g)}$ and $b_{(j,g)} \ge \epsilon_{(j,g)}$ hold for any $i \in \{1,2,\cdots,m\}, j \in \{1,2,\cdots,l\}, g \in \{0,1,\cdots,u-1\}$. Then we have

$$p^u > \sum_i a_i + \sum_j b_j + \frac{m}{2}(p-1) + D \ge (\sum_i \sum_{g=0}^{u-1} \delta_{(i,g)}p^g) + (\sum_j \sum_{g=0}^{u-1} \epsilon_{(j,g)}p^g)$$

Let η be the uth coefficient of the p-adic expansion of $(\sum_i \delta_i) + (\sum_j \epsilon_j) = \frac{p^d-1}{2} + s - q + tp^d$. Then η satisfies $\eta \equiv \sum_i \delta_{(i,u)} + \sum_j \epsilon_{(j,u)}$ $mod\ p$. And we have

$$p^u > (\sum_i a_i + \sum_j b_j + \frac{m}{2}p + D - q) + (\sum_{h=0}^{u-1} \frac{p-1}{2}p^h)$$

Then we have $\eta = \frac{p-1}{2}$. Therefore there exists $i \in \{1, 2, \cdots, m\}$ such that $\delta_{(i,u)} \neq 0$ or there exists $j \in \{1, 2, \cdots, l\}$ such that $\epsilon_{(j,u)} \neq 0$.

On the other hand, any $i \in \{1, 2 \cdots, m\}$ satisfies

$$p^u > a_i + \frac{p-1}{2} + A_i p$$

Therefore we have $a_{(i,u)} = 0$. It is clear that any j satisfies $b_{(j,u)} = 0$. By Lucas's theorem ([3]),

$$\binom{\tilde{a}_i + \frac{p^d-1}{2}}{\delta_i} \equiv 0 \ mod\ p \quad or \quad \binom{\tilde{b}_j}{\epsilon_j} \equiv 0\ mod\ p$$

Thus, in both cases, we have (iii). By definition of $\tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$, we have $(i), (ii)$. This proves the first half of the lemma.

Next, we will prove the second half of the lemma.

- Suppose $b_1 = 0$

We set $f_1 = 1$ and take any $e_1, \cdots, e_m, f_2, \cdots, f_l, \alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_l$ that satisfy $p \not| (\prod_{i=1}^m e_i)(\prod_{j=1}^l f_j)$. We apply the first half of the lemma to them. By the proof of the first half of the lemma, we can take $\tilde{b}_1 = p$. We can take a sufficiently large d that satisfies (v), because $p \neq 2$. Therefore we can take d that satisfies $(iv), (v)$ and (vi).

- Suppose $b_1 \neq 0$ and $l \equiv 0\ mod\ 2$.

By Dirichlet's theorem on arithmetic progressions, there exists $N \in \mathbb{Z}_{>0}$ such that $b_1 + p + Np^2$ is a prime number. We take $f_1 = 1 + Np$, $\beta_1 = b_1$, $e_1 = e_2 = \cdots = e_m = f_2 = \cdots = f_l = 2$, $\alpha_1 = \cdots = \alpha_m = \beta_2 = \cdots = \beta_l = 1$. We apply the first half of the lemma to them. By the proof of the first half of the lemma, we can take $\tilde{b}_1 = b_1 + p + Np^2$. Then $\tilde{b}_1$ is a prime number and $\tilde{b}_1 \geq 1 + p + p^2$, in particular $(p^2 - p, \tilde{b}_1) = 1$. Any $d \geq d_0$ satisfies (v), because $\tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l, s-1$ are odd numbers. Thus, if we take sufficiently large d that satisfies (iv), $d, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$ satisfy $(i), (iii) \sim (v)$. If $\tilde{b}_1 \nmid p^d - 1$, then we also have (vi). If $\tilde{b}_1 | p^d - 1$ (i.e. (vi) is not satisfied), we have $p^{d+1} - 1 = (p-1)(p^d + (p^{d-1} + \cdots + p + 1)) \equiv (p-1)p^d\ mod\ \tilde{b}_1$. Hence $d + 1, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$ satisfy $(i), (iii) \sim (vi)$.

- Suppose $b_1 \neq 0$ and $l \equiv 1\ mod\ 2$.

By assumption, we have $m \neq 0$ or $l \geq 3$. Suppose $l \geq 3$ (resp. $m \neq 0$). By Dirichlet's theorem on arithmetic progressions, there exists $N \in \mathbb{Z}_{>0}$ such that $b_1 + p + Np^2$ is a prime number. We take

$f_1 = 1+Np,\ \beta_1 = b_1\ f_2 = 4,\ \beta_2 = 2,\ e_1 = \cdots = e_m = f_3 = \cdots = f_l = 2,\ \alpha_1 = \cdots = \alpha_m = \beta_3 = \cdots = \beta_l = 1$ (resp. $f_1 = 1+Np,\ \beta_1 = b_1,\ e_1 = 4,\ \alpha_1 = 2,\ e_2 = \cdots = e_m = f_2 = \cdots = f_l = 2,\ \alpha_2 = \cdots = \alpha_m = \beta_2 = \cdots = \beta_l = 1$). We apply the first half of the lemma to them. By the proof of the first half of the lemma, we can take $\tilde{b}_1 = b_1 + p + Np^2$. Then $\tilde{b}_1$ is a prime number and $\tilde{b}_1 \geq 1+p+p^2$, in particular $(p^3-p, \tilde{b}_1) = 1$. $\tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l, s-1$ are odd numbers except $\tilde{b}_2$ (resp. $\tilde{a}_1$), and $\tilde{b}_2$ (resp. $\tilde{a}_1$) $\equiv 2\ mod\ 4$. Hence all $d \in 2\mathbb{Z}_{>0}$ satisfy (v). Thus, if we take sufficiently large d that satisfies (iv), $d, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$ satisfy $(i), (iii) \sim (v)$. If $\tilde{b}_1 \nmid p^d - 1$, then we also have (vi). If $\tilde{b}_1 | p^d - 1$, then we have $p^{d+2} - 1 = (p-1)(p^d(p+1) + (p^{d-1} + \cdots + p + 1)) \equiv (p-1)(p^d(p+1))\ mod\ \tilde{b}_1$. Hence $d+2, \tilde{a}_1, \cdots, \tilde{a}_m, \tilde{b}_1, \cdots, \tilde{b}_l$ satisfy $(i), (iii) \sim (vi)$.

