The 12-th roots of the discriminant of an elliptic curve and the torsion points

Kohei Fukuda, Sho Yoshikawa

Abstract
Given an elliptic curve over a field of characteristic different from 2,3, its discriminant defines a $\mu_{12}$-torsor over the field. In this paper, we give an explicit description of this $\mu_{12}$-torsor in terms of the 3-torsion points and of the 4-torsion points on the given elliptic curve. As an application, we generalize a result of Coates on the 12-th root of the discriminant of an elliptic curve.

1 Introduction
Let $E$ be an elliptic curve over a field $K$. Then, the discriminant $\Delta_E$ of $E$ is defined to be a value in $K^\times/(K^\times)^{12}$, which depends only on the isomorphism class of $E$.

To study $\Delta_E$, it suffices to consider $\Delta_E \mod (K^\times)^n$ for $n = 3, 4$ separately, because $K^\times/(K^\times)^{12} \cong K^\times/(K^\times)^3 \times K^\times/(K^\times)^4$. In the rest of this introduction, we suppose that $n = 3, 4$ and that $K$ be a field of characteristic prime to $n$. Then, we may focus on the $\mu_n$-torsor $\mu_n \sqrt[12]{\Delta_E}$ over $K$ consisting of $n$-th roots of $\Delta_E$ since $\Delta_E \mod (K^\times)^n$ corresponds to the $\mu_n$-torsor $\mu_n \sqrt[12]{\Delta_E}$ via the isomorphism $K^\times/(K^\times)^n \cong H^1(K, \mu_n)$ from Kummer theory.

The goal of this paper is to give an explicit description of the $\mu_n$-torsor $\mu_n \sqrt[12]{\Delta_E}$ out of $E$. More precisely, we construct a $\wedge^2 E[n]$-torsor $T_n(E[n])$ over $K$ and define a canonical isomorphism $w_n$ from $T_n(E[n])$ to the $\mu_n$-torsor $\mu_n \sqrt[12]{\Delta_E}$ over $K$ such that the following diagram is commutative:

$$
\begin{array}{ccc}
\wedge^2 E[n] \times T_n(E[n]) & \xrightarrow{\text{action}} & T_n(E[n]) \\
\downarrow e_n \times w_n & & \downarrow \quad w_n \\
\mu_n \times \mu_n \sqrt[12]{\Delta_E} & \xrightarrow{\text{action}} & \mu_n \sqrt[12]{\Delta_E},
\end{array}
$$

where $e_n$ is the Weil pairing normalized as in Remark 2.8 and Remark 2.10.

We now describe the organization of this paper.
In Section 2, we give a brief review of several results on elliptic curves. The results on Tate curves and modular curves will be crucial in the proof of our main theorem.

Sections 3 and 4 give a preparation for stating our main theorem. Our first task is to construct a $\wedge^2 E[n]$-torsor $T_n(E[n])$, which are explained in Section 3 as we mentioned above. Since this construction only uses the fact $E[n] \cong (\mathbb{Z}/(n))^2$, Section 3 deals with an abstract free $\mathbb{Z}/(n)$-module of rank 2. The second task is to construct a bijection $w_n : T_n(E[n]) \to \mu_n \sqrt[12]{\Delta_E}$, which is done
in Section 4. Also, we give a simple description of the action of $\Lambda^2 E[n]$ on $T_n(E[n])$ when $E$ is a Tate curve. The constructions of $w_n$ are based on [4] and [7].

Next, integrating the results of the previous two sections, we proceed to the main part of this paper; in Section 5, we give the precise statement of the main theorem and prove it. In its proof, using the modular curves of level 3 and 4, we reduce a claim on general elliptic curves to a claim on a single Tate curve. As such an elliptic curve, we choose the Tate curve over a Laurent series field $\mathbb{Q}(\!(q)\!)$. This choice enables us to compute concretely both the map $w_n : T_n(E[n]) \to \mu_n \sqrt{\Delta_E}$ and the Weil pairing for the Tate curve.

In the last section, we give a consequence of our main theorem extending the result of Coates [2] in the following sense:

**Corollary 6.1.** Let $E$ and $E'$ be elliptic curves over $K$ of characteristic $\text{char}(K) \neq 2, 3$, and $\varphi : E \to E'$ be an isogeny over $K$. If $d = \text{deg} \varphi$ is prime to 12, then we have $\Delta_E = (\Delta_{E'})^d$ in $K^\times/(K^\times)^{12}$.

**Acknowledgment**

The authors wish to express their hearty gratitude to their advisor, Professor Takeshi Saito. He not only gave them a lot of suggestive advice, but also patiently encouraged them when they were in trouble with their study. Also, the authors sincerely appreciate Professor J.-P. Serre, because originally he suggested the theme of this paper to Professor Saito. This work was supported by the Program for Leading Graduate Schools, MEXT, Japan.

**Convention and Terminology**

Let $\varphi : G \to H$ be a homomorphism of groups and $f : X \to Y$ be a map, where $X$ (resp. $Y$) is a $G$-set (resp. $H$-set). We say that $f$ is compatible with $\varphi$ if for any $x \in X$ and $g \in G$ we have $f(g \cdot x) = \varphi(g) \cdot f(x)$.

Also, we often denote by $\omega$ (resp. $i$) a primitive cubic (resp. 4th) root of unity.

**2 Review on elliptic curves**

In this section, we review some results on elliptic curves we need in this paper. We omit all the proofs of these results, and only give references.

**2.1 Elliptic curves**

**Definition 2.1.** Let $S$ be a scheme. An elliptic curve over $S$ is a pair $(E, O)$ such that $E$ is a proper smooth scheme over $S$ whose geometric fibers are connected algebraic curves of genus 1, and that $O$ is a section of $E \to S$.

