RIMS-1939

Reconstruction of open subschemes of elliptic curves in positive characteristic by their geometric fundamental groups under some assumptions

By

Akira Sarashina

February 2021

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

Reconstruction of open subschemes of elliptic curves in positive characteristic by their geometric fundamental groups under some assumptions

Akira Sarashina

Abstract

The goal of this paper is the reconstruction of the isomorphism class of a nonempty open subscheme of an elliptic curve over an algebraic closure of a finite field by its étale fundamental group under some assumptions. First we will prove a certain general property of elliptic curves over finite fields. This shows the existence of linear relations of the cusps. On the other hand, the author's previous work shows that the existence of linear relations of the cusps can be characterized by the étale fundamental group and a certain subgroup. By combining these results, we prove the main reconstruction result.

1 Introduction

This paper consists of three parts related to each other.

1.1 Elliptic Curves

First we will discuss general properties of elliptic curves over finite fields. More precisely, we will show a certain relation between the group structure on elliptic curves and the additive structure on $\mathbb{P}^1$ as follows.

Let p be a prime number, let $q = p^n$ $(n \geq 1)$, and E an elliptic curve over $\mathbb{F}_q$ which is defined by a nonsingular Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

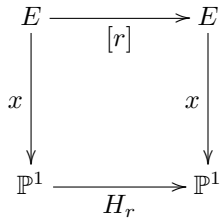
where a_1, a_2, a_3, a_4, $a_6 \in \mathbb{F}_q$. Let $\mathcal{O}$ be the identity element of E,

$$x : E \to \mathbb{P}^1$$

the finite morphism of degree 2 such that $x((a, b)) = a$ and $x(\mathcal{O}) = \infty$.

Definition. For any positive integer r, let H_r be the endmorphism of $\mathbb{P}^1$ which

makes the following diagram commutative.



Here, $[r]$ stands for the multiplication by r.

For any endmorphism f of E, set

$$E[f] \stackrel{\text{def}}{=} \{P \in E(\overline{\mathbb{F}}_p) \mid f(P) = \mathcal{O}\}.$$

If $f = [r]$, we write $E[r]$ as $E[[r]]$.

The main result of the first part is the following.

Theorem 1.1 (cf. Theorem 2.6)**.** Let m be a positive integer. Then there exists a positive even integer r which satisfies the following.

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p})$$

Here, $\langle x(E[r])\setminus\{\infty\}\rangle_{\mathbb{F}_p}$ stands for the $\mathbb{F}_p$-vector subspace generated by $x(E[r])\setminus\{\infty\}$ in $\overline{\mathbb{F}}_p = \mathbb{A}^1(\overline{\mathbb{F}}_p)$. □

An equality $H_r(x(E[r])) = \{\infty\}$ clearly holds. So $\langle - \rangle_{\mathbb{F}_p}$ on the right hand side of the main result is necessary, and the main result shows a relation between the group structure on elliptic curves and the additive structure on $\mathbb{P}^1$. Let $P \in E(\overline{\mathbb{F}}_p)$.

$$x(P) \in H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p})$$

holds if and only if we have

$$x([r]^{-1}(P)) \cap \langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p} \neq \phi.$$

This means that at least one of the points of $x([r]^{-1}(P))$ can be written as a linear combination of the points of $x(E[r]) \setminus \{\infty\}$.

1.2 Anabelian Geometry

In the second part, we will discuss an application of Theorem 1.1 to anabelian geometry. Theorem 1.1 shows the existence of linear relations, and [3] Theorem 3.3 (cf. Lemma 3.4) shows that the existence of linear relations can be characterized by the étale fundamental groups under some assumptions.

Let U_1 and U_2 be nonempty affine open subschemes of elliptic curves $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ over $\overline{\mathbb{F}}_p$ respectively such that

$$\alpha_1 : \pi_1(U_1) \stackrel{\sim}{\to} \pi_1(U_2).$$

The goal of this section is to prove the following isomorphism under some assumptions.

$$U_1 \simeq U_2$$

Theorem 1.2 ([3] Corollary 4.10)**.** We have the following isomorphism of $\mathbb{F}_p$-schemes.

$$E_1 \simeq E_2$$

□

We identify E_1 with E_2 and write $(E, \mathcal{O})$ instead of $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$.
By a similar argument to [3] Lemma 4.2, α_1 induces

$$\alpha_s : \pi_1([s]^{-1}(U_1)) \xrightarrow{\sim} \pi_1([s]^{-1}(U_2))$$

for each $s > 0$, which makes the following diagram commutative.

$$\begin{array}{ccc} \pi_1([s]^{-1}(U_1)) & \xrightarrow[\alpha_s]{\sim} & \pi_1([s]^{-1}(U_2)) \\ \downarrow & & \downarrow \\ \pi_1(U_1) & \xrightarrow[\alpha_1]{\sim} & \pi_1(U_2) \end{array}$$

Set $S_1 \overset{\text{def}}{=} E \setminus U_1$ and $S_2 \overset{\text{def}}{=} E \setminus U_2$. By [4] Theorem 2.5, α_s naturally induces a bijection

$$\phi_s : [s]^{-1}(S_1) \simeq [s]^{-1}(S_2)$$

for each $s > 0$. By [4] Corollary 1.10, α_1 naturally induces an isomorphism

$$\theta : \pi_1(E) \simeq \pi_1(E)$$

which makes the following diagram commutative.

$$\begin{array}{ccc} \pi_1(U_1) & \xrightarrow{\sim} & \pi_1(U_2) \\ \downarrow & & \downarrow \\ \pi_1(E) & \xrightarrow[\theta]{\sim} & \pi_1(E) \end{array}$$

We put the following assumption.

(A1) θ is contained in the image of the map $\pi_1 : Aut_{\mathbb{F}_p}(E) \to Aut(\pi_1(E))$.

By Lemma 3.2, we can assume

- $\mathcal{O} \in S_1$ and $\mathcal{O} \in S_2$.
- $\phi_s|_{E[s]} = id|_{E[s]}$ for any $s > 0$.

Let m be a positive integer such that

$$S_1 \subset E[m].$$

By Theorem 1.1, we can take a positive even integer r such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p}).$$

Let $P \in S_1$. This implies that there is a point $Q \in [r]^{-1}(P)$ which satisfies the equality

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu$$

for some $a_\mu \in \mathbb{F}_p$ ($\mu \in x(E[r]) \setminus \{\infty\}$). The group $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ acts on E as follows.

$$gP = \begin{cases} P & (g = \overline{0}) \\ -P & (g = \overline{1}) \end{cases}$$

where $g \in \mathbb{Z}/2\mathbb{Z}$ and $P \in E$. We put the following assumptio

(A2) S_1 and S_2 are closed under the action of $\mathbb{Z}/2\mathbb{Z}$.

By using this assumption, we can show the following fact.

- $[s]^{-1}(S_1)$ and $[s]^{-1}(S_2)$ are closed under the action of $\mathbb{Z}/2\mathbb{Z}$ for any $s > 0$.

Definition. Let

$$L_{i,r} = \ker(\pi_1([r]^{-1}(U_i)) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r}) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}).$$

Here, $T_{i,r} = x([r]^{-1}(S_i))$ ($i = 1, 2$). Note that we can define the natural surjection $[r]^{-1}(U_i) \to \mathbb{P}^1 \setminus T_{i,r}$ because $[r]^{-1}(S_i)$ is closed under the action of $\mathbb{Z}/2\mathbb{Z}$.