■

Definition ([7]§3)

Let γ be an integer such that $\gamma \geq 1$, $p \not| \gamma$ and $2|\gamma$. We define

$$\tilde{H}(\mathbb{Z}/\gamma\mathbb{Z}) \stackrel{\text{def}}{=} \{(c_P)_{P\in S}, c_P \in \mathbb{Z}/\gamma\mathbb{Z} \mid (\ < c_P >_{P \in S} =\ \mathbb{Z}/\gamma\mathbb{Z}\ ) \text{ and } (\sum_{P\in S} c_P = 0)\}$$

$$H(\mathbb{Z}/\gamma\mathbb{Z}) \stackrel{\text{def}}{=} \tilde{H}(\mathbb{Z}/\gamma\mathbb{Z})/(\mathbb{Z}/\gamma\mathbb{Z})^\times$$

The natural identification $\mathrm{Surj}(Q, \mathbb{Z}/\gamma\mathbb{Z}) \simeq \tilde{H}(\mathbb{Z}/\gamma\mathbb{Z})$ and the restriction map $\mathrm{Hom}(Q, \mathbb{Z}/\gamma\mathbb{Z}) \to \mathrm{Hom}(Q_U, \mathbb{Z}/\gamma\mathbb{Z})$ yield the following map

$$H(\mathbb{Z}/\gamma\mathbb{Z}) \simeq \{H' \subset \pi_1(\mathbb{P}^1 \setminus S) : \text{open subgroup } \mid \pi_1(\mathbb{P}^1 \setminus S)/H' \simeq \mathbb{Z}/\gamma\mathbb{Z}\}$$
$$\to \{H \subset \pi_1(U) : \text{open subgroup } \mid (\ \pi_1(U)/H \simeq \mathbb{Z}/\gamma\mathbb{Z} \text{ or } \pi_1(U)/H \simeq \mathbb{Z}/\frac{1}{2}\gamma\mathbb{Z}\ ) \text{ and } L_U \subset H\}$$

Fix closed points $\rho_0 \neq \rho_\infty \in \mathbb{P}^1$. For each isomorphism $\phi : \mathbb{P}^1 \simeq \mathbb{P}^1$ with $\phi(\rho_0) = 0, \phi(\rho_\infty) = \infty$, we obtain a bijection $\mathbb{P}^1(k)\backslash\{\rho_\infty\} \simeq \mathbb{P}^1(k)\backslash\{\infty\} = k$. This bijection does not depend on the choice of ϕ up to scalar multiplication. Hence the additive structure on $\mathbb{P}^1(k)\backslash\{\rho_\infty\}$ that is induced by this bijection does not depend on the choice of ϕ, and only depends on the choice of ρ_0 and ρ_∞.

Theorem 3.3

For any $a_P \in \mathbb{F}_p$ ($P \in S \setminus \{P_0, P_\infty\}$), consider the following condition

$$\sum_{P \in S \setminus \{P_0, P_\infty\}} a_P P = P_0 \qquad \text{(with respect to the additive structure associated with } P_0 \text{ and } P_\infty)$$

Then whether this condition holds or not can be determined group-theoretically by $\pi_1(U)$ and L_U.

Proof

We define $a_1, \cdots, a_m, b_1, \cdots, b_l \in \{0, 1, \cdots, p-1\}$ by $a_i\ mod\ p = a_{P_i}$, $b_j\ mod\ p = a_{R_j}$ ($i = 1, \cdots, m$, $j = 1, \cdots, l$), and apply Lemma 3.2 to them. Then we obtain $\tilde{a}_{P_i} \stackrel{\text{def}}{=} \tilde{a}_i$, $\tilde{a}_{R_j} \stackrel{\text{def}}{=} \tilde{b}_j$, d that satisfy $(i), (iii), (iv), (v), (vi)$. Let H (resp. H') be the open subgroup of $\pi_1(U)$ (resp. $\pi_1(\mathbb{P}^1 \backslash S)$) associated with $(c_P)_{P\in S} \in H(\mathbb{Z}/(p^d-1)\mathbb{Z})$, where $c_{P_\infty} = 1$, $c_{P_0} = s-1 \stackrel{\text{def}}{=} \sum_{P \in S\setminus\{P_0,P_\infty\}} \tilde{a}_P - 1$, $c_P = -\tilde{a}_P$ ($P \neq P_0, P_\infty$).

Set $X_H \overset{\text{def}}{=} (U_H)^{cpt}$, $(\mathbb{P}^1)_{H'} \overset{\text{def}}{=} ((\mathbb{P}^1 \backslash S)_{H'})^{cpt}$,
$\phi : X_H \to X$ and $\psi : X_H \to (\mathbb{P}^1)_{H'}$.

$$\begin{array}{ccc} \mathbb{P}^1 & \xleftarrow{x} & X \\ \uparrow & & \uparrow \phi \\ (\mathbb{P}^1)_{H'} & \xleftarrow{\psi} & X_H \end{array}$$

By Lemma3.2 (vi), we have $(p^d - 1, \tilde{a}_{R_1}) = 1$. Then R_1 is totally ramified in $(\mathbb{P}^1)_{H'} \to \mathbb{P}^1$. On the other hand, by definition, R_1 is unramified in $X \to \mathbb{P}^1$. Hence the above commutative diagram is a cartesian product on generic points. In particular, the degree of $X_H \to X$ is $p^d - 1$, that is the degree of $(\mathbb{P}^1)_{H'} \to \mathbb{P}^1$. Then by Theorem 2.1 and Corollary 2.2, whether $(\pi_1(X_H)^{ab}/p)(\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}}) = 0$ holds or not can be determined group-theoretically (here, $\tilde{\mu}_{(1,1)} \in \tilde{X}$ is a point above $\mu_{(1,1)}$). By Artin-Schreier theory,

$$(\pi_1(X_H)^{ab}/p)^* \overset{\text{def}}{=} Hom(\pi_1(X_H)^{ab}/p, \mathbb{F}_p) = Hom_{cont}(\pi_1(X_H), \mathbb{F}_p) = H^1_{et}(X_H, \mathbb{F}_p) = H^1(X_H, \mathcal{O}_{X_H})[F-1]$$

This, together with [5]Proposition 9, implies

$$\begin{aligned} &(\pi_1(X_H)^{ab}/p)(\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}}) = 0 \\ \Leftrightarrow &(\pi_1(X_H)^{ab}/p)^*((\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})^{-1}) = 0 \\ \Leftrightarrow &\text{The Frobenius } F \text{ on} \sum_r H^1(X_H, \mathcal{O}_{X_H})((\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})^{-p^r}) \text{ is nilpotent} \\ \Leftrightarrow &\text{The Cartier operator } C \text{ on} \sum_r H^0(X_H, \Omega_{X_H})((\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})^{p^r}) \text{ is nilpotent} \end{aligned}$$

By fixing a suitable coordinate choice of $\mathbb{P}^1$, set $B \overset{\text{def}}{=} k[x, x^{-1}, (x-P_1)^{-1}, (x-P_2)^{-1}, \cdots, (x-P_m)^{-1}, (x-R_1)^{-1}, \cdots, (x-R_l)^{-1}][z]/ < z^2 - x(x-P_1)\cdots(x-P_m) >$, then we can write $U = SpecB$. Set $B_H \overset{\text{def}}{=} B[y]/ < y^{p^d-1} - x^{s-1} \prod_{P \in S \backslash \{P_0, P_\infty\}} (x-P)^{-\tilde{a}_P} >$, then we can write $U_H = SpecB_H$. Because $\Omega_{\mathbb{P}^1 \backslash S} = \mathcal{O}_{\mathbb{P}^1 \backslash S}(dx) = \mathcal{O}_{\mathbb{P}^1 \backslash S}(dx/x)$ and $\mathbb{P}^1 \backslash S \leftarrow U_H$ is étale, we have $\Omega_{U_H} = \mathcal{O}_{U_H}(dx/x)$. By Lemma 3.2$(vi)$, we have $(p^d - 1, \tilde{a}_{R_1}) = 1$, which implies that we have $\Gamma(U_H, \Omega_{U_H})(\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}}) = By(dx/x)$.

Let $f \in B$ and set $\omega = fy(\frac{dx}{x}) \in \Gamma(U_H, \Omega_{U_H})(\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})$. We will consider a necessary and sufficient condition for $\omega \in \Gamma(X_H, \Omega_{X_H})(\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})$. This can be checked at each $\nu \in X_H \setminus U_H$. Let t_ν be a prime element of $\mathcal{O}_{X_H,\nu}$.