If there is no risk of confusion, we omit to write $O$ and simply call $E$ an elliptic curve. It is well-known as the Abel-Jacobi theorem (THEOREM 2.1.2, [3]) that every elliptic curve $(E, O)$ admits a structure of a commutative group scheme with $O$ the unit section. For each positive integer $N$, we denote by $E[N]$ the $N$-torsion subgroup scheme of $E$.
Remark 2.2. If $N$ is invertible on $S$, then $E[N]$ is a finite étale commutative group scheme. If, in addition, $S$ is a spectrum of a field $K$, then we often identify the finite étale commutative group scheme $E[N]$ over $K$ with the associated $G_K = \text{Gal}(\overline{K}/K)$-module $E[N](\overline{K})$.

Definition 2.3. For a Weierstrass equation over a ring $A$ of the form
\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,
\]
we define $b_i \in A \ (i = 2, 4, 6, 8)$ by
\[
\begin{align*}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= a_3^2 + 4a_6, \\
b_6 &= 2a_4 + a_1a_3, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 + a_4^2,
\end{align*}
\]
and define the discriminant $\Delta$ of the Weierstrass equation by
\[
\Delta := 9b_2b_4b_6 - b_2^2b_8 - 8b_3^4 - 27b_6^2.
\]

The following theorem actually characterizes the definition of elliptic curves.

Theorem 2.4. Let $E/S$ be an elliptic curve. Then there exists an affine covering \{${U_i}$\} of $S$ such that, for each $i \in I$, $E_{U_i}/U_i$ is given by a Weierstrass equation over $\Gamma(U_i, \mathcal{O})$ with the discriminant invertible on $\Gamma(U_i, \mathcal{O})$.

Proof. See (2.2), [3] \hfill \blacksquare

Remark 2.5. (1) It is well-known (for example, see [8]) that, for a Weierstrass equation, the only change of variables fixing $[0 : 1 : 0]$ and preserving the general Weierstrass form is
\[
\begin{align*}
x &= u^2X + r, \\
y &= u^3Y + sX + t,
\end{align*}
\]
with $u \in A^\times$ and $r, s, t \in A$. Let $b_i$ and $\Delta$ ( $b_i'$ and $\Delta'$, respectively) be the constants defined in Definition 2.1 for the Weierstrass equation with coordinates $(x, y)$ ($(X, Y)$, respectively). Then the above change of variable gives the following formula:
\[
\begin{align*}
u^2b_2' &= b_2 + 12r, \\
u^4b_4' &= b_4 + rb_2 + 6r^2, \\
u^{12}\Delta' &= \Delta. \\
\end{align*}
\]

(2) Suppose that 2 is invertible on a ring $A$. Then, any Weierstrass equation can be made into the form
\[
y^2 = x^3 + a_2x^2 + a_4x + a_6
\]
over $A$, and
\[
x = u^2X + r, \quad y = u^3Y \quad (u \in A^\times, r \in A)
\]
is the only change of variables fixing the point $[0 : 1 : 0]$ and preserving such a Weierstrass form.
Let $E$ be an elliptic curve over a field $K$. Take a Weierstrass equation for $E$ and consider its discriminant $\Delta$. The Remark 2.5 (1) implies that the image of $\Delta$ in $K^\times/(K^\times)^{12}$ only depends on $E$. We denote it by $\Delta_E \in K^\times/(K^\times)^{12}$, and call it the discriminant of $E$.

### 2.2 The modular curve of level $r \geq 3$

In the following, we recall the representability of a moduli problem on elliptic curves. This result will be used in the proof of our main theorem to reduce Proposition 5.1 to the Tate curve case (Lemma 4.12).

**Theorem 2.6.** For a positive integer $r$, let $M(r) : \text{Sch}/\mathbb{Z}[1/r] \to \text{Sets}$ be a functor defined as follows; for a scheme $S$ over $\mathbb{Z}[1/r]$, $M(r)(S)$ is the set of isomorphism classes of the pair $(E, \alpha)$, where $E$ is an elliptic curve over $S$ and $\alpha : (\mathbb{Z}/(r))^2 \xrightarrow{\sim} E[r]$ is an isomorphism of group schemes over $S$.

1. If $r = 1$, then the morphism $j : M \to \mathcal{A}\mathbb{Z}_1$ taking the $j$-invariant makes $\mathcal{A}\mathbb{Z}_1$ into the coarse moduli of $M := M(1)$.
2. If $r \geq 3$, then $M(r)$ has the fine moduli $Y(r)$, which is a connected smooth curve over $\mathbb{Z}[1/r]$.

**Proof.** See Corollary 8.40, [5] for (1) and Lemma 8.37, [5] for (2). \hfill \square

In this paper, we call $Y(r)$ the modular curve of level $r$.

### 2.3 Weil pairing

Next, we recall the Weil pairing of an elliptic curve. We make explicit the sign convention of the pairing, which is an important point in our result.

**Theorem 2.7.** Let $N$ be a positive integer. For any elliptic curve $E/S$, there exists a canonical bilinear pairing 

$$ e_N : E[N] \times E[N] \to \mu_N, $$

which is alternating and induces a self-duality of $E[N]$. The construction of this pairing is functorial in the sense that it defines a morphism of functors 

$$ M(N) \to \mu_N. $$

$$ [(E/S, (P, Q))] \mapsto e_N(P, Q) $$

**Proof.** See (2.8), [3]. \hfill \square

**Remark 2.8.** There are two choices of the sign of $e_N$. We choose $e_N$ so that it satisfies the following equality: for any elliptic curve $E \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ ($\tau \in \mathcal{H}$) over $\mathbb{C}$, we have 

$$ e_N \left( \frac{1}{N}, \frac{\tau}{N} \right) = \exp \left( \frac{2\pi i}{N} \right). $$

We call the pairing of such a choice the normalized Weil pairing.
2.4 The Tate curve

Finally, we recall some properties of the Tate curves. The main references on this topic are [6] and [8].