We consider the following assumption, which depends on r.

(A3(r)) $\alpha_r(L_{1,r}) = L_{2,r}$.

The condition (A3(r)) implies that the condition

(A3(r)′) ϕ_r preserves the action of $\mathbb{Z}/2\mathbb{Z}$.

holds, hence there is a unique bijection $\psi_r : T_{1,r} \to T_{2,r}$ which makes the following diagram commutative.

$$\begin{array}{ccc} [r]^{-1}(S_1) & \xrightarrow[\phi_r]{\sim} & [r]^{-1}(S_2) \\ \downarrow x & & \downarrow x \\ T_{1,r} & \xrightarrow[\psi_r]{\sim} & T_{2,r} \end{array}$$

(See Lemma 3.3.) Note that the equality $\phi_r|_{E[r]} = id|_{E[r]}$ induces the equality $\psi_r|_{x(E[r])} = id|_{x(E[r])}$.

By [3] Theorem 3.3 (cf. Lemma 3.4) and the linear relation

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu,$$

the following equality holds.

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \psi_r(\mu) = x(\phi_r(Q)).$$

This means that

$$x(P) = x(\phi_1(P)).$$

By applying the above argument to all the points of S_1 (note that r does not depend on the choice of P), we have the following theorem, which is a conditional generalization of [3] Theorem 4.9.

Theorem 1.3 (cf. Theorem 3.5)**.** Let $p \geq 3$ be a prime number, U_1 and U_2 nonempty affine open subschemes of an elliptic curve $(E, \mathcal{O})$ over $\overline{\mathbb{F}}_p$ such that

$$\pi_1(U_1) \simeq \pi_1(U_2).$$

We assume that

$$\mathcal{O} \in S_1,$$

$$\mathcal{O} \in S_2$$

and

$$\phi_1(\mathcal{O}) = \mathcal{O}.$$

Let m be a positive integer such that $S_1 \subset E[m]$, r a positive even integer such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}).$$

(Note that such r exists by Theorem 1.1.) We assume (A1), (A2) and (A3(r)). Then

$$U_1 \simeq U_2$$

holds.

1.3 Observation on $L_{i,r}$

Lemma 3.4 (and hence Theorem 1.3) requires condition (A3(r)), but it is not known whether $L_{i,r}$ can be characterized by the étale fundamental group. In the third part, we will observe a relationship among conditions (A2), (A3(r)) and (A3(r)$'$) (cf. Proposition 4.7), and prove that $L_{i,r}$ can be characterized by the étale fundamental group in special cases (cf. Proposition 4.8).

2 Elliptic Curves

In this section, we will show a certain relation between the group structure on elliptic curves and the additive structure on $\mathbb{A}^1$.

We use the same notation as in section 1.1. Let F be the q-power Frobenius endmorphism on E, $Tr(F)$ the trace of F (i.e. $X^2 - Tr(F)X + q$ is the characteristic polynomial of F), α and β the roots of $X^2 - Tr(F)X + q$.

First we will show some properties of the trace of the Frobenius maps.

Lemma 2.1 ([1] Exercise 9.10.10)**.** Let k be a positive integer. Then the following equalities hold.

1. $Tr(F^{2k}) = Tr(F^k)^2 - 2q^k$
2. $Tr(F^{3k}) = Tr(F^{2k})Tr(F^k) - q^k Tr(F^k)$

Proof. Note that $Tr(F^{mk}) = \alpha^{mk} + \beta^{mk}$ and $\alpha^{mk}\beta^{mk} = q^{mk}$ for any m. So we have

$$\begin{aligned} Tr(F^{2k}) &= \alpha^{2k} + \beta^{2k} \\ &= (\alpha^k + \beta^k)^2 - 2\alpha^k\beta^k \\ &= Tr(F^k)^2 - 2q^k \end{aligned}$$

and

$$\begin{aligned} Tr(F^{3k}) &= \alpha^{3k} + \beta^{3k} \\ &= (\alpha^{3k} + \alpha^{2k}\beta^k + \alpha^k\beta^{2k} + \beta^{3k}) - (\alpha^{2k}\beta^k + \alpha^k\beta^{2k}) \\ &= (\alpha^{2k} + \beta^{2k})(\alpha^k + \beta^k) - \alpha^k\beta^k(\alpha^k + \beta^k) \\ &= Tr(F^{2k})Tr(F^k) - q^k Tr(F^k) \end{aligned}$$

□

Proposition 2.2. Let k be a positive integer. Then there exists a positive integer m such that

$$Tr(F^{mk}) > 0.$$

Proof. We consider two cases.
• Suppose $Tr(F^{mk}) \neq 0$ for any m.
At least one of $Tr(F^k), Tr(F^{2k})$ and $Tr(F^{3k})$ is positive because of the second equality in Lemma 2.1.
• Suppose $Tr(F^{m_0 k}) = 0$ for some m_0.
Since the first equality in Lemma 2.1 holds, we have

$$\begin{aligned} Tr(F^{4m_0k}) &= Tr(F^{2m_0k})^2 - 2q^{2m_0k} \\ &= (Tr(F^{m_0k}) - 2q^{m_0k})^2 - 2q^{2m_0k} \\ &= 4q^{2m_0k} - 2q^{2m_0k} = 2q^{2m_0k}. \end{aligned}$$

Thus, $Tr(F^{4m_0k})$ is positive. □

Remark 2.3. We can explicitly calculate the smallest value of m_0 in the second case of the proof of Proposition 2.2.

If E is ordinary, the first case of the proof of Proposition 2.2 only occurs.

If E is supersingular, [6] Theorem 4.1 shows that one of the following conditions holds. (recall that $q = p^n$.)

1. nk is even and $Tr(F^k) = \pm 2q^{\frac{k}{2}}$.
2. nk is even and $Tr(F^k) = \pm q^{\frac{k}{2}}$.
3. nk is odd, $p = 2, 3$ and $Tr(F^k) = \pm p^{\frac{nk+1}{2}}$.
4. $Tr(F^k) = 0$.

In the first case, we have $\alpha^k = \beta^k = \pm q^{\frac{k}{2}}$ and

$$Tr(F^{mk}) = \alpha^{mk} + \beta^{mk} = (\pm 1)^m 2q^{\frac{mk}{2}}$$

for any m. So the first case of the proof of Proposition 2.2 only occurs.

In the second case, by Lemma 2.1, we have $Tr(F^{2k}) = -q^k$, $Tr(F^{3k}) = \mp 2q^{\frac{3k}{2}}$ and $\alpha^{3k} = \beta^{3k} = \mp q^{\frac{3k}{2}}$. Let s and t be the integers such that $m = 3s + t$ and $0 \leq t < 3$. Then we have

$$Tr(F^{mk}) = \begin{cases} (\mp 2q^{\frac{3k}{2}})^s & (t = 0) \\ (\mp 2q^{\frac{3k}{2}})^s (\pm q^{\frac{k}{2}}) & (t = 1) \\ (\mp 2q^{\frac{3k}{2}})^s (-q^k) & (t = 2). \end{cases}$$

So the first case of the proof of Proposition 2.2 only occurs.