- Suppose $\phi(\nu) = \lambda_\infty$

The ramification index of $\psi(\nu)$ over P_∞ is $p^d - 1$. The ramification index of $\phi(\nu) = \lambda_\infty$ over P_∞ is 2. By Abhyankar's lemma, the ramification index of ν over λ_∞ is $(p^d-1)/2$ and ν is unramified over $\psi(\nu)$. By $(dx/dt_\nu) = -x^2(dx^{-1}/dt_\nu)$ and $ord_\nu(dx^{-1}/dt_\nu) = p^d - 2$, we have $ord_\nu(dx/dt_\nu) = -p^d$, and

$$\begin{aligned} ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) &= \frac{p^d-1}{2} ord_{\lambda_\infty}(f) + 1 - p^d + (p^d - 1) \\ &= \frac{p^d-1}{2} ord_{\lambda_\infty}(f) \end{aligned}$$

therefore

$$\begin{aligned} &\omega = (fy\frac{dx}{dt_\nu}x^{-1})dt_\nu \in \Omega_{X_H,\nu} \\ \Leftrightarrow\ & ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) \geq 0 \\ \Leftrightarrow\ & ord_{\lambda_\infty}(f) \geq 0 \end{aligned}$$

- Suppose $\phi(\nu) = \lambda_0$

Set $e_{P_0} \stackrel{\text{def}}{=} (p^d - 1)/(p^d - 1, s - 1)$ which is the ramification index of $\psi(\nu)$ over P_0. By Lemma 3.2(v), we have $2|e_{P_0}$. By the same argument as above, the ramification index of ν over λ_0 is $e_{P_0}/2$ and that ν is unramified over $\psi(\nu)$. Then

$$\begin{aligned} ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) =& \frac{e_{P_0}}{2} ord_{\lambda_0}(f) + \frac{(s-1)e_{P_0}}{p^d - 1} + (e_{P_0} - 1) - e_{P_0} \\ =& \frac{e_{P_0}}{2}(ord_{\lambda_0}(f) + \frac{2((s-1) - (p^d - 1, s - 1))}{p^d - 1}) \end{aligned}$$

By Lemma 3.2(iv), we have $p^d - 1 \geq 2s > 2((s-1) - (s-1, p^d - 1)) \geq 0$. Therefore

$$\begin{aligned} &\omega = (fy\frac{dx}{dt_\nu}x^{-1})dt_\nu \in \Omega_{X_H,\nu} \\ \Leftrightarrow\ & ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) \geq 0 \\ \Leftrightarrow\ & ord_{\lambda_0}(f) \geq -\frac{2((s-1) - (p^d - 1, s - 1))}{p^d - 1} \\ \Leftrightarrow\ & ord_{\lambda_0}(f) \geq 0 \end{aligned}$$

- Suppose $\phi(\nu) = \lambda_i$ $(i = 1, 2, \cdots, m)$

Set $e_{P_i} \stackrel{\text{def}}{=} ((p^d - 1)/(p^d - 1, \tilde{a}_{P_i}))$, this is the ramification index of $\psi(\nu)$ over P_i. By Lemma 3.2(v), we have $2|e_{P_i}$. By the same argument as above, the ramification index of ν over λ_i is $e_{P_i}/2$ and ν is unramified over $\psi(\nu)$. Then

$$\begin{aligned} ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) =& \frac{e_{P_i}}{2} ord_{\lambda_i}(f) - \frac{\tilde{a}_{P_i}e_{P_i}}{p^d - 1} + (e_{P_i} - 1) \\ =& \frac{e_{P_i}}{2}(ord_{\lambda_i}(f) + 2\frac{(p^d - 1) - (\tilde{a}_{P_i} + (p^d - 1, \tilde{a}_{P_i}))}{p^d - 1}) \end{aligned}$$

By definition, $2 > 2((p^d - 1) - (\tilde{a}_{P_i} + (p^d - 1, \tilde{a}_{P_i})))/(p^d - 1)$ is clear. By Lemma 3.2(iv), we have $p^d - 1 \geq 4s > 2(\tilde{a}_{P_i} + (p^d - 1, \tilde{a}_{P_i}))$, hence $2((p^d - 1) - (\tilde{a}_{P_i} + (p^d - 1, \tilde{a}_{P_i})))/(p^d - 1) > 1$. Therefore

$$\begin{aligned} &\omega = (fy\frac{dx}{dt_\nu}x^{-1})dt_\nu \in \Omega_{X_H,\nu} \\ \Leftrightarrow\ & ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) \geq 0 \\ \Leftrightarrow\ & ord_{\lambda_i}(f) \geq -2\frac{(p^d - 1) - (\tilde{a}_{P_i} + (p^d - 1, \tilde{a}_{P_i}))}{p^d - 1}) \\ \Leftrightarrow\ & ord_{\lambda_i}(f) \geq -1 \end{aligned}$$

- Suppose $\phi(\nu) = \mu_{(i,j)}$ $(i = 1, 2, \cdots, l\ ,\ j = 1, 2)$

Set $e_{R_i} \stackrel{\text{def}}{=} ((p^d - 1)/(p^d - 1, \tilde{a}_{R_i}))$, which is the ramification index of $\psi(\nu)$ over R_i. $\mu_{(i,j)}$ is unramified over R_i. Thus the ramification index of ν over $\mu_{(i,j)}$ is e_{R_i} and ν is unramified over $\psi(\nu)$. Then

$$\begin{aligned} ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) =& e_{R_i}ord_{\mu_{(i,j)}}(f) - \frac{\tilde{a}_{R_i}e_{R_i}}{p^d-1} + (e_{R_i}-1) \\ =& e_{R_i}(ord_{\mu_{(i,j)}}(f) - \frac{\tilde{a}_{Ri} + (p^d-1, \tilde{a}_{R_i})}{p^d-1} + 1) \end{aligned}$$

By Lemma 3.2(iv), we have $p^d - 1 > \tilde{a}_{Ri} + (p^d-1, \tilde{a}_{R_i}) > 0$. Therefore

$$\begin{aligned} & \omega = (fy\frac{dx}{dt_\nu}x^{-1})dt_\nu \in \Omega_{X_H,\nu} \\ \Leftrightarrow\ & ord_\nu(fy\frac{dx}{dt_\nu}x^{-1}) \geq 0 \\ \Leftrightarrow\ & ord_{\mu_{(i,j)}}(f) \geq \frac{\tilde{a}_{Ri} + (p^d-1, \tilde{a}_{R_i})}{p^d-1} - 1 \\ \Leftrightarrow\ & ord_{\mu_{(i,j)}}(f) \geq 0 \end{aligned}$$