Let \((K, v)\) be a complete discrete valuation field. We fix an element \(q \in K^\times\) satisfying \(v(q) > 0\). Consider the elliptic curve (called the Tate curve) over \(K\) defined by the following Weierstrass equation:

\[
E_q : y^2 + xy = x^3 + \left(-5 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n}\right) x + \left(-\frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3)q^n}{1 - q^n}\right).
\]

The discriminant \(\Delta\) of this Weierstrass equation is given by

\[
\Delta = q \prod_{m \geq 1} (1 - q^m)^{24}. \tag{2.3}
\]

The curve \(E_q\) has the following important properties:

**Theorem 2.9.** Let the notation be as above. Let \(u\) be an indeterminate, and \(x = x(u, q)\) and \(y = y(u, q)\) be the two power series in \(\mathbb{Z}[u, u^{-1}][][q]\) defined by

\[
x(u, q) := \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n \geq 1} \frac{nq^n}{1 - q^n} \tag{2.4}
\]

\[
y(u, q) := \sum_{n \in \mathbb{Z}} \frac{q^{2n} u^2}{(1 - q^n u)^3} + \sum_{n \geq 1} \frac{nq^n}{1 - q^n}. \tag{2.5}
\]

1. Then the map

   \[
   \mathbb{K}^\times/q^\mathbb{Z} \longrightarrow E_q(K)
   \]

   \[
   u \mapsto (x(u, q), y(u, q))
   \]

   is an isomorphism of abelian groups.

   More generally, the map

   \[
   \bar{\mathbb{K}}^\times/q^\mathbb{Z} \longrightarrow E_q(\bar{K})
   \]

   \[
   u \mapsto (x(u, q), y(u, q))
   \]

   makes sense and is an isomorphism of \(G_{\mathbb{K}}\)-modules.

2. For each positive integer \(N\) prime to the characteristic of \(K\), there exists a canonical exact sequence

   \[
   0 \to \mu_N(\bar{K}) \to E_q[N](\bar{K}) \to \mathbb{Z}/(N) \to 0 \tag{2.6}
   \]

   of \(G_{\mathbb{K}}\)-modules.

**Remark 2.10.** Let us consider here the Tate curve \(E_q\) over \(K = \mathbb{Q}((q))\). Then, the exact sequence (2.5) does not split as \(G_{\mathbb{K}}\)-modules. However, consider the base change of \(E_q/K\) by the injection

\[
K \longrightarrow L := \mathbb{Q}(\zeta_N)((z))
\]

\[
q \mapsto z^N.
\]
Then, we have the isomorphism of $GL$-modules

$$
\mathbb{Z}/(N) \xrightarrow{\cong} \mu_{N,L}(\mathbb{L})
$$

$$
1 \mapsto \zeta_N.
$$

We also obtain the canonical section

$$
\mathbb{Z}/(N) \longrightarrow E_{q,L}[N](\mathbb{L}).
$$

$$
1 \mapsto z
$$

of the homomorphism $E_{q,L}[N](\mathbb{L}) \to \mathbb{Z}/(N)$ in the exact sequence (2.5). Therefore, the exact sequence splits and gives a canonical identification

$$
E_{q,L}[N] \cong \mu_{N,L} \times \mathbb{Z}/(N)
$$

$$
\cong \mathbb{Z}/(N) \times \mathbb{Z}/(N).
$$

Under this identification, it is known that the normalized Weil pairing $e_N$ sends each $((a,b), (c,d)) \in (\mathbb{Z}/(N) \times \mathbb{Z}/(N))^2$ to $\zeta_N^{-ad-bc}$; that is, $e_N(\zeta_N, z) = \zeta_N$. (See [1, VII, 1, 16].)

### 3 Construction of torsors

Our description of the 12-th roots of the discriminant of an elliptic curve by the torsion points consists of the following two parts: one needs some geometric properties of elliptic curves, and the other only needs a bit knowledge of linear algebra. In this section, we explain the linear-algebraic part. Throughout this section, we assume that $n = 3, 4$, and let $V$ denote a free $\mathbb{Z}/(n)$-module of rank 2. Our tasks here are to construct a set $T_n(V)$, which will later describe $\mu_n \sqrt{\Delta_E}$ when $V = E[n]$, and to define a simply transitive action of $\Lambda^2 V$ on $T_n(V)$.

#### 3.1 The construction of $T_3(V)$

Here, $V$ is a 2-dimensional vector space over $\mathbb{F}_3$. We construct a set $T_3(V)$ attached to $V$. We write $\mathbb{P}(V) := (V \setminus \{0\})/\{\pm 1\}$ for the projective line associated with $V$, and $\overrightarrow{P}$ for the image of a point $P \in V \setminus \{0\}$ in $\mathbb{P}(V)$. Note that $\# \mathbb{P}(V) = 4$.

**Definition 3.1.** We define a set $T_3(V)$ by

$$
T_3(V) = \{\{X, Y\} | X \sqcup Y = \mathbb{P}(V), \#X = \#Y = 2\}.
$$

That is, this is the set of 2-2 partitions of $\mathbb{P}(V)$.