In the third case, we have

$$Tr(F^{2k}) = (p-2)q^k$$

and

$$Tr(F^{3k}) = \pm(p-3)p^{\frac{3nk+1}{2}}.$$

So $m_0 = 2$ (resp. $m_0 = 3$) is the smallest positive integer such that $Tr(F^{m_0 k}) = 0$ if $p = 2$ (resp. $p = 3$).

In the final case, we can take m_0 as 1.

We will show two lemmas to prove the main theorem of this section (Theorem 2.6).

Lemma 2.4. Let N and M be positive integers such that $(p, M) = 1$. Then there exists a positive integer k which satisfies the following conditions.

1. $Tr(F^k) > 0$
2. $E[N] \subset E(\mathbb{F}_{q^k})$
3. $q^k \equiv 1 \bmod M$

Proof. Clearly, we can take k which satisfies the conditions 2 and 3, and we can replace k with any multiple. So, by Proposition 2.2, we can take k which satisfies all the conditions. □

Lemma 2.5. Let V be a finite dimensional vector space over $\mathbb{F}_p$, S a subset of V. If $\#V < p(\#S)$, we have

$$V = \langle S \rangle_{\mathbb{F}_p}.$$

Here, $\#V$ (resp. $\#S$) stands for the cardinality of V (resp. S).

Proof. We calculate the dimension of $\langle S \rangle_{\mathbb{F}_p}$.

$$\begin{aligned}
\dim \langle S \rangle_{\mathbb{F}_p} &= \log_p(\#\langle S \rangle_{\mathbb{F}_p}) \\
&\geq \log_p(\#S) \\
&= \log_p(p\#S) - 1 \\
&> \log_p(\#V) - 1 \\
&= \dim V - 1
\end{aligned}$$

This means that $\dim \langle S \rangle_{\mathbb{F}_p} \geq \dim V$. On the other hand, $\langle S \rangle_{\mathbb{F}_p}$ is a subspace of V. So we have

$$V = \langle S \rangle_{\mathbb{F}_p}.$$

□

Theorem 2.6. Let d and m be positive integers. Then there exists a positive integer r which satisfies the following.

$$x(E[m]) \subset H_{dr}(\langle x(E[dr]) \setminus \{\infty\} \rangle_{\mathbb{F}_p})$$

Proof. Let a, b and l be the nonnegative integers such that

$$m = 2^a p^b l,$$

$$(2p, l) = 1$$

if $p \geq 3$, and

$$m = p^b l,$$

$$(p, l) = 1$$

if $p = 2$. By applying Lemma 2.4 to $N = 4dm$ (resp. $N = 2dm$) and $M = 4l$ (resp. $M = l$) if $p \geq 3$ (resp. $p = 2$), we can take k which satisfies the following.

(C1) $Tr(F^k) > 0$

(C2) $E[4dm] \subset E(\mathbb{F}_{q^k})$ if $p \geq 3$

(C3) $q^k \equiv 1 \bmod 4l$ if $p \geq 3$

(C4) $E[2dm] \subset E(\mathbb{F}_{q^k})$ if $p = 2$

(C5) $q^k \equiv 1 \bmod l$ if $p = 2$

First we will calculate the cardinalities of $E[F^k + 1]$ and $x(E[F^k + 1])$. Let $P \in E[F^k - 1]$. Then we have the following.

$$\begin{aligned} P \in E[2] &\iff P = -P \\ &\iff F^k(P) = -P \\ &\iff P \in E[F^k + 1] \end{aligned}$$

In other words, we have $E[F^k - 1] \cap E[F^k + 1] = E[F^k - 1] \cap E[2]$. By the conditions (C2) and (C4), $E[2] \subset E(\mathbb{F}_{q^k}) = E[F^k - 1]$ holds. Thus, we have

$$E[F^k - 1] \cap E[F^k + 1] = E[2].$$

Let $P \in E(\overline{\mathbb{F}}_p)$. Then we have the following.

$$\begin{aligned} P \in x^{-1}(\mathbb{P}^1(\mathbb{F}_{q^k})) &\iff F^k(x(P)) = x(P) \\ &\iff x(F^k(P)) = x(P) \\ &\iff F^k(P) = \pm P \\ &\iff P \in E[F^k - 1] \cup E[F^k + 1] \end{aligned}$$

In other words, we have

$$x^{-1}(\mathbb{P}^1(\mathbb{F}_q^k)) = E[F^k - 1] \cup E[F^k + 1].$$

By using these equalities, we have

$$\begin{aligned} \#E[F^k + 1] &= \#x^{-1}(\mathbb{P}^1(\mathbb{F}_{q^k})) - \#E[F^k - 1] + \#E[2] \\ &= (2q^k + 2 - \#E[2]) - (q^k + 1 - Tr(F^k)) + \#E[2] \\ &= q^k + 1 + Tr(F^k) \end{aligned}$$

and

$$\begin{aligned} \#x(E[F^k + 1]) &= \frac{1}{2}(q^k + 1 + Tr(F^k) - \#E[2]) + \#E[2] \\ &= \frac{1}{2}(q^k + 1 + Tr(F^k) + \#E[2]). \end{aligned}$$

We will apply Lemma 2.5 to the $\mathbb{F}_p$-vector space $\mathbb{A}^1(\mathbb{F}_{q^k})$ and its subset

$$x(E[F^k + 1]) \setminus \{\infty\}.$$

By condition (C1) (i.e. $Tr(F^k) > 0$) and the inequality $\#(E[2]) > 0$, we have

$$\begin{aligned} p(\#(x(E[F^k + 1]) - \{\infty\})) &= \frac{p}{2}(q^k - 1 + Tr(F^k) + \#E[2]) \\ &> \frac{p}{2}q^k \\ &\geq q^k = \#\mathbb{A}^1(\mathbb{F}_{q^k}). \end{aligned}$$

(In particular, $\#(x(E[F^k+1]) \setminus \{\infty\}) > 0$.) Thus, we have

$$\mathbb{A}^1(\mathbb{F}_{q^k}) = \langle x(E[F^k+1]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}.$$

Let $r = \#E[F^k+1] = q^k + 1 + Tr(F^k)$. It is clear that

$$E[F^k+1] \subset E[r] \subset E[dr].$$

Since $H_{dr}(P) = \infty$ for any $P \in x(E[F^k+1]) \setminus \{\infty\}$ $(\neq \phi)$, we have

$$\infty \in H_{dr}(\langle x(E[F^k+1]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}) = H_{dr}(\mathbb{A}^1(\mathbb{F}_{q^k})).$$

Then we have

$$\begin{aligned} H_{dr}(\mathbb{P}^1(\mathbb{F}_{q^k})) &= H_{dr}(\mathbb{A}^1(\mathbb{F}_{q^k})) \\ &= H_{dr}(\langle x(E[F^k+1]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}) \\ &\subset H_{dr}(\langle x(E[dr]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}). \end{aligned}$$

By the definition of H_{dr}, we have

$$\begin{aligned} H_{dr}(\mathbb{P}^1(\mathbb{F}_{q^k})) &= x([dr](x^{-1}(\mathbb{P}^1(\mathbb{F}_{q^k})))) \\ &= x([dr](E[F^k-1] \cup E[F^k+1])) \\ &= x([dr](E[F^k-1])) \\ &= x([dr + d\#(E[F^k-1])](E[F^k-1])) \\ &= x([2d(q^k+1)](E[F^k-1])) \\ &= x([2d(q^k+1)](E(\mathbb{F}_{q^k}))). \end{aligned}$$

Then it suffices to show that

$$E[m] \subset [2d(q^k+1)](E(\mathbb{F}_{q^k})).$$

We consider two cases $p \geq 3$ and $p = 2$ separately.