Set $D \overset{\text{def}}{=} \lambda_1 + \lambda_2 + \cdots + \lambda_m \in Div(X)$. By the above computation,

$$\omega \in \Omega_{X_H} \Leftrightarrow f \in \Gamma(X, \mathscr{L}(D))$$

Let K_X be the canonical divisor of X. By Hurwitz's formula, we have $g \overset{\text{def}}{=} g(X) = m/2$, and $deg(K_X) = m-2$. Thus by the Riemann-Roch theorem, we have $dim_k\Gamma(X, \mathscr{L}(D)) = g+1$. The valuations of $1, (x/z), (x^2/z), \cdots, (x^g/z) \in \Gamma(X, \mathscr{L}(D))$ at λ_0 are mutually different, hence these functions are linearly independent over k. Then we have $\Gamma(X, \mathscr{L}(D)) =< 1, (x/z), (x^2/z), \cdots, (x^g/z) >$. By Lemma 3.2($iv$) (which implies $p^d - 1 > s - 1$) and the following formula

$$C^d(x^j y^{\alpha p^d} z^{\beta p^d} \frac{dx}{x}) = \begin{cases} x^{j/p^d} y^\alpha z^\beta \frac{dx}{x} & (j \in p^d\mathbb{Z}) \\ 0 & (j \in \mathbb{Z}\backslash p^d\mathbb{Z}) \end{cases}$$

we have

$$\begin{aligned} C^d(y\frac{dx}{x}) &= C^d(x^{1-s}(x-P_1)^{\tilde{a}_{P_1}} \cdots (x-P_m)^{\tilde{a}_m}(x-R_1)^{\tilde{a}_{R_1}} \cdots (x-R_l)^{\tilde{a}_{R_l}} y^{p^d} \frac{dx}{x}) \\ &= -(a_{P_1}P_1 + \cdots + a_{P_m}P_m + a_{R_1}R_1 + \cdots + a_{R_l}R_l)y\frac{dx}{x} \end{aligned}$$

On the other hand, for any $q \in \{1, 2\cdots, g\}$, we have

$$\begin{aligned} & C^d(\frac{x^q}{z}y\frac{dx}{x}) \\ &= C^d(x^{(q+1-s+\frac{p^d-1}{2})}(x-P_1)^{(\tilde{a}_{P_1}+\frac{p^d-1}{2})} \cdots (x-P_m)^{(\tilde{a}_{P_m}+\frac{p^d-1}{2})}(x-R_1)^{\tilde{a}_{R_1}} \cdots (x-R_l)^{\tilde{a}_{R_l}} \left(\frac{y}{z}\right)^{p^d} \frac{dx}{x}) \\ &= \sum_t \sum_{(\delta_1,\cdots,\delta_m,\epsilon_1,\cdots,\epsilon_l)} (\prod_i \binom{\tilde{a}_{P_1} + \frac{p^d-1}{2}}{\delta_i} (-P_i)^{(\tilde{a}_{P_i}+\frac{p^d-1}{2}-\delta_i)})(\prod_j \binom{\tilde{a}_{R_j}}{\epsilon_j} (-R_j)^{(\tilde{a}_{R_j}-\epsilon_j)}) x^{t+1}\frac{y}{z}\frac{dx}{x} \end{aligned}$$

In this formula, t runs over all the integers that satisfy $q+1-s+((p^d-1)/2) \leq (t+1)p^d \leq q+1+(m+1)((p^d-1)/2)$ (hence $(m/2)-1 \geq t \geq 0$ by Lemma 3.2(iv)). $\delta_1, \cdots, \delta_m, \epsilon_1, \cdots, \epsilon_l$ run over all the non-negative integers that satisfy $\sum_i \delta_i + \sum_j \epsilon_j = \frac{p^d-1}{2} + s - q + tp^d$. By Lemma 3.2($iii$), for any $q \in \{1, 2, \cdots, g\}$, we have

$$C^d(\frac{x^q}{z} y \frac{dx}{x}) = 0$$

Thus, $a_{P_1}P_1 + \cdots + a_{P_m}P_m + a_{R_1}R_1 + \cdots a_{R_l}R_l = 0$ holds if and only if the Cartier operator C on $\sum_r H^0(X_H, \Omega_{X_H})((\chi_{\tilde{\mu}_{(1,1)},d}^{-\tilde{a}_{R_1}})^{p^r})$ is nilpotent. Therefore whether

$$a_{P_1}P_1 + \cdots + a_{P_m}P_m + a_{R_1}R_1 + \cdots a_{R_l}R_l = 0$$

holds or not can be determined group-theoretically from $\pi_1(U)$ and L_U.

■

4 Reconstruction of curves of (1,1)-type by their fundamental group

In this section, we consider curves of (1,1)-type, which are one-punctured elliptic curves (We are considering that the unique cusp is the identity element of the elliptic curve) . We will first prove that the linear relations of the images of m-torsion points in $\mathbb{P}^1$ are determined by the fundamental group (Corollary 4.8). Then we will use this corollary, and prove that the isomorphism class (as a scheme) of such a curve is determined by the fundamental group (Theorem 4.9). We will use the same symbols as in the previous sections for elliptic curves and their open subschemes.. Let E be a (complete) elliptic curve over k.

Proposition 4.1

Fix $\mathcal{O} \in E(k)$. Let x, x' be finite morphisms $E \to \mathbb{P}^1$ of degree 2 that are ramified at $\mathcal{O}$. Then there exists an isomorphism $\phi : \mathbb{P}^1 \simeq \mathbb{P}^1$ that satisfies $x = \phi \circ x'$.

Proof

Set $P \overset{\text{def}}{=} x(\mathcal{O}),\ P' \overset{\text{def}}{=} x'(\mathcal{O})$. When we think of P, P' as elements of $Div(\mathbb{P}^1)$, we have $\mathscr{L}(P) \simeq \mathscr{L}(P') \simeq \mathscr{O}(1)$. By definition, we have $x^*(\mathscr{L}(P)) = \mathscr{L}(2\mathcal{O}) = x'^*(\mathscr{L}(P'))$. Then both x and x' correspond to a linear system that is a subset of $|\mathscr{L}(2\mathcal{O})|$ of dimension 1. By the Riemann-Roch theorem, we have $dim|\mathscr{L}(2\mathcal{O})| = 1$. Thus both x and x' correspond to $|\mathscr{L}(2\mathcal{O})|$. By [2] II Remark 7.8.1, they are equivalent up to an isomorphism of $\mathbb{P}^1$.

■

By Proposition 4.1, when we fix a ramified point $\mathcal{O}$, for any finite set $A \subset E(k)$ that includes the four ramified points and satisfies $A = x^{-1}(x(A))$, $L_{E\backslash A}$ is unique. For any elliptic curve that has additive structure with respect to $\mathcal{O}$, we fix a finite morphisms $x : E \to \mathbb{P}^1$ of degree 2 that is ramified at $\mathcal{O}$ from now on (By Proposition 4.1, this finite morphism x is unique up to isomorphism of $\mathbb{P}^1$).

Lemma 4.2

For any $m \in \mathbb{Z}_{>0}$, the open subgroup $\pi_1(E\backslash E[m]) \subset \pi_1(E\backslash\mathcal{O})$ that corresponds to the multiplication-by-m map $[m] : E\backslash E[m] \to E\backslash\mathcal{O}$ can be recovered from $\pi_1(E\backslash\mathcal{O})$.

Proof

By Theorem 2.1, the natural morphism $\pi_1(E\backslash\mathcal{O}) \to \pi_1(E) \to \pi_1(E)/m$, hence its kernel $\pi_1(E\backslash E[m])$, can be recovered from $\pi_1(E\backslash\mathcal{O})$.

■

Theorem 4.3 (Tamagawa)

For any $m \in 2\mathbb{Z}_{>0}$ and $\mathcal{P} \in E[m]$, $L_{E\backslash E[m]}$ $(\subset \pi_1(E\backslash E[m])) \hookrightarrow \pi_1(E\backslash\mathcal{O})$ that is defined by $(E,\mathcal{P})$ can be recovered from $\pi_1(E\backslash\mathcal{O})$.