For a basis $(P, Q)$ of $V$, we write $[P, Q] \in T_3(V)$ for $\{\overrightarrow{P}, \overrightarrow{Q}, \overrightarrow{P+Q}, \overrightarrow{P-Q}\}$. Since $\mathbb{P}(V) = \{\overrightarrow{P}, \overrightarrow{Q}, \overrightarrow{P+Q}, \overrightarrow{P-Q}\}$, the set $T_3(V)$ consists of 3 elements $[P, Q]$, $[P, P+Q]$, and $[P, P-Q]$.

**Remark 3.2.** For the later use, note that $T_3(V)$ has canonically a simply transitive action of the alternating group $\mathcal{A}(\text{Aut}(T_3(V)))$.  


3.2 The construction of $T_4(V)$

In this subsection, we define a set $T_4(V)$ for a free $\mathbb{Z}/(4)$-module $V$ of rank 2. Our construction of $T_4(V)$ for $n = 4$ is motivated by the definition of $w_4$ in Subsection 4.2.

Denote $V[2] = \ker(2 \times : V \to V)$ and define a set $S_4(V)$ by

$$S_4(V) = \{(P, Q, R) \in V^3 \mid \{2P, 2Q, 2R\} = V[2] \setminus 0\}.$$

For each $\sigma \in S_3$, define an involution $[\sigma]$ of $S_4(V)$ by $[\sigma](P_1, P_2, P_3) := (P'_1, P'_2, P'_3)$ with

$$P'_{\sigma(1)} = P_{\sigma(1)}, \quad P'_{\sigma(2)} = P_{\sigma(2)} + 2P_{\sigma(1)}, \quad \text{and} \quad P'_{\sigma(3)} = P_{\sigma(3)}.$$

Since $[\sigma]$'s commute with each other, we obtain an action of $F_2^3$ on $S_4(V)$. Combining this action with a canonical action of $S_3$ on $S_4(V)$ by permutations, we obtain an action of $G := S_3 \times F_2^3$ on $S_4(V)$. Here, the left action of $S_3$ on $F_2^3$ defining the semidirect product is given by $\tau \cdot [\sigma] = [\tau \sigma]$ for $\sigma, \tau \in S_3$. Let $N$ be the kernel of the composite

$$r : F_2^3 \to F_2^3 \to \{\pm 1\},$$

where the first map is the restriction to $\mathfrak{A}_3$ and the second map is the one sending $\sum a_\sigma[\sigma]$ to $(-1)^{\sum a_\sigma}$. Since the action of $S_3$ on $F_2^3$ defining the semidirect product induces an action of $\mathfrak{A}_3$ on $N$, we obtain $H := \mathfrak{A}_3 \rtimes N \triangleleft G$.

**Definition 3.3.** Under the above setting, define the set $T_4(V)$ by the quotient

$$T_4(V) := H \setminus S_4(V).$$

The equivalence class of $(P, Q, R) \in S_4(V)$ is denoted by $[P, Q, R] \in T_4(V)$.

Note that $T_4(V)$ has an action of $G/H = S_3/\mathfrak{A}_3 \times \{\pm 1\}$.

**Remark 3.4.**

1. The element $-1 \in G/H$ acts on $T_4(V)$ by

$$[P, Q, R] \mapsto -[P, Q, R] := [-P, -Q, -R].$$

Indeed, $-1 = r(\sum_{\sigma \in S_3}[\sigma])$ and

$$\sum_{\sigma \in S_3} [\sigma](P, Q, R) = (P + 2Q + 2R, Q + 2R + 2P, R + 2P + 2Q)$$

$$= (-P, -Q, -R)$$

in $S_4(V)$.

2. Define a set $S_2(V[2])$ by

$$S_2(V[2]) = \{(A, B, C) \in V[2]^3 \mid \{A, B, C\} = V[2] \setminus 0\}$$

equipped with the canonical action by $S_3$. Consider the quotient

$$T_2(V[2]) := \mathfrak{A}_3 \setminus S_2(V)$$

by the cyclic permutations; that is, it is the set of the cyclic orders on $V[2] \setminus 0$. The equivalence class of an element $(A, B, C) \in S_2(V[2])$ is denoted by
Remark 3.7. Let assertion follows from this and $G/H$ 

\[(12)\]

\[\text{Proof.}\]

By Lemma 3.11, the action of $C$ which is a contradiction. This shows (1) since $\#X = 4$.

Lemma 3.8. Let $C \in T_2(V[2])$. The map

\[\tilde{\pi} : S_4(V) \rightarrow S_2(V[2])\]

\[(P, Q, R) \mapsto (2P, 2Q, 2R)\]

is compatible with $\text{pr}_1 : G \rightarrow \mathfrak{S}_3$. Hence, it induces a map

\[\pi : T_4(V) \rightarrow T_2(V[2]),\]

which is compatible with $\text{pr}_1 : G/H \rightarrow \mathfrak{S}_3/\mathfrak{A}_3$. Thus $\mathfrak{S}_3/\mathfrak{A}_3 \subset G/H$ switches the fibers of $\pi$ and $\{\pm 1\} = \ker(\text{pr}_1) \subset G/H$ preserves each fiber of $\pi$.

**Lemma 3.5.** The action of $G$ on $S_4(V)$ is simply transitive.

**Proof.** We use the notation in Remark 3.4. Since the action of $\mathfrak{S}_3$ on $S_2(V)$ is simply transitive and $\tilde{\pi}$ is compatible with $\text{pr}_1 : G \rightarrow \mathfrak{S}_3$, it is enough to prove that $\mathbb{F}_2^{\mathfrak{S}_3} = \ker(\text{pr}_1)$ acts on each fiber of $\tilde{\pi}$ simply transitively.