• Suppose that $p \geq 3$.

Recall that $m = 2^a p^b l$. By condition (C3), we have the following equalities.

- $(\frac{q^k+1}{2}, 2) = 1$
- $(\frac{q^k+1}{2}, l) = 1$ (note that l is odd.)

As $(\frac{q^k+1}{2}, p) = 1$ clearly holds, these equalities implies that

$$(\frac{q^k+1}{2}, m) = 1.$$

By condition (C2), we have

$$\begin{aligned} E[m] &= [\frac{q^k+1}{2}](E[m]) \\ &= [2d(q^k+1)](E[4dm]) \\ &\subset [2d(q^k+1)](E(\mathbb{F}_{q^k})). \end{aligned}$$

• Suppose that $p = 2$.

Recall that $m = p^b l$. By condition (C5), we have the following equality.

• $(q^k + 1, l) = 1$ (note that l is odd.)

As $(q^k + 1, p) = 1$ clearly holds, this equality implies that

$$(q^k + 1, m) = 1.$$

By condition (C4), we have

$$\begin{aligned} E[m] &= [q^k + 1](E[m]) \\ &= [2d(q^k + 1)](E[2dm]) \\ &\subset [2d(q^k + 1)](E(\mathbb{F}_{q^k})). \end{aligned}$$

□

3 Anabelian Geometry

In this section, we assume that $p \geq 3$. Let $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ be elliptic curves over $\overline{\mathbb{F}}_p$ defined by Legendre forms

$$y^2 = x(x-1)(x-\lambda_1)$$

and

$$y^2 = x(x-1)(x-\lambda_2)$$

respectively, where $\lambda_1, \lambda_2 \in \overline{\mathbb{F}}_p$.

Let U_1 and U_2 be nonempty affine open subschemes of E_1 and E_2 respectively, such that

$$\alpha_1 : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2).$$

By [3] Corollary 4.11, we have $E_1 \simeq E_2$. So we can (and do) assume $\lambda_1 = \lambda_2$ and identify E_1 with E_2. Write $(E, \mathcal{O})$ instead of $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$.

By a similar argument to the proof of [3] Lemma 4.2, we can identify $\pi_1([s]^{-1}(U_i))$ with a subgroup of $\pi_1(U_i)$ $(i = 1, 2)$, and α_1 induces an isomorphism

$$\alpha_s : \pi_1([s]^{-1}(U_1)) \xrightarrow{\sim} \pi_1([s]^{-1}(U_2)).$$

for each $s > 0$.

Let $S_1 = E \setminus U_1$ and $S_2 = E \setminus U_2$. By [4] Lemma 2.1 and [4] Theorem 2.5, we can identify $[s]^{-1}(S_1)$ with the set of the equivalence classes of the inertia subgroups, and obtain a bijection

$$\phi_s : [s]^{-1}(S_1) \to [s]^{-1}(S_2)$$

from α_s for each $s > 0$.

First we discuss the condition $\phi_s|_{E[s]} = id_{E[s]}$. Note that the open immersion $U_i \to E$ induces a surjective homomorphism $\pi_1(U_i) \to \pi_1(E)$ $(i = 1, 2)$.

Lemma 3.1 ([4] Corollary 1.10)**.** The isomorphism α_1 induces an isomorphism

$$\theta : \pi_1(E) \xrightarrow{\sim} \pi_1(E).$$

□

Let $Aut_{\mathbb{F}_p}(E)$ be the set of $\mathbb{F}_p$-automorphisms of E. We put the following assumption.

(A1) θ is contained in the image of a map $\pi_1 : Aut_{\mathbb{F}_p}(E) \to Aut(\pi_1(E))$.

Lemma 3.2. There are open immersions $(U_i \to E)_{s>0,i=1,2}$ such that

$$\mathcal{O} \in S_1,$$

$$\mathcal{O} \in S_2$$

and

$$\phi_s|_{E[s]} = id_{E[s]}$$

for any $s > 0$.

Proof. Let $\sigma \in Aut_{\mathbb{F}_p}(E)$ such that $\theta = \pi_1(\sigma)$. Then we have the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi_1(E) & \xrightarrow{\pi_1([s])} & \pi_1(E) & \longrightarrow & E[s] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \sigma|_{E[s]}} & & \\ 0 & \longrightarrow & \pi_1(E) & \xrightarrow{\pi_1([s])} & \pi_1(E) & \longrightarrow & E[s] & \longrightarrow & 0 \end{array}$$

Here the horizontal sequences are exact. We can assume that $\mathcal{O} \in S_1, \mathcal{O} \in S_2$ and $\phi_s(\mathcal{O}) = \mathcal{O}$. We have that $\phi_s|_{E[s]} = \sigma|_{E[s]}$. So by replacing the open immersion $U_1 \to E$ with

$$U_1 \to E \xrightarrow{\sigma^{-1}} E,$$

and replacing S_1, ϕ_s and θ with those which correspond to $U_1 \to E \xrightarrow{\sigma^{-1}} E$,

$$\phi_s|_{E[s]} = id_{E[s]}$$

holds. □

We assume that $\mathcal{O} \in S_1, \mathcal{O} \in S_2$ and $\phi_s|_{E[s]} = id_{E[s]}$ for any $s > 0$ from now on.

Let

$$x : E \to \mathbb{P}^1$$

be the finite morphism of degree 2 defined by $x((a, b)) = a$ and $x(\mathcal{O}) = \infty$.

The group $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ acts on E as follows.

$$gP = \begin{cases} P & (g = \overline{0}) \\ -P & (g = \overline{1}) \end{cases}$$

where $g \in \mathbb{Z}/2\mathbb{Z}$ and $P \in E$.

We put the following assumption from now on.

(A2) S_1 and S_2 are closed under the action of $\mathbb{Z}/2\mathbb{Z}$.

Let m be a positive integer such that

$$S_1 \subset E[m].$$

By Theorem 2.6, we can take a positive even integer r such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p}).$$

The isogeny $[r]$ preserves the action of $\mathbb{Z}/2\mathbb{Z}$. So $[r]^{-1}(S_i)$ is closed under the action. This means that $x : E \to \mathbb{P}^1$ restricts to a finite morphism

$$x : [r]^{-1}(U_i) \to \mathbb{P}^1 \setminus T_{i,r},$$

where

$$T_{i,r} = x([r]^{-1}(S_i))$$

for $i = 1, 2$.

Definition. Let U be an open subscheme of E such that $E \setminus U$ is closed under the action of $\mathbb{Z}/2\mathbb{Z}$. Then we set

$$L_U = \ker(\pi_1(U) \to \pi_1(\mathbb{P}^1 \setminus x(E \setminus U)) \to \pi_1(\mathbb{P}^1 \setminus x(E \setminus U))^{ab,p'}).$$

We write $L_{i,r}$ instead of $L_{[r]^{-1}(U_i)}$ for $i = 1, 2$.

We consider the following conditions, which depend on r.

(A3(r)) $\alpha_r(L_{1,r}) = L_{2,r}$.

(A3(r)′) ϕ_r preserves the action of $\mathbb{Z}/2\mathbb{Z}$.

We use the condition that r is even in the following lemmas.