We will need some definitions and lemmas for the proof of Theorem 4.3.

Definition

Let N be a group, M a left N-module. Set $M^N \stackrel{\text{def}}{=} \{m \in M |$ for any $g \in N$, $gm = m$ $\}$, $M_N \stackrel{\text{def}}{=} M/ < gm - m \mid g \in N, m \in M >$, $M^\vee \stackrel{\text{def}}{=} Hom_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ (the action of N on $\mathbb{Q}/\mathbb{Z}$ is trivial).

Lemma 4.4

Let k be an algebraically closed field of characteristic $p \geq 0$, l a prime that is not p, X and Y curves over k, $X \to Y$ a finite morphism over k, U (resp. V) a non-empty open subscheme of X (resp. Y). Suppose that $X \to Y$ restricts to a Galois cover $U \to V$. Let G be the Galois group of $U \to V$. Then we get a natural isomorphism

$$((\pi_1(X)^{ab,l})_G) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq (\pi_1(Y)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

Proof

Applying [4]Corollary 7.2.5 (Hochschild-Serre spectral sequence) to the natural exact sequence $1 \to \pi_1(U) \to \pi_1(V) \to G \to 1$, we get an exact sequence

$$0 \to H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^1(\pi_1(V), \mathbb{Q}/\mathbb{Z}) \to H^1(\pi_1(U), \mathbb{Q}/\mathbb{Z})^G \to H^2(G, \mathbb{Q}/\mathbb{Z})$$

By the general property of homological algebra $H^1(N, \mathbb{Q}/\mathbb{Z}) \simeq Hom(N^{ab}, \mathbb{Q}/\mathbb{Z})$ and [4]Theorem 2.9.6(Pontryagin duality), We get an exact sequence

$$0 \leftarrow G^{ab} \leftarrow \pi_1(V)^{ab} \leftarrow (\pi_1(U)^{ab})_G \leftarrow H^2(G, \mathbb{Q}/\mathbb{Z})^\vee$$

Take the l-Sylow subgroups and the tensor products with $\mathbb{Q}_l$, we have

$$0 \leftarrow G^{ab,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \leftarrow (\pi_1(V)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \leftarrow ((\pi_1(U)^{ab,l})_G) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \leftarrow H^2(G, \mathbb{Q}_l/\mathbb{Z}_l)^\vee \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

Since $G^{ab,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $H^2(G, \mathbb{Q}_l/\mathbb{Z}_l)^\vee \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ are torsion $\mathbb{Q}_l$ vector spaces, they are trivial. Then we have

$$((\pi_1(U)^{ab,l})_G) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq (\pi_1(V)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

By the general theory of étale fundamental groups (cf, [1] Exposé V, corollaire 2.4), the kernel of $((\pi_1(V)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \to (\pi_1(Y)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$ is $A \stackrel{\text{def}}{=} (\Sigma_{P \in Y\backslash V} I_P) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and the kernel of $((\pi_1(U)^{ab,l})_G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \to (\pi_1(X)^{ab,l})_G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$ is $B \stackrel{\text{def}}{=}$ (the image of $(\Sigma_{P \in X\backslash U} I_P) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ in $(\pi_1(U)^{ab,l})_G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$) (Here, for

$P \in Y\backslash V$ (resp. $P \in X\backslash U$), I_P stands for the image of the inertia subgroup at P in $\pi_1(V)^{ab,p'}$ (resp. $\pi_1(U)^{ab,p'}$)). Observe that $((\pi_1(U)^{ab,l})_G) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \xrightarrow{\sim} (\pi_1(V)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ sends A onto B. Therefore we have

$$((\pi_1(X)^{ab,l})_G) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq (\pi_1(Y)^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

■

Definition

Let M be an abelian group equipped with a $\mathbb{Z}/2\mathbb{Z}$-action. We define $M^+ \stackrel{\text{def}}{=} M^{\mathbb{Z}/2\mathbb{Z}}$, $M^- \stackrel{\text{def}}{=} \{a \in M | \tau a = -a\}$, where τ is the unique generator of $\mathbb{Z}/2\mathbb{Z}$.

Let m be an even positive integer. The Galois group of $E\backslash E[m] \to \mathbb{P}^1\backslash S$ acts on $E\backslash E[m]$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Lemma 4.5

$$(\pi_1(E\backslash E[m])^{ab,p'})^- = ker(\pi_1(E\backslash E[m])^{ab,p'} \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'})$$

Proof

By G.A.G.A Theorems, $\pi_1(\mathbb{P}^1\backslash S)^{ab,p'}$ is a free $\hat{\mathbb{Z}}^{p'}$-module. It is clear that $ker(\pi_1(E\backslash E[m])^{ab,p'} \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'})$ contains $(\pi_1(E\backslash E[m])^{ab,p'})^-$. Thus, we have a natural surjective morphism

$$\pi_1(E\backslash E[m])^{ab,p'}/(\pi_1(E\backslash E[m])^{ab,p'})^- \twoheadrightarrow R,$$

where $R \stackrel{\text{def}}{=} Im(\pi_1(E\backslash E[m])^{ab,p'} \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'})$. At first we will prove that R is a free $\hat{\mathbb{Z}}^{p'}$-module. We have a short exact sequence

$$1 \to R \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'} \to \mathbb{Z}/2\mathbb{Z} \to 1$$

Because R and $\pi_1(\mathbb{P}^1\backslash S)^{ab,p'}$ are profinite abelian groups, we have $R^{2'} \simeq \pi_1(\mathbb{P}^1\backslash S)^{ab,p',2'}$ and $1 \to R^2 \to \pi_1(\mathbb{P}^1\backslash S)^{ab,2} \to \mathbb{Z}/2\mathbb{Z} \to 1$ (here, R^2 stands for the Sylow 2-subgroup of R). This exact sequence is a sequence of $\mathbb{Z}_2$-modules and $\mathbb{Z}_2$ is a PID, therefore R^2 is a free $\mathbb{Z}_2$-module and $rank_{\mathbb{Z}_2}(R^2) = rank_{\mathbb{Z}_2}(\pi_1(\mathbb{P}^1\backslash S)^{ab,2})$. Thus R is a free $\hat{\mathbb{Z}}^{p'}$-module and $rank_{\hat{\mathbb{Z}}^{p'}}(R) = rank_{\hat{\mathbb{Z}}^{p'}}(\pi_1(\mathbb{P}^1\backslash S)^{ab,p'})$.