To prove this, let us fix an element $(A_1, A_2, A_3) \in S_4(V)$ and consider its fiber $F$ of $\tilde{\pi}$. We make an identification $f : \mathbb{F}_2^{\mathfrak{S}_3} \xrightarrow{\sim} V[2]^3$ by sending $[\sigma]$ to $(A_1, A_2, A_3)$ with $A_1^\sigma(2) = A_2^\sigma(1)$ and $A_1^\sigma(1) = A_2^\sigma(3) = 0$. If we define an action of $V[2]^3$ on $F$ by the componentwise addition, then the action $\mathbb{F}_2^{\mathfrak{S}_3}$ on $F$ is identified via $f$ with the action $V[2]^3$ on it, which obviously acts simply and transitively on $F$. \[\square\]

**Corollary 3.6.** We have $\#T_4(V) = 4$.

**Proof.** By Lemma 3.11, the action of $G/H$ on $T_4(V)$ is simply transitive. Our assertion follows from this and $\#G/H = 4$. \[\square\]

**Remark 3.7.** Let $[P, Q, R] \in T_4(V)$. Since $G/H = \mathfrak{A}_3 \times \{\pm 1\}$ is generated by $(12, 1)$ and $(id, -1)$, we see that

\[T_4(V) = (G/H) \cdot [P, Q, R]\]

\[= \{\pm [P, Q, R], \pm [Q, P, R]\}.\]

We use the following lemma and remark in the next subsection to define an action of $\mathbb{A}^2 \times V$ on $T_4(V)$.

**Lemma 3.8.** Let $X$ be a set consisting of 4 elements. Denote by $S_1$ the set of cyclic subgroup of order 4 in $\text{Aut}(X)$, and by $S_2$ the set of elements in $\text{Aut}(X)$ of order 2 with no fixed points on $X$.

1. For any $C \in S_1$, the action of $C$ on $X$ is simply transitive. In particular, the order 2 element $\tau$ in $C$ belongs to $S_2$.

2. Mapping each $C \in S_1$ to its element of order 2 defines a bijection $d : S_1 \xrightarrow{\sim} S_2$. For any $\tau \in S_2$, we denote $d^{-1}(\tau)$ by $B(\tau)$.

**Proof.** (1) Considering the orbit decomposition of $X$ by $C$, we see that the action of $C$ on $X$ is transitive; if not, any element of $C$ must be of order 1 or 2, which is a contradiction. This shows (1) since $\#C = \#X = 4$.

(2) By (1), we can define the map $d$. Note that $\text{Aut}(X)$ acts transitively on both $S_1$ and $S_2$ by conjugation, and that $d$ commutes with these actions. Also, $\#S_1 = \#S_2 = 3$, since there are 6 elements of order 4 in $\text{Aut}(X)$ and each $C \in S_1$ has two generators, and since $S_2$ is identified with the set of 2-2 partitions via the orbit decompositions. These shows that $d$ is bijective. \[\square\]
3.3 The action of $\bigwedge^2 V$ on $T_n(V)$

For each basis $(P, Q)$ of $V$, we denote by $\varphi_{P, Q} \in \text{SL}(V)$ the map determined by $\varphi_{P, Q}(P) = P$ and $\varphi_{P, Q}(Q) = P + Q$.

**Lemma 3.9.** There exists a unique surjective homomorphism $\varphi : \bigwedge^2 V \twoheadrightarrow \text{SL}(V)^{ab}$ such that, for any basis $(P, Q)$ of $V$, $\varphi$ maps $P \wedge Q$ to $\varphi_{P, Q} \in \text{SL}(V)^{ab}$.

**Proof.** For a basis $(P, Q)$ of $V$, mapping a generator $P \wedge Q$ of $\bigwedge^2 V$ to $\varphi_{P, Q} \in \text{SL}(V)^{ab}$ defines a homomorphism $\varphi : \bigwedge^2 V \rightarrow \text{SL}(V)^{ab}$. To see that $\varphi$ is independent of the choice of $(P, Q)$, we claim that, for $u \in \text{GL}(V)$, we have $\varphi_{P, Q}^{\det u} \equiv \varphi_{uP, uQ}$ in $\text{SL}(V)^{ab}$. Let $v$ be an element of $\text{GL}(V)$ given by $v(P) = P$ and $v(Q) = (\det u)Q$. Then, we have $\varphi_{P, Q}^{\det u} = \varphi_{P, (\det u)Q} = v \varphi_{P, Q} v^{-1}$. Also, $\varphi_{uP, uQ} = u \varphi_{P, Q} u^{-1}$. Since $u^{-1}v \in \text{SL}(V)$, the claim follows.

By the above claim, we see that $\varphi$ is surjective as follows. Because $\text{SL}(V)$ is generated by all the elements $\varphi_{uP, uQ} = u \varphi_{P, Q} u^{-1}$ with $u \in \text{GL}(V)$, the claim shows that $\text{SL}(V)^{ab}$ is generated by $\varphi_{P, Q}^{-1} 1$, and thus by $\varphi(P \wedge Q) = \varphi_{P, Q}$.

We let $\text{SL}(V)$ canonically act on $T_n(V)$ and consider the corresponding homomorphism $\tilde{\psi} : \text{SL}(V) \twoheadrightarrow \text{Aut}(T_n(V))$.

**Proposition 3.10.** (1) Let $C$ denote the subgroup $\mathfrak{A}(\text{Aut}(T_3(V)))$ (resp. $C(-1)$ as in Lemma 3.8) of $\text{Aut}(T_n(V))$ for $n = 3$ (resp. $n = 4$). Then, the map $\psi$ induces an isomorphism

$$\psi : \text{SL}(V)^{ab} \cong C.$$

(2) The surjective map $\varphi : \bigwedge^2 V \rightarrow \text{SL}(V)^{ab}$ in Lemma 3.9 is an isomorphism.