Lemma 3.3 ([3] Proposition 3.1)**.** The condition (A3(r)) implies the condition (A3(r)′). Under the condition (A3(r)′), we have the bijection

$$\psi_r : T_{1,r} \to T_{2,r}$$

induced by ϕ_r. □

We assume (A3(r)) from now on. The key lemma is the following.

Lemma 3.4 ([3] Theorem 3.3)**.** For any $a_\mu \in \mathbb{F}_p$ ($\mu \in T_{1,r} \setminus \{\infty\}$), we have the following.

$$\sum_\mu a_\mu \mu = 0 \iff \sum_\mu a_\mu \psi_r(\mu) = 0$$

□

Next we will show the existence of linear relations by using Theorem 2.6. Let $P \in S_1$. $x(P) \in H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p})$ holds if and only if we have

$$x([r]^{-1}(P)) \cap \langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p} \neq \phi.$$

This means that there is a linear relation

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu$$

for some $Q \in [r]^{-1}(P)$ and some $a_\mu \in \mathbb{F}_p$ ($\mu \in x(E[r] \setminus \{\infty\}) \subset T_{1,r}$). By Lemma 3.4, we have the following.

$$x(\phi_r(Q)) = \psi_r(x(Q)) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \psi_r(\mu).$$

Recall that $\phi_r|_{E[r]} = id_{E[r]}$, hence $\psi_r|_{x(E[r])} = id_{x(E[r])}$. Thus,

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \psi_r(\mu) = x(\phi_r(Q))$$

holds. This implies that $x(P) = x(\phi_1(P))$. By applying the above argument to all the points of S_1, $U_1 = U_2$ holds. So we obtain the following theorem.

Theorem 3.5. Let $p \geq 3$ be a prime number, U_1 and U_2 nonempty affine open subschemes of elliptic curves $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ respectively over $\overline{\mathbb{F}}_p$ such that

$$\pi_1(U_1) \simeq \pi_1(U_2).$$

(1) [[3] Corollary 4.11]. We have that

$$E_1 \simeq E_2.$$

(2). We assume that

$$(E, \mathcal{O}) \stackrel{\text{def}}{=} (E_1, \mathcal{O}_1) = (E_2, \mathcal{O}_2),$$
$$\mathcal{O} \in S_1 = E \setminus U_1,$$
$$\mathcal{O} \in S_2 = E \setminus U_2$$

and

$$\phi_1(\mathcal{O}) = \mathcal{O}.$$

Let m be a positive integer such that $S_1 \subset E[m]$, r a positive even integer such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p}).$$

(Note that such r exists by Theorem 2.6.) We assume (A1), (A2) and (A3(r)). Then

$$U_1 \simeq U_2$$

holds. □

Remark 3.6. We can prove the tame version of Theorem 3.5 (where $\pi_1(U_1)$ and $\pi_1(U_2)$ are replaced with the tame fundamental groups $\pi_1^t(U_1)$ and $\pi_1^t(U_2)$ respectively) by using the theorems of [5] section 5.

4 Observation on $L_{i,r}$

In this section, we will observe a relationship between (A2), (A3(r)) and (A3(r)$'$), and prove a generalization of [3] Theorem 4.3.

We assume that $p \geq 3$. Let U_1 and U_2 be nonempty affine open subschemes of an elliptic curve E over $\overline{\mathbb{F}}_p$ such that

$$\alpha_1 : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2).$$

Set $S_1 = E \setminus U_1$ and $S_2 = E \setminus U_2$. (In this section, we do not assume $\mathcal{O} \in S_1$ or $\mathcal{O} \in S_2$.) Recall that the isomorphism α_1 induces the isomorphism

$$\alpha_r : \pi_1([r]^{-1}(U_1)) \xrightarrow{\sim} \pi_1([r]^{-1}(U_2)),$$

and that α_r induces the bijection

$$\phi_r : [r]^{-1}(S_1) \to [r]^{-1}(S_2)$$

for each $r > 0$. We consider the following conditions.

(A2) S_1 and S_2 are closed under the action of $\mathbb{Z}/2\mathbb{Z}$

(A3(r)) $\alpha_r(L_{1,r}) = L_{2,r}$

(A3(r)$'$) ϕ_r preserves the action of $\mathbb{Z}/2\mathbb{Z}$

Recall that $L_{i,r}$ is defined as follows under condition (A2).

$$L_{i,r} = \ker(\pi_1([r]^{-1}(U_i)) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r}) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'})$$

Here, $T_{i,r} = x([r]^{-1}(S_i))$ $(i = 1, 2)$.

Definition. Set

$$A^- \stackrel{\text{def}}{=} \{a \in A \mid \overline{1}a = -a\}$$

for any abelian group A equipped with an action of $\mathbb{Z}/2\mathbb{Z}$, and set

$$M_{i,r} \stackrel{\text{def}}{=} \pi_1([r]^{-1}(U_i))^{ab,p'}$$

for any $i = 1, 2$ and any $r > 0$.

Lemma 4.1. Assume condition (A2). Then we have

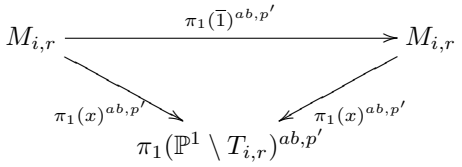
$$(M_{i,r})^- = \ker(M_{i,r} \xrightarrow{\pi_1(x)^{ab,p'}} \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}).$$

for any $i = 1, 2$ and any $r > 0$.

Proof. Note that the action of $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ on $[r]^{-1}(U_i)$ induces an action of $\mathbb{Z}/2\mathbb{Z}$ on $M_{i,r}$. We have

$$(M_{i,r})^- \subset \ker(M_{i,r} \to \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'})$$

because of the following commutative diagram and the fact that $\pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}$ is torsion-free.



So we have the following homomorphism.

$$M_{i,r}/(M_{i,r})^- \to \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}$$

By [3] Lemma 4.4, we have

$$(M_{i,r}^l)_{\mathbb{Z}/2\mathbb{Z}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

for any prime number l that is not p. So $\pi_1(x)$ induces an isomorphism

$$((M_{i,r})_{\mathbb{Z}/2\mathbb{Z}})/T \simeq R$$

where T stands for the torsion subgroup of

$$(M_{i,r})_{\mathbb{Z}/2\mathbb{Z}},$$

and R stands for the image of

$$M_{i,r} \xrightarrow{\pi_1(x)^{ab,p'}} \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}.$$

Here, we have used the fact that R is torsion-free. Set

$$N = \{\overline{1}a - a \mid a \in M_{i,r}\}.$$

By the definition of $(-)_{\mathbb{Z}/2\mathbb{Z}}$, $(M_{i,r})_{\mathbb{Z}/2\mathbb{Z}} = M_{i,r}/N$ holds. By easy computation, we have

$$2(M_{i,r})^- \subset N \subset (M_{i,r})^-.$$

Note that $M_{i,r}/(M_{i,r})^-$ is torsion-free. Thus, we have

$$\begin{aligned} M_{i,r}/(M_{i,r})^- &\simeq ((M_{i,r})_{\mathbb{Z}/2\mathbb{Z}})/T \\ &\simeq R. \end{aligned}$$

□

So $(M_{i,r})^-$ is the image of $L_{i,r}$ under

$$\pi_1([r]^{-1}(U_i)) \to M_{i,r}.$$

for any $i = 1, 2$ and any $r > 0$.