Let $((\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}})_T$ be the torsion subgroup of $(\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}}$. By Lemma 4.4, we have $(\pi_1(E\backslash E[m])^{ab,l})_{\mathbb{Z}/2\mathbb{Z}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq \pi_1(\mathbb{P}^1\backslash S)^{ab,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ for any prime number l that is not p. From this, we deduce $(\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}}/((\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}})_T \simeq R$. By an easy computation, we have $2((\pi_1(E\backslash E[m])^{ab,p'})^-) \subset (\tau - 1)(\pi_1(E\backslash E[m])^{ab,p'}) \subset (\pi_1(E\backslash E[m])^{ab,p'})^-$ and that $\pi_1(E\backslash E[m])^{ab,l}/(\pi_1(E\backslash E[m])^{ab,l})^-$ is torsion free. Thus we have

$$\pi_1(E\backslash E[m])^{ab,p'}/(\pi_1(E\backslash E[m])^{ab,p'})^- \simeq (\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}}/((\pi_1(E\backslash E[m])^{ab,p'})_{\mathbb{Z}/2\mathbb{Z}})_T \simeq R$$

■

Lemma 4.6

$$(\pi_1(E\backslash E[m])^{ab,p'})^{E[m]} \subset (\pi_1(E\backslash E[m])^{ab,p'})^-$$

Proof

$[m] : E\backslash E[m] \to E\backslash\{\mathcal{O}\}$ is a Galois cover with Galois group $E[m]$ (when $p|m$, $[m] : E \to E$ is decomposed uniquely as $[m] = [m]' \circ \phi$, where $[m]' : E' \to E$ (resp. $\phi : E \to E'$) is a separable (resp. purely inseparable) isogeny of eliptic curves, and we consider $[m]' : E' \to E$ instead of $[m] : E \to E$). $E\backslash E[2] \to \mathbb{P}^1\backslash\{0, 1, \lambda, \infty\}$ is a Galois cover with Galois group $\mathbb{Z}/2\mathbb{Z}$. $[m] : E \to E$ is the unique maximal abelian cover whose Galois group is killed by m. Then $E\backslash E[2m] \overset{[m]}{\to} E\backslash E[2] \to \mathbb{P}^1\backslash\{0, 1, \lambda, \infty\}$ is a Galois cover with Galois group $G \overset{\text{def}}{=} E[m] \rtimes \mathbb{Z}/2\mathbb{Z}$. By Lemma 4.4, we have $(\pi_1(E\backslash E[m])^{ab,l})_G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq (\pi_1(\mathbb{P}^1\backslash\{\infty\})^{ab,l}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = 0$ (for each $l \neq p$). Because G is a finite group and $\mathbb{Q}_l$ is a field of characteristic 0, then we have $(\pi_1(E\backslash E[m])^{ab,l})^G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq (\pi_1(E\backslash E[m])^{ab,l})_G \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = 0$. As $(\pi_1(E\backslash E[m])^{ab,l})^G$ is a free $\mathbb{Z}_l$-module, then $((\pi_1(E\backslash E[m])^{ab,l})^{E[m]})^+ = (\pi_1(E\backslash E[m])^{ab,l})^G = 0$. Therefore $(\pi_1(E\backslash E[m])^{ab,l})^{E[m]} \subset (\pi_1(E\backslash E[m])^{ab,l})^-$, hence $(\pi_1(E\backslash E[m])^{ab,p'})^{E[m]} \subset (\pi_1(E\backslash E[m])^{ab,p'})^-$

■

Let W be the sum of all inertia subgroups in $\pi_1(E\backslash E[m])^{ab,p'}$. By G.A.G.A theorems, W is isomorphic to $(\oplus_{P\in E[m]}\hat{\mathbb{Z}}^{p'})/\Delta(\hat{\mathbb{Z}}^{p'})$, where $\hat{\mathbb{Z}}^{p'}$ at each $P \in E[m]$ corresponds to the inertia subgroup at P and $\Delta(\hat{\mathbb{Z}}^{p'})$ stands for the diagonal. W is closed under the action of the Galois group of $E\backslash E[2m] \overset{[m]}{\to} E\backslash E[2] \to \mathbb{P}^1\backslash\{0, 1, \lambda, \infty\}$.

Lemma 4.7

$$\#(\pi_1(E\backslash E[m])^{ab,p'})^-/(W^- \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}) < \infty$$

Proof

At first, we prove $\#(\pi_1(E\backslash E[m])^{ab,p'})/(W \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}) < \infty$. We consider the following diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & W & \longrightarrow & \pi_1(E\backslash E[m])^{ab,p'} & \longrightarrow & \pi_1(E)^{p'} & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & W^{E[m]} & \longrightarrow & (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]} & \longrightarrow & (\pi_1(E)^{p'})^{E[m]} & \longrightarrow & C \longrightarrow 1
\end{array}$$

Where C is the cokernel of $(\pi_1(E\backslash E[m])^{ab,p'})^{E[m]} \to (\pi_1(E)^{ab,p'})^{E[m]}$. Note that $\pi_1(E)$ is abelian.

The two horizontal sequences are exact. C is a subgroup of $H^1(E[m], W)$. $E[m]$ acts transitively on $E[m]$, hence we have $W^{E[m]} = 1$. Let P be an element of $E[m]$. We have the following commutative diagram.

$$\begin{array}{ccc}
\pi_1(E)^{p'} & \xrightarrow{\pi_1(+P)} & \pi_1(E)^{p'} \\
 & {\scriptstyle \pi_1([m])} \searrow \quad \swarrow {\scriptstyle \pi_1([m])} & \\
 & \pi_1(E)^{p'} &
\end{array}$$

This implies that $E[m]$ acts trivially on $\pi_1(E)^{p'}$, hence we have $(\pi_1(E)^{ab,p'})^{E[m]} = \pi_1(E)^{ab,p'}$. By chasing the diagram, we have $W \cap (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]} = W^{E[m]} = 1$ (in $\pi_1(E\backslash E[m])^{ab,p'}$) and

$\pi_1(E\backslash E[m])^{ab,p'}/(W \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}) \simeq C$. By the general property of homological algebra, we have $(\#(E[m])) \cdot H^1(E[m], W) = 1$. Thus we have $(\#(E[m])) \cdot ((\pi_1(E\backslash E[m])^{ab,p'})/(W \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]})) = 0$. As $\pi_1(E\backslash E[m])^{ab,p'}$ is a finitely generated $\hat{\mathbb{Z}}^{p'}$-module, this shows $\#(\pi_1(E\backslash E[m])^{ab,p'})/(W \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]})) < \infty$

By definition, $((\pi_1(E\backslash E[m])^{ab,p'})^-) \cap (W \oplus ((\pi_1(E\backslash E[m]))^{ab,p'})^{E[m]}) = W^- \oplus ((\pi_1(E\backslash E[m]))^{ab,p'})^{E[m]}$. Then we have a natural injective homomorphism $(\pi_1(E\backslash E[m])^{ab,p'})^-/(W^- \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}) \hookrightarrow (\pi_1(E\backslash E[m])^{ab,p'})/(W \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]})$. Thus, $\#(\pi_1(E\backslash E[m])^{ab,p'})^-/(W^- \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}) < \infty$.