**Proof.** (1) (2) We first prove that the map $\tilde{\psi}$ induces a surjective homomorphism

$$\psi : \text{SL}(V)^{ab} \rightarrow C.$$

Since $\text{SL}(V)$ is generated by the elements $\varphi_{X,Y}$ for all bases $(X, Y)$ of $V$, it suffices to show that, for a basis $(P, Q)$ of $V$, $\psi$ maps $\varphi_{P, Q}$ to a generator of $C$.

For $n = 3$, this follows because $T_3(V) = \{[P, Q], [P, P + Q], [P, 2P + Q]\}$ and $\varphi_{P, Q}(P, P + Q) = [P, (i + 1)P + Q]$.

We next consider the case $n = 4$. Since $\varphi_{P, Q}^{-1}[P, Q, P + Q] = [P, Q + 2P, (P + Q) + 2P] = ([\text{id}] + [23])[P, Q, P + Q] = -[P, Q, P + Q]$, we see that $\psi(\varphi_{P, Q})$ is of order 4. Further, by Lemma 3.8, $\psi(\varphi_{P, Q}^2)$ is of order 2 with no fixed points, which implies that $\varphi_{P, Q}^2 \in \text{SL}(V)^{ab}$ must be $[Q, P, P + Q]$. Therefore, $\tilde{\psi}(\varphi_{P, Q}^2) = -1$ and $C(-1)$ is generated by $\varphi_{P, Q}$.

The surjective maps $\psi$ and $\varphi$ are actually bijective because $\# \bigwedge^2 V = \# C(=4)$.

We now define an action of $\bigwedge^2 V$ on $T_n(V)$ by the composition

$$\psi \circ \varphi : \bigwedge^2 V \twoheadrightarrow \text{SL}(V)^{ab} \cong C \subset \text{Aut}(T_n(V)).$$

**Corollary 3.11.** The action of $\bigwedge^2 V$ on $T_n(V)$ is simply transitive.
Proof. This follows from Remark 3.2, Lemma 3.8 (1), and Proposition 3.10. \(\square\)

Next, we see that the action \(\bigwedge^2 V \cong T_n(V)\) has a simple description when \(V\) is moreover accompanied with an extension

\[
0 \to L \to V \xrightarrow{p} \mathbb{Z}/(n) \to 0
\]

(3.1) of \(\mathbb{Z}/(n)\). We observe the following:

1. Denote \(p^{-1}(1)\) by \(T\). Then, mapping each \(P \in L\) to \(P \wedge Q\) with \(Q \in T\) defines an isomorphism \(\epsilon : L \xrightarrow{\cong} \bigwedge^2 V\), which is independent of the choice of \(Q \in T\).

2. Corresponding to the above extension, we let \(L\) act on \(V\) by an injective homomorphism \(\tilde{\varphi} : L \hookrightarrow \text{SL}(V)\) defined by \(\tilde{\varphi}(P)(Q) := Q + p(Q)P\) for \(P \in L\) and \(Q \in V\). Note that, if we define a subgroup \(M\) of \(\text{SL}(V)\) by

\[
M = \{ \sigma \in \text{SL}(V) : \sigma(P) = P \text{ for all } P \in L \},
\]

then \(\tilde{\varphi}\) induces an isomorphism \(\tilde{\varphi} : L \xrightarrow{\cong} M\), whose inverse \(f : M \to L\) is obviously given by

\[
f(\sigma) = \sigma(Q) - Q\]

with any \(Q \in T\). We also remark that the action \(L \cong M \acts V\) preserves \(T\), which coincides with the canonical action by translations; in particular, this action of \(L\) on \(T\) is obviously simply transitive.

Example 3.12. (1) If \(V = E[n]\) for a Tate curve \(E\), then we have a canonical extension (2.6) in Theorem 2.9.

(2) If we fix a basis \((P, Q)\) of \(V\), then we have an extension

\[
0 \to \langle P \rangle \to V \xrightarrow{p} \mathbb{Z}/(n) \to 0,
\]

(3.2) where \(p : V \to \mathbb{Z}/(n)\) is given by \(p(P) = 0\) and \(p(Q) = 1\).

Remark 3.13. (1) Any extension (3.1) can becomes of the form (3.2) by taking a basis \((P, Q)\) with \(P\) a generator of \(L\) and \(Q \in T\).

(2) For any extension (3.1), the following diagram is commutative:

\[
\begin{array}{ccc}
L & \xrightarrow{\epsilon} & \bigwedge^2 V \\
\downarrow \varphi & & \downarrow \varphi \\
M & \xrightarrow{\text{quotient}} & \text{SL}(V)_{\text{ab}}
\end{array}
\]

To see this, we may assume that (3.1) is of the form (3.2) by (1). Then, we obtain \(\varphi(P)(Q) = \varphi_{P,Q}\) and \(\epsilon(P) = P \wedge Q\) so that \(\varphi(\epsilon(P)) = \varphi_{P,Q} \in \text{SL}(V)_{\text{ab}}\).

For the given extension (3.1), we define a map \(\tau : T \to T_n(V)\) by \(\tau(Q) = [P, Q]\) (resp. \(\tau(Q) = \left[Q, P, -(P + Q)\right]\) for \(n = 3\) (resp. \(n = 4\)) with \(P\) a generator of \(L\).

Lemma 3.14. (1) The map \(\tau\) is independent of the choice of \(P\).

(2) The map \(\tau\) is compatible with \(\epsilon : L \xrightarrow{\cong} \bigwedge^2 V\).