Definition. Let

$$W_{i,r}\ (\subset M_{i,r})$$

be the sum of the images of the inertia subgroups under

$$\pi_1([r]^{-1}(U_i)) \to M_{i,r}$$

($i = 1, 2$ and $r > 0$). Let

$$\sigma_{M,G} : M \to M$$

be the homomorphism which is defined by

$$m \mapsto \Sigma_{g \in G} gm\ (m \in M)$$

for any group G and any G-module M. Note that if $G = \mathbb{Z}/2\mathbb{Z}$, we have

$$M^- = \ker(\sigma_{M,\mathbb{Z}/2\mathbb{Z}}).$$

Lemma 4.2. The kernel and the cokernel of the natural homomorphism

$$(M_{i,r})^{E[r]} \to M_{i,1},$$

which is the composite of the natural homomorphisms

$$(M_{i,r})^{E[r]} \hookrightarrow M_{i,r},$$

$$M_{i,r} \twoheadrightarrow (M_{i,r})_{E[r]}$$

and

$$(M_{i,r})_{E[r]} \to M_{i,1},$$

are finite for any $i = 1, 2$ and any $r > 0$.

Proof. By applying [2] Corollary 7.2.5 (Hochschild-Serre spectral sequence) to the exact sequence

$$1 \to \pi_1([r]^{-1}(U_i)) \to \pi_1(U_i) \to E[r] \to 1,$$

we have the following exact sequence.

$$\begin{aligned} 0 \to\ & H^1(E[r], \mathbb{Q}/\mathbb{Z}) \to H^1(\pi_1(U_i), \mathbb{Q}/\mathbb{Z}) \\ & \to H^1(\pi_1([r]^{-1}(U_i)), \mathbb{Q}/\mathbb{Z})^{E[r]} \to H^2(E[r], \mathbb{Q}/\mathbb{Z}) \end{aligned}$$

By applying [2] Theorem 2.9.6 (Pontryagin duality) to this, we have the following exact sequence.

$$0 \leftarrow E[r] \leftarrow \pi_1(U_i)^{ab} \leftarrow (\pi_1([r]^{-1}(U_i))^{ab})_{E[r]} \leftarrow \mathrm{Hom}_{\mathbb{Z}}(H^2(E[r], \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z})$$

This implies that the kernel and the cokernel of the homomorphism

$$(M_{i,r})_{E[r]} \to M_{i,1}$$

are finite. So it suffices to show that the kernel and the cokernel of the homomorphism

$$(M_{i,r})^{E[r]} \to (M_{i,r})_{E[r]}$$

are finite. Let

$$\sigma : (M_{i,r})_{E[r]} \to (M_{i,r})^{E[r]}$$

be the homomorphism which is induced by $\sigma_{M_{i,r},E[r]}$. First we consider the composite of the following homomorphisms.

$$(M_{i,r})_{E[r]} \xrightarrow{\sigma} (M_{i,r})^{E[r]} \to (M_{i,r})_{E[r]}$$

This is equal to the multiplication by $\#(E[r])$. So its cokernel is finite, and so is the cokernel of the homomorphism

$$(M_{i,r})^{E[r]} \to (M_{i,r})_{E[r]}.$$

Next we consider the composite of the following homomorphisms.

$$(M_{i,r})^{E[r]} \to (M_{i,r})_{E[r]} \xrightarrow{\sigma} (M_{i,r})^{E[r]}$$

This is also equal to the multiplication by $\#(E[r])$. Note that

$$(M_{i,r})^{E[r]}$$

is torsion-free. So this composite homomorphism is injective. Thus, the homomorphism

$$(M_{i,r})^{E[r]} \to (M_{i,r})_{E[r]}$$

is also injective. □

Lemma 4.3. Let M and N be $\mathbb{Z}/2\mathbb{Z}$-modules,

$$f : M \to N$$

a homomorphism of $\mathbb{Z}/2\mathbb{Z}$-modules. We let

$$f^- : M^- \to N^-$$

denote the homomorphism induced by f. Then the following hold.

1. The kernel of f is finite $\Rightarrow$ the kernel of f^- is finite.
2. The kernel and the cokernel of f are finite $\Rightarrow$ the cokernel of f^- is finite.

Proof. We consider the following commutative diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & M^- & \longrightarrow & M & \xrightarrow{\sigma_{M,\mathbb{Z}/2\mathbb{Z}}} & M \\ & & \downarrow{\scriptstyle f^-} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ 0 & \longrightarrow & N^- & \longrightarrow & N & \xrightarrow{\sigma_{N,\mathbb{Z}/2\mathbb{Z}}} & N \end{array}$$

Here, the horizontal sequences are exact. Then we obtain an injection

$$\ker(f^-) \to \ker(f),$$

an exact sequence

$$\ker(\mathrm{im}(\sigma_{M,\mathbb{Z}/2\mathbb{Z}}) \to \mathrm{im}(\sigma_{N,\mathbb{Z}/2\mathbb{Z}})) \to \mathrm{coker}(f^-) \to \mathrm{coker}(f)$$

and an injection

$$\ker(\mathrm{im}(\sigma_{M,\mathbb{Z}/2\mathbb{Z}}) \to \mathrm{im}(\sigma_{N,\mathbb{Z}/2\mathbb{Z}})) \to \ker(f).$$

Now the assertions clearly hold.

□

Lemma 4.4. Assume condition (A2). The kernel and the cokernel of the natural homomorphism

$$((M_{i,r})^{E[r]})^- \to (M_{i,1})^-$$

are finite for any $i = 1, 2$ and any $r > 0$.

Proof. This follows from Lemma 4.2 and Lemma 4.3. □

Lemma 4.5. We have

$$\#(M_{i,r}/((M_{i,r})^{E[r]} + W_{i,r})) < \infty$$

for any $i = 1, 2$ and any $r > 0$.

Proof. We have the following commutative diagram.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & W_{i,r} & \longrightarrow & M_{i,r} & \xrightarrow{f_r} & \pi_1(E)^{p'} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \pi_1([r])^{ab,p'}} & & \downarrow{\scriptstyle \pi_1([r])^{ab,p'}} & & \\
0 & \longrightarrow & W_{i,1} & \longrightarrow & M_{i,1} & \xrightarrow[f_1]{} & \pi_1(E)^{p'} & \longrightarrow & 0 \\
 & & & & & & \downarrow & & \\
 & & & & & & E[r]^{p'} & & \\
 & & & & & & \downarrow & & \\
 & & & & & & 0 & &
\end{array}$$

Here, f_r and f_1 stand for the natural homomorphisms arising from the open immersions $[r]^{-1}(U_i) \hookrightarrow E$ and $U_i \hookrightarrow E$, respectively, and the horizontal and vertical sequences are exact. So it suffices to show that

$$\#(\pi_1(E)^{p'}/(f_1 \circ \pi_1([r])^{ab,p'})((M_{i,r})^{E[r]})) < \infty.$$

By Lemma 4.2, we have

$$\#(M_{i,1}/(\pi_1([r])^{ab,p'}((M_{i,r})^{E[r]})) < \infty.$$

This implies that

$$\#(\pi_1(E)^{p'}/(f_1 \circ \pi_1([r])^{ab,p'})((M_{i,r})^{E[r]})) < \infty.$$

□

Lemma 4.6. Assume condition (A2). Then we have

$$\#((M_{i,r})^-/(((M_{i,r})^{E[r]})^- + (W_{i,r})^-)) < \infty$$

for any $i = 1, 2$ and any $r > 0$.