■

Proof of Theorem 4.3

By Theorem 2.1 and Lemma 4.2, $\pi_1(E\backslash E[m])^{ab,p'}$ can be recovered from $\pi_1(E\backslash \mathcal{O})$. Then if $ker(\pi_1(E\backslash E[m])^{ab,p'} \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'})$ could be recovered, $L_{E\backslash E[m]}$ could be recovered. By Lemma 4.7 and the fact that R (see the proof of Lemma 4.5) is torsion free, we have $ker(\pi_1(E\backslash E[m])^{ab,p'} \to \pi_1(\mathbb{P}^1\backslash S)^{ab,p'}) = \{a \in \pi_1(E\backslash E[m])^{ab,p'} | \text{ for some } n \in \mathbb{N},\ na \in W^- \oplus (\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}\}$. It is clear that the action of $E[m]$ on $\pi_1(E\backslash E[m])^{ab,p'}$ can be recovered from $\pi_1(E\backslash \mathcal{O})$, hence $(\pi_1(E\backslash E[m])^{ab,p'})^{E[m]}$ can be recovered from $\pi_1(E\backslash \mathcal{O})$. Recall that W is isomorphic to $(\oplus_{P\in E[m]}\hat{\mathbb{Z}}^{p'})/\Delta(\hat{\mathbb{Z}}^{p'})$. Let pr_P be a projection map $\oplus_{P\in E[m]}\hat{\mathbb{Z}}^{p'} \to \hat{\mathbb{Z}}^{p'}$ at P and i_P an isomorphism $\Delta(\hat{\mathbb{Z}}^{p'}) \to \oplus_{P\in E[m]}\hat{\mathbb{Z}}^{p'} \stackrel{pr_P}{\to} \hat{\mathbb{Z}}^{p'}$. Then $W^- =< i_P(a) - i_{-P}(a) | a \in \Delta(\hat{\mathbb{Z}}^{p'}), P \in E[m] >$. By Theorem 2.1, $E[m]$ can be recovered as (a quotient of) the set of inertia subgroups from $\pi_1(E\backslash E[m])$. Then W, the additive structure on $E[m]$ with identity element $\mathcal{P}$ (cf. the proof of Theorem 4.9 below) and the action of $E[m]$ on W can be recovered from $\pi_1(E\backslash \mathcal{O})$. Therefore W^- can be recovered from $\pi_1(E\backslash \mathcal{O})$. Hence $L_{E\backslash E[m]}$ can be recovered from $\pi_1(E\backslash \mathcal{O})$.

■

Corollary 4.8

For any even integer m that is bigger than 2 and $a_P \in \mathbb{F}_p$ $(P \in x(E[m])\backslash\{P_0 = x(\lambda_0), P_\infty = x(\lambda_\infty)\})$, whether the following linear relations holds or not can be determined by $\pi_1(E\backslash \mathcal{O})$.

$$\sum_{P\in x(E[m])\backslash\{P_0,P_\infty\}} a_P P = P_0 \qquad \text{(with respect to the additive structure associated with } P_0 \text{ and } P_\infty)$$

Proof

This is established by Theorem 3.3 and Theorem 4.3.

■

Recall that F means the algebraic closure of $\mathbb{F}_p$ in k.

Theorem 4.9

Let U be a curve over k. Supose E is defined over F (i.e. there exists a curve E' over F that satisfies

$E \simeq E' \times_F k$). Then the following equivalence holds.

$$\pi_1(U) \simeq \pi_1(E \backslash \mathcal{O}) \Leftrightarrow U \simeq E \backslash \mathcal{O} \text{ (as schemes)}$$

Proof

($\Leftarrow$) is clear. Thus it is sufficient to show ($\Rightarrow$). Fix an isomorphisms $\pi_1(E\backslash\mathcal{O}) \simeq \pi_1(U)$.

By Theorem 2.1, the genus of $X \stackrel{\text{def}}{=} U^{cpt}$ is 1, and $\#(X\backslash U) = 1$. Set $X\backslash U = \{\mathcal{O}'\}$. We consider the additive structure on E (resp. X) defined by the elliptic curve $(E, \mathcal{O})$ (resp. $(X, \mathcal{O}')$). Let m be an even number bigger than 2. Then the isomorphism $\pi_1(E\backslash\mathcal{O}) \simeq \pi_1(U)$ induces an isomorphism $\pi_1(E\backslash E[m]) \simeq \pi_1(X\backslash X[m])$ by Lemma 4.2, which induces a bijection $\phi : E[m] \simeq X[m]$ by Theorem 2.1. We may consider a unique translation of X that sends $\phi(\mathcal{O})$ to $\mathcal{O}'$, and assume $\phi(\mathcal{O}) = \mathcal{O}'$. By using the group isomorphisms $E[m] \simeq Aut((E\backslash E[m])/(E\backslash\mathcal{O}))$ $(Q \mapsto (R \mapsto R + Q))$, $X[m] \simeq Aut((X\backslash X[m])/(X\backslash\mathcal{O}')$, we see that ϕ is a group isomorphism.

By taking suitable closed immersions to $\mathbb{P}^2$, we may assume that X is defined by $y^2 = x(x-1)(x-\lambda)$, $\mathcal{O}' = \infty$, E is defined by $y^2 = x(x-1)(x-\lambda_E)$, $\mathcal{O} = \infty$, $\phi((\lambda_E, 0)) = (\lambda, 0)$ and $\phi((i, 0)) = (i, 0)$ $(i = 0, 1)$.

For any $P \in k \simeq \mathbb{P}^1(k)\backslash\{\infty\}$, let $\alpha(P)$ (resp.$\beta(P)$) be a point of E (resp.X) above P. For any P except $0, 1, \lambda_E$ (resp. λ), there exist two points above P, but we choose α and β that satisfy $\phi(E[m] \cap Im(\alpha)) = X[m] \cap Im(\beta)$.

Set $P, Q, P', Q' \in \mathbb{P}^1(k)\backslash\{\infty\}$. Suppose $\alpha(P), \alpha(Q), \alpha(P+Q) \in E[m]$, $\phi(\alpha(P)) = \beta(P')$, $\phi(\alpha(Q)) = \beta(Q')$. By the equation $x(\alpha(P+Q)) - x(\alpha(P)) - x(\alpha(Q)) = 0$ and Corollaly 4.8, we have $x(\phi(\alpha(P+Q))) - x(\beta(P')) - x(\beta(Q')) = 0$. Thus,

$$\begin{aligned}\alpha(P), \alpha(Q), \alpha(P+Q) \in E[m]\ ,\ \phi(\alpha(P)) = \beta(P')\ ,\ \phi(\alpha(Q)) = \beta(Q')\\ \Rightarrow \phi(\alpha(P+Q)) = \beta(P'+Q')\end{aligned}$$

By [6]Theorem 1.16 (Addition theorem), for any $a, b \in \mathbb{F}_p$ $(b \neq 0)$,

$$\begin{aligned}x(\alpha(aP) + \alpha(aP+b)) + x(\alpha(aP) - \alpha(aP+b)) =& \frac{2}{b^2}(a^3P^3 + (3b - 2 - 2\lambda_E)a^2P^2 + (2 - 2b)a\lambda_E P)\\ &+ \frac{2}{b}\lambda_E - 4aP + (6 - \frac{4}{b})\end{aligned}$$

and

$$\begin{aligned}x(\beta(aP') + \beta(aP'+b)) + x(\beta(aP') - \beta(aP'+b)) =& \frac{2}{b^2}(a^3P'^3 + (3b - 2 - 2\lambda)a^2P'^2 + (2 - 2b)a\lambda P')\\ &+ \frac{2}{b}\lambda - 4aP' + (6 - \frac{4}{b})\end{aligned}$$

Suppose $a = \pm 1$, $b = 1$. Then

$$\begin{aligned}x(\alpha(P) + \alpha(P+1)) + x(\alpha(P) - \alpha(P+1)) + x(\alpha(-P) + \alpha(-P+1)) + x(\alpha(-P) - \alpha(-P+1))\\ = -4\lambda_E P^2 + 2P^2 + 4\lambda_E + 4\end{aligned}$$

and

$$x(\beta(P')+\beta(P'+1))+x(\beta(P')-\beta(P'+1))+x(\beta(-P')+\beta(-P'+1))+x(\beta(-P')-\beta(-P'+1))$$
$$=-4\lambda P'^2+2P'^2+4\lambda+4$$