(3) The map \(\tau\) is bijective.
Proof. (1) The other generator of \( L \) is \(-P\) for both cases \( n = 3 \) and \( n = 4 \). If \( n = 3 \), then it defines the same point in \( \mathbb{P}(V) \) as \( P \). If \( n = 4 \), then we see that 
\[
[Q, -P, -(P + Q)] = ([123] + [id] + [13])[Q, P, -(P + Q)] = [Q, P, -(P + Q)]
\]
for \( Q \in T \). These prove (1).

(2) First, note that \( \tau \) is tautologically compatible with \( \tilde{\varphi} : L \to \text{SL}(V) \). By Proposition 3.10 (1), it is compatible with the composite map \( L \xrightarrow{\tilde{\varphi}} \text{SL}(V) \to \text{SL}(V)^{ab} \), which coincides with the composite map \( L \xrightarrow{\varphi} \bigwedge^2 V \xrightarrow{\tilde{\varphi}} \text{SL}(V)^{ab} \) by Remark 3.13 (2). Thus (2) follows, since the action of \( \bigwedge^2 V \) on \( T_n(V) \) is defined via \( \varphi : \bigwedge^2 V \xrightarrow{\tilde{\varphi}} \text{SL}(V)^{ab} \).

Remark 3.15. We can also deduce Corollary 3.11 from Lemma 3.14 as follows. Fix an extension \([3.1]\). By Lemma \([3.14]\), we identify the action \( \bigwedge^2 V \rhd T_n(V) \) with the action \( L \rhd T \), which is obviously simply transitive.

4 A bijection \( w_n : T_n(E[n]) \to \mu_n \sqrt{\Delta_E} \)

Here, let \( n \) be 3 or 4, and \( E \) be an elliptic curve given by a Weierstrass equation over a field \( K \) of characteristic prime to \( n \). We apply the construction in Section 3 to \( V = E[n] \), and construct a bijection \( w_n : T_n(E[n]) \to \mu_n \sqrt{\Delta_E} \).

4.1 The case \( n = 3 \)

The result in this section is based on 5.5, [7]. Fix a Weierstrass equation
\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}
\]
for \( E \), and denote its discriminant by \( \Delta \). Let \( b_i \) \((i = 2, 4, 6, 8)\) be the constants defined in Definition 2.3. For a point \( P \) on \( E \), we denote by \((x_P, y_P)\) its coordinate in terms of this Weierstrass equation, and by \( \Delta \) the discriminant of it. If \( P \) is a point of order 3, then \( P \) satisfies \( x_P = x_{-P} = x_{2P} \). Since
\[
x_{2P} = \frac{x_P^4 - b_4x_P^2 - 2b_6x_P - b_8}{4x_P^3 + b_2x_P^2 + 2b_4x_P + b_6}
\]

(III, 2.3, [8]), the \( x \)-coordinate of any point of order 3 is a solution of the equation
\[
x = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6};
\]
that is,
\[
x^4 + \frac{b_2}{3}x^3 + b_4x^2 + b_6x + \frac{b_8}{3} = 0. \tag{4.2}
\]
For \( \{X, Y\} \in T_3(E[3]) \), let \( x_1 \) and \( x_2 \) be the \( x \)-coordinates of the elements in \( X \), and \( x_3 \) and \( x_4 \) be the \( x \)-coordinates of the elements in \( Y \). Using this, we define
\[
w_3(\{X, Y\}) := b_4 - 3(x_1x_2 + x_3x_4),
\]
which is obviously \( G_K \)-equivariant.

**Lemma 4.1.** Let the notation be as above. Then,
\[
T^3 - \Delta = \prod (T - w_3(\{X, Y\})),
\]
where the product is taken over \( T_3(E[3]) \). In other words, \( w_3 \) defines a bijection \( w_3 : T_3(E[3]) \to \mu_3 \sqrt{\Delta_E} \).

**Proof.** We first show our assertion when \( E \) is defined over a field \( K \) and (4.1) is of the Deuring normal form
\[
y^2 + \alpha xy + y = x^3 \quad (\alpha \in \bar{K}, \alpha^3 \neq 27).
\]
In this case, we have
\[
b_2 = \alpha^2, b_4 = \alpha, b_6 = 1, b_8 = 0, \text{ and } \Delta = \alpha^3 - 27.
\]
Then, (4.2) is
\[
X^4 + \frac{1}{3}\alpha^2 X^3 + \alpha X^2 + X = 0,
\]
and the solutions of (4.4) are just the \( x \)-coordinates \( x_1, \ldots, x_4 \) of \( E[3] \); one of which is 0, say \( x_4 = 0 \). It follows that
\[
X^3 + \frac{1}{3}\alpha^2 X^2 + \alpha X + 1 = (X - x_1)(X - x_2)(X - x_3).
\]
Note that, under our present assumption, (4.3) becomes
\[
T^3 - (\alpha^3 - 27) = \prod_{1 \leq i < j \leq 3} (T - \alpha + 3x_ix_j).
\]
Replacing \( Y = T - \alpha \) reduces the problem to showing that
\[
Y^3 + 3\alpha Y^2 + 3\alpha^2 Y + 27 = (Y + 3x_1x_2)(Y + 3x_2x_3)(Y + 3x_1x_3).
\]
This is true from the following computation: Setting \( X = 3/Y \) in (4.5) and using \( x_1x_2x_3 = -1 \), we see that (4.5) becomes
\[
\frac{1}{Y^3}(27 + 3\alpha^2 Y + 3\alpha Y^2 + Y^3) = \frac{1}{Y^3}(3 - x_1Y)(3 - x_2Y)(3 - x_3Y)
\]
\[
= -\frac{x_1x_2x_3}{Y^3}(-3x_1^{-1} + Y)(-3x_2^{-1} + Y)(-3x_3^{-1} + Y)
\]
\[
= \frac{1}{Y^3}(3x_2x_3 + Y)(3x_1x_3 + Y)(3x_1x_2 + Y),
\]
which is none other than (4.6).