Proof. Let $N_{i,r}$ denote

$$(M_{i,r})^{E[r]} + W_{i,r}.$$

The second statement of Lemma 4.3 and Lemma 4.5 imply that $M_{i,r}^-/N_{i,r}^-$ is finite. Next we consider the following exact sequence.

$$\begin{aligned} 0 \to N_{i,r}^-/(((M_{i,r})^{E[r]})^- + (W_{i,r})^-) \\ \to M_{i,r}^-/(((M_{i,r})^{E[r]})^- + (W_{i,r})^-) \to M_{i,r}^-/N_{i,r}^- \to 0 \end{aligned}$$

Since

$$2N_{i,r}^- \subset ((M_{i,r})^{E[r]})^- + (W_{i,r})^- \subset N_{i,r}^-,$$

the group

$$N_{i,r}^-/(((M_{i,r})^{E[r]})^- + (W_{i,r})^-)$$

is finite. So

$$M_{i,r}^-/(((M_{i,r})^{E[r]})^- + (W_{i,r})^-)$$

is also finite. □

Definition. Let M be a $\hat{\mathbb{Z}}^{p'}$-module and N a submodule of M. Then we define

$$T_M(N)$$

to be the smallest subgroup of M such that $M/T_M(N)$ is torsion-free and that $N \subset T_M(N)$.

Proposition 4.7. Assume condition (A2). Then condition (A3(r)) holds if and only if conditions (A3(r)′) and (A3(1)) hold.

Proof. We have already seen that (A3(r)) implies (A3(r)′). ([3] Proposition 3.1 (hence Lemma 3.3) requires that

$$x : U_i \to \mathbb{P}^1 \setminus T_{i,1}$$

is unramified, but this condition is not necessary.) So it suffices to show the equivalence between (A3(r)) and (A3(1)) by using (A2) and (A3(r)′).

- (A3(r)) $\Rightarrow$ (A3(1))

First we assume (A3(r)). By Lemma 4.4, the cokernel of the homomorphism

$$\pi_1([r])^{ab,p'} : M_{i,r}^- \to M_{i,1}^-$$

is finite. Note that

$$M_{i,1}/M_{i,1}^-$$

is torsion-free. So

$$M_{i,1}^- = T_{M_{i,1}}(\pi_1([r])^{ab,p'}(M_{i,r}^-)).$$

holds. By Lemma 4.1, Condition (A3(r)) means that

$$\alpha_r^{ab,p'}(M_{1,r}^-) = M_{2,r}^-.$$

So we have

$$\begin{aligned}\alpha_1^{ab,p'}(M_{1,1}^-) &= \alpha_1^{ab,p'}(T_{M_{1,1}}(\pi_1([r])^{ab,p'}(M_{1,r}^-))) \\ &= T_{M_{2,1}}((\pi_1([r])^{ab,p'} \circ \alpha_r^{ab,p'})(M_{1,r}^-)) \\ &= T_{M_{2,1}}(\pi_1([r])^{ab,p'}(M_{2,r}^-)) \\ &= M_{2,1}^-.\end{aligned}$$

By Lemma 4.1, this means that condition (A3(1)) holds.

- (A3(1)) $\Rightarrow$ (A3(r))

Next we assume (A3(1)). Set

$$I_{i,r} = (\pi_1([r])^{ab,p'})^{-1}(M_{i,1}^-) \cap M_{i,r}^{E[r]} \ (\supset (M_{i,r}^{E[r]})^-).$$

First we will prove that

$$I_{i,r}/(M_{i,r}^{E[r]})^-$$

is finite. We consider the following commutative diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \ker(M_{i,r}^{E[r]} \to M_{i,1}) & \longrightarrow & M_{i,r}^{E[r]} & \longrightarrow & M_{i,1} \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & \ker(I_{i,r} \to M_{i,1}^-) & \longrightarrow & I_{i,r} & \longrightarrow & M_{i,1}^- \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
\end{array}$$

Here, the horizontal and vertical sequences are exact. By Lemma 4.2, the kernel of the homomorphism

$$M_{i,r}^{E[r]} \to M_{i,1}$$

is finite, and so is the kernel of the homomorphism

$$I_{i,r} \to M_{i,1}^{-}.$$

Then we consider the following commutative diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (M_{i,r}^{E[r]})^{-} & \longrightarrow & I_{i,r} & \longrightarrow & I_{i,r}/(M_{i,r}^{E[r]})^{-} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \pi_1([r])^{ab,p'}((M_{i,r}^{E[r]})^{-}) & \longrightarrow & M_{i,1}^{-} & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

Here, C stands for the cokernel of the homomorphism

$$(M_{i,r}^{E[r]})^{-} \to M_{i,1}^{-},$$

and the horizontal and vertical sequences are exact. By Lemma 4.4, C is finite. We have already seen that the kernel of the homomorphism

$$I_{i,r} \to M_{i,1}^{-}$$

is finite. So the kernel of the homomorphism

$$I_{i,r}/(M_{i,r}^{E[r]})^{-} \to C$$

is also finite, and so is

$$I_{i,r}/(M_{i,r}^{E[r]})^{-}.$$

Now, by Lemma 4.6,

$$M_{i,r}^{-} = T_{M_{i,r}}((M_{i,r}^{E[r]})^{-} + W_{i,r}^{-})$$

holds. By using the finiteness of

$$I_{i,r}/(M_{i,r}^{E[r]})^{-},$$

we have

$$M_{i,r}^{-} = T_{M_{i,r}}(I_{i,r} + W_{i,r}^{-}).$$

Note that condition (A3(1)) means that

$$\alpha_1^{ab,p'}(M_{1,1}^{-}) = M_{2,1}^{-}$$

by Lemma 4.1, and that $I_{i,r}$ is the inverse image of $M_{i,1}^{-}$ under

$$M_{i,r}^{E[r]} \to M_{i,1}.$$

So the equality

$$\alpha_r^{ab,p'}(I_{1,r}) = I_{2,r}$$

holds. Condition (A3$(r)'$) implies that

$$\alpha_r^{ab,p'}(W_{1,r}^-) = W_{2,r}^-$$

So we have

$$\begin{aligned}
\alpha_r^{ab,p'}(M_{1,r}^-) &= \alpha_r^{ab,p'}(T_{M_{1,r}}((M_{1,r}^{E[r]})^- + W_{1,r}^-)) \\
&= \alpha_r^{ab,p'}(T_{M_{1,r}}(I_{1,r} + W_{1,r}^-)) \\
&= T_{M_{2,r}}(\alpha_r^{ab,p'}(I_{1,r}) + \alpha_r^{ab,p'}(W_{1,r}^-)) \\
&= T_{M_{2,r}}(I_{2,r} + W_{2,r}^-) \\
&= T_{M_{2,r}}((M_{2,r}^{E[r]})^- + W_{2,r}^-) \\
&= M_{2,r}^-
\end{aligned}$$