Therefore, by Corollary 4.8,

$$\begin{aligned}&\alpha(\pm P),\alpha(\pm P+1),\alpha(P^2),\alpha(\lambda_E P^2)\in E[m]\ ,\ \phi(\alpha(P))=\beta(P')\ ,\ \phi(\alpha(P^2))=\beta(P'^2)\\&\Rightarrow\ \phi(\alpha(\lambda_E P^2))=\beta(\lambda P'^2)\end{aligned}\tag{1}$$

Suppose $a=1,\ b=\pm 1$. Then

$$x(\alpha(P)+\alpha(P+1))+x(\alpha(P)-\alpha(P+1))-x(\alpha(P)+\alpha(P-1))-x(\alpha(P)-\alpha(P-1))$$
$$=6P^2-4\lambda_E P+4\lambda_E-8$$

and

$$x(\beta(P')+\beta(P'+1))+x(\beta(P')-\beta(P'+1))-x(\beta(P')+\beta(P'-1))-x(\beta(P')-\beta(P'-1))$$
$$=6P'^2-4\lambda_E P'+4\lambda_E-8$$

Therefore, by Corollary 4.8, when $p\neq 3$,

$$\begin{aligned}&\alpha(P),\alpha(P\pm 1),\alpha(\lambda_E P),\alpha(P^2)\in E[m]\ ,\ \phi(\alpha(P))=\beta(P')\ ,\ \phi(\alpha(\lambda_E P))=\beta(\lambda_E P')\\&\Rightarrow\phi(\alpha(P^2))=\beta(P'^2)\end{aligned}\tag{2}$$

When $p=3$,

$$\begin{aligned}&\alpha(P),\alpha(P\pm 1),\alpha(\lambda_E P)\in E[m]\ ,\ \phi(\alpha(P))=\beta(P')\\&\Rightarrow\phi(\alpha(\lambda_E P))=\beta(\lambda P')\end{aligned}\tag{3}$$

By using [6]Theorem 1.16 (Addition theorem) again, we have

$$x(\alpha(\lambda_E)+\alpha(\lambda_E+1))=\lambda_E^2$$
$$x(\beta(\lambda)+\beta(\lambda+1))=\lambda^2$$

Therefore, by Corollary 4.8,

$$\alpha(\lambda_E+1),\alpha(\lambda_E^2)\in E[m]\Rightarrow\ \phi(\alpha(\lambda_E^2))=\beta(\lambda^2)\tag{4}$$

Let f be a minimal polynomial of λ_E over $\mathbb{F}_p$. We take m such that $\alpha(-\lambda_E),\alpha(\lambda_E-1),\alpha(\pm\lambda_E+1),\alpha(\pm\lambda_E^2),\alpha(\lambda_E^2-1),\alpha(\pm\lambda_E^2+1),\alpha(\pm\lambda_E^3),\cdots,\alpha(\pm\lambda_E^{degf-1}),\alpha(\lambda_E^{degf-1}-1),\alpha(\pm\lambda_E^{degf-1}+1),\alpha(\lambda_E^{degf})\in E[m]$. We will prove $\phi(\alpha(\lambda_E^i))=\beta(\lambda^i)\ \ (i=0,1,\cdots,degf)$ by induction.

Suppose $p=3$.
By (3), for any $i=1,2,\cdots,degf-1$,

$$\phi(\alpha(\lambda_E^i))=\beta(\lambda^i)\Rightarrow\phi(\alpha(\lambda_E^{i+1}))=\beta(\lambda^{i+1})$$

Thus, by induction, we have $\phi(\alpha(\lambda_E^i))=\beta(\lambda^i)\ \ (i=0,1,\cdots,degf)$.

Suppose $p \neq 3$.
By (1), for any $i = 1, 2, \cdots, degf - 1$,

$$i \equiv 0 \ mod \ 2 \ , \ \phi(\alpha(\lambda_E^{i/2})) = \beta(\lambda^{i/2}) \ , \ \phi(\alpha(\lambda_E^{i})) = \beta(\lambda^{i}) \\ \Rightarrow \phi(\alpha(\lambda_E^{i+1})) = \beta(\lambda^{i+1})$$

By (2),

$$i \equiv 1 \ mod \ 2 \ , \ i \neq 1 \ , \ \phi(\alpha(\lambda_E^{(i+1)/2})) = \beta(\lambda^{(i+1)/2}) \ , \ \phi(\alpha(\lambda_E^{(i+3)/2})) = \beta(\lambda^{(i+3)/2}) \\ \Rightarrow \phi(\alpha(\lambda_E^{i+1})) = \beta(\lambda^{i+1})$$

By (4),

$$i = 1 \Rightarrow \phi(\alpha(\lambda_E^{i+1})) = \beta(\lambda^{i+1})$$

Thus, by induction, we have $\phi(\alpha(\lambda_E^{i})) = \beta(\lambda^{i}) \ \ (i = 0, 1, \cdots, degf)$.

By Corollary 4.8, we conclude $f(\lambda) = 0$. Therefore there exists an isomorphism $\varphi : k \simeq k$ that satisfies $\varphi(\lambda_E) = \lambda$. Thus,

$$E\backslash\{\mathcal{O}\} \simeq (E\backslash\{\mathcal{O}\}) \times_{k,\varphi} k \simeq U$$

■

Corollary 4.10
Suppose that E is defined over F. Let $S_E \subset E(k)$ be a finite set that is not empty and U a curve over k. Then the following implication holds.

$$\pi_1(U) \simeq \pi_1(E\backslash S_E) \Rightarrow U^{cpt} \simeq E \text{ (as schemes)}$$

Proof
Fix $P \in S_E$. By Theorem 2.1, the isomorphism $\pi_1(U) \simeq \pi_1(E\backslash S_E)$ induces an isomorphism $\pi_1(U^{cpt}\backslash P') \simeq \pi_1(E\backslash \mathcal{P})$ for some $P' \in (U^{cpt}\backslash U)(k)$. By applying Theorem 4.9 to the latter isomorphism, we obtain $U^{cpt}\backslash P' \simeq E\backslash P$, hence $U^{cpt} \simeq E$.

■

Acknowledgments

I am grateful to Professor Akio Tamagawa for helpful discussions. I also thank Koichiro Sawada for many useful comments.

References

[1] Grothendieck, A. , *Revêtemental étales et groupe fondamental (SGA1)*, Lecture Notes in Mathematics 224, Springer-Verlag, 1971

[2] Hartshorne, R. , *Algebraic Geometry*, Graduate Texts in Mathematics ; 52, Springer-Verlag, New York Inc., 1977

[3] Lucas, E. , *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., 1 (2), 184-196; 1 (3), 197-240; 1 (4), 289-321 , 1878

[4] Ribes, L. and Zalesskii, P., *Profinite Groups*, Second edition, Springer-Verlag, Berlin Heidelberg, 2010

[5] Serre, J.-P. , *Sur la topologie des variétés algébriques en caractéristique* p, Symposium internacional de topología algebraica, pp. 24-53, Universidad Nacional Autónoma de México and UNESCO, Mexico City , 1958

[6] Schmitt, S. , Zimmer, H.G. , *Elliptic Curves: A Computational Approach*, Walter de Gruyter GmbH & Co. KG, Berlin, Germany, 2003

[7] Tamagawa, A. , *On the fundamental groups of curves over algebraically closed fields of characteristic* > 0, Internat. Math. Res. Notices 1999, no.16, 853-873