By Lemma 4.1, this means that condition (A3(r)) holds. □

Finally, we consider the case of $\#S_1 \in \{1, 2\}$. First we assume $\#S_1 = 2$. We can assume that S_1 is closed under the action of $\mathbb{Z}/2\mathbb{Z}$ by replacing the open immersion $U_1 \to E$ with a suitable one as follows. Let $S_1 = \{P_1, P_1'\}$ such that $P_1 \neq P_1'$ and take $R \in E$ such that $2R = -P_1 - P_1'$. Then we have

$$-(P_1 + R) = -P_1 + R - 2R = -P_1 + R + P_1 + P_1' = P_1' + R.$$

So by replacing $U_1 \to E$ with $U_1 \to E \xrightarrow{+R} E$, we have $S_1 = \{P_1 + R, -(P_1 + R)\}$. By applying the same argument to U_2, we can and do assume (A2), and let $S_1 = \{P_1, -P_1\}$. Given any $r > 0$, we can assume both (A2) and (A3$(r)'$) by replacing $U_1 \to E$ and $[r]^{-1}(U_1) \to E$ with suitable ones. Indeed, let $Q \in [r]^{-1}(S_1)$, $R \in E[r]$ such that $\phi_r^{-1}(-\phi_r(Q)) = -Q + R$, and let $W \in E[2r]$ such that $2W = R$. Then we have the following.

$$\begin{array}{ccccc}
\phi_r(Q) & \xleftarrow{\phi_r} & Q & \xleftarrow{+W} & Q - W \\
-\phi_r(Q) & \xleftarrow{\phi_r} & -Q + R & \xleftarrow{+W} & -Q + W
\end{array}$$

We replace the open immersions $U_1 \to E$ and $[r]^{-1}(U_1) \to E$ with $U_1 \to E \xrightarrow{+rW} E$ and $[r]^{-1}(U_1) \to E \xrightarrow{+W} E$ respectively (then ϕ_r is replaced with $\phi_r \circ (+W)$), and we replace Q with $Q - W$. Note that $\{P_1 - rW, -P_1 - rW\}$ is closed under the action of $\mathbb{Z}/2\mathbb{Z}$ because $rW \in E[2]$.

$$\begin{array}{ccccc}
\pi_1([r]^{-1}(U_2)) & \xleftarrow[\alpha_r]{\sim} & \pi_1([r]^{-1}(E\backslash\{P_1,-P_1\})) & \xleftarrow[\pi_1(+W)]{\sim} & \pi_1([r]^{-1}(E\backslash\{P_1-rW,-P_1-rW\})) \\
\downarrow{\scriptstyle \pi_1([r])} & & \downarrow{\scriptstyle \pi_1([r])} & & \downarrow{\scriptstyle \pi_1([r])} \\
\pi_1(U_2) & \xleftarrow[\alpha_1]{\sim} & \pi_1(E\backslash\{P_1,-P_1\}) & \xleftarrow[\pi_1(+rW)]{\sim} & \pi_1(E\backslash\{P_1-rW,-P_1-rW\})
\end{array}$$

Then we have $-\phi_r(Q) = \phi_r(-Q)$. Let

$$\sigma_r : E[r] \simeq E[r]$$

be the isomorphism defined by the following commutative diagram. (Recall that θ is defined in Lemma 3.1.)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi_1(E) & \xrightarrow{\pi_1([r])} & \pi_1(E) & \longrightarrow & E[r] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \sigma_r} & & \\ 0 & \longrightarrow & \pi_1(E) & \xrightarrow{\pi_1([r])} & \pi_1(E) & \longrightarrow & E[r] & \longrightarrow & 0 \end{array}$$

Here the horizontal sequences are exact. Then we have the equality

$$\phi_r(P + R) = \phi_r(P) + \sigma_r(R)$$

for any $P \in [r]^{-1}(S_1)$ and any $R \in E[r]$. Any point of $[r]^{-1}(S_1)$ can be written as $Q + R$ or $-Q + R$ for some $R \in E[r]$. Then we have

$$\begin{aligned} \phi_r(-(Q + R)) &= \phi_r(-Q) - \sigma_r(R) \\ &= -\phi_r(Q) - \sigma_r(R) \\ &= -\phi_r(Q + R). \end{aligned}$$

We also have the equality $\phi_r(Q - R) = -\phi_r(-Q + R)$. So ϕ_r preserves the action of $\mathbb{Z}/2\mathbb{Z}$.

Next, we assume $\#S_1 = 1$. We can assume (A2) by replacing the open immersion $U_i \to E$ with $U_i \to E \xrightarrow{-R_i} E$ for $i = 1, 2$ (here $S_i = \{P_i\}$ and $R_i \in P_i + E[2]$). By using a similar argument as above, we can assume (A3$(r)'$) in this situation.

Now we prove the following proposition, which is a generalization of [3] Theorem 4.3.

Proposition 4.8. Let r be a positive integer. Assume that $\#S_1 \in \{1, 2\}$. In this case, we can assume conditions (A2) and (A3$(r)'$) for suitable open immersions

$$[r]^{-1}(U_i) \hookrightarrow E$$

$(i = 1, 2)$. Then condition (A3(r)) holds.

Proof. By [4] Theorem 1.9, we have $\#S_2 = \#S_1$. Set

$$S_i = \{P_i, -P_i\} \quad (i = 1, 2)$$

(we admit $P_i = -P_i$), and assume $\phi_1(P_1) = P_2$. We have observed that condition (A3$(r)'$) holds for suitable open immersions. By Proposition 4.7, it suffices to show that condition (A3(1)) holds. By [3] Lemma 4.4,

$$\begin{aligned} (\pi_1(E \setminus \{P_i, -P_i\})^{ab,l})^{\mathbb{Z}/2\mathbb{Z}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l &\simeq (\pi_1(E \setminus \{P_i, -P_i\})^{ab,l})_{\mathbb{Z}/2\mathbb{Z}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \\ &\simeq \pi_1(\mathbb{P}^1 \setminus \{x(P_i)\})^{ab,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \\ &= 0 \end{aligned}$$

holds for any prime number $l \neq p$. Note that

$$(\pi_1(E \setminus \{P_i, -P_i\})^{ab,p'})^{\mathbb{Z}/2\mathbb{Z}}$$

is torsion-free. So we have

$$(\pi_1(E \setminus \{P_i, -P_i\})^{ab,p'})^{\mathbb{Z}/2\mathbb{Z}} = 0.$$

This implies that

$$(\pi_1(E \setminus \{P_i, -P_i\})^{ab,p'})^{-} = \pi_1(E \setminus \{P_i, -P_i\})^{ab,p'}.$$

By Lemma 4.1, we have

$$L_{i,1} = \pi_1(E \setminus \{P_i, -P_i\}).$$

So condition (A3(1)) clearly holds. □

Acknowledgments

I am grateful to Professor Akio Tamagawa for helpful discussions.

References

[1] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge Univ. Press, 2012.

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

[3] A. Sarashina. Reconstruction of one-punctured elliptic curves in positive characteristic by their geometric fundamental groups. *manuscripta mathematica*, Vol. 163, No. 1, pp. 201–225, 2020.

[4] A. Tamagawa. On the fundamental groups of curves over algebraically closed fields of characteristic > 0. *Internat. Math. Res. Notices*, Vol. 1999, No. 16, pp. 853–857, 1999.

[5] A. Tamagawa. On the tame fundamental groups of curves over algebraically closed fields of characteristic > 0. In *Galois groups and fundamental groups*, Vol. 41 of *Math. Sci. Res. Inst. Publ.*, pp. 47–105. Cambridge Univ. Press, Cambridge, 2003.

[6] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, Vol. 2, pp. 521–560, 1969.