Next, we prove the general case. Suppose we are given two Weierstrass equations for \( E \) over \( K \) with coordinates \( (x, y) \) and \( (x', y') \). We use the notation in Remark 2.5. (1). By (2.1) and (2.3), we obtain
\[
b_4 - 3(x_1x_j + x_kx_l) = u^4(b'_4 - 3(x'_1x'_j + x'_kx'_l)).
\]
By (2.3) and (4.7), it follows that (4.3) for \((x, y)\) is equivalent to (4.3) for \((x', y')\). Then, the assertion follows from the fact that any elliptic curve over \(K\) has a Weierstrass equation of the Deuring normal form over \(\bar{K}\). (This requires \(\text{char}(K) \neq 3\). For the detail, see Proposition 1.3, Appendix A, [8].)

Let us check how the map \(w_3\) changes if we take another Weierstrass equation for \(E\). Let the notation be as in Remark 2.5 (1), and denote by \(w'_3\) the map as above for another Weierstrass equation for \(E\) with the coordinate \((x', y')\).

**Lemma 4.2.** We have \(w_3 = u^4w'_3\).

**Proof.** Let \((P, Q)\) be a basis of \(E[3]\). Then \(x_P, x_Q, x_{P+Q},\) and \(x_{P-Q}\) are all distinct, and they must satisfy the above equation. Considering the coefficients of \(x^3\) in (4.2), we obtain

\[
x_P + x_Q + x_{P+Q} + x_{P-Q} = -\frac{b_2}{3}.
\]

Using this equality and the relations in Remark 2.5 (1), we obtain \(w_3([P, Q]) = u^4w'_3([P, Q])\). \(\square\)

Lemma 4.2 and \(\Delta = u^{12}\Delta'\) imply that the diagram

\[
\begin{array}{ccc}
T_3(E[3]) & \xrightarrow{w_3} & \mu_3 \sqrt{\Delta} \\
\downarrow & & \downarrow \\
\mu_3 \sqrt{\Delta} & \xrightarrow{u^4} & \mu_3 \sqrt{\Delta'}
\end{array}
\]

is commutative. Since the vertical map \(u^4\) is an isomorphism of \(\mu_3\)-torsors over \(k\), we identify \(w_3\) and \(w'_3\), and we consider them as a map from \(T_3(E[3])\) to the \(\mu_3\)-torsor \(\mu_3 \sqrt{\Delta_E}\). We denote this map again by \(w_3\).

**Remark 4.3.** The construction of \(T_3(E[3])\) and \(w_3\) are easily generalized to the case that \(E\) is an elliptic curve over a scheme \(S\) with 3 invertible. This is done by considering the locally constant étale sheaf \(E[3]\) over \(S\) and by étale descent.

#### 4.2 The case \(n = 4\)

Since \(K\) is of characteristic prime to 2, we can take a Weierstrass equation for \(E\) of the form

\[
y^2 = x^3 + a_2x^2 + a_4x + a_6.
\]

In this subsection, we only consider Weierstrass equations of this form. In order to write a 4-th root of \(\Delta_E\) in terms of \(E[4]\), first we prove the following lemma.

(See also [4, §11].)

**Lemma 4.4.** Let the notation be as above. Let \(A \in E\) be a point of order 2, and \(P\) and \(P'\) be points of \(E\) satisfying \(2P = 2P' = A\) and \(P \neq \pm P'\). Then we have

\[
\left(\frac{y_P - y_{P'}}{x_P - x_{P'}}\right)^2 = x_A - x_{P-P'}.
\]
Proof. Denote $B$ and $C$ for the points of order 2 on $E$ other than $A$. Then, note that
\[ x^3 + a_2x^2 + a_4x + a_6 = (x - x_A)(x - x_B)(x - x_C), \]
and in particular we have $x_A + x_B + x_C = -a_2$. Since $P + P' + (-P - P') = O$, the three points $P, P'$, and $-P - P'$ are colinear. So the solutions for the equation
\[ \left( \frac{y_P - y_{P'}}{x_P - x_{P'}} \right) (x - x_P) + y_P \right)^2 = x^3 + a_2x^2 + a_4x + a_6 \]
are exactly $x_P, x_{P'},$ and $x_{-P - P'}(= x_{P + P'})$. Considering the coefficients of $x^2$, we have
\[ x_P + x_{P'} + x_{P + P'} = \left( \frac{y_P - y_{P'}}{x_P - x_{P'}} \right)^2 - a_2. \tag{4.8} \]
On the other hand, we show
\[ x_P + x_{P'} = 2x_A. \tag{4.9} \]
To prove (4.9), let $T$ be a 4-division point of $E$ with $2T = A$. Then the same argument as above shows that
\[ 2x_T + x_A = \left( \frac{y_T - y_A}{x_T - x_A} \right)^2 - a_2. \tag{4.10} \]
Combining (4.10) with
\[ (y_T - y_A)^2 = y_T^2 = (x_T - x_A)(x_T - x_B)(x_T - x_C), \]
we have the following quadratic equation for $x_T$:
\[ x_T^2 - (-a_2 + x_A - x_B - x_C)x_T - (x_A^2 + a_2x_A + x_Bx_C) = 0. \]
Since the solutions for this equation are exactly $x_P$ and $x_{P'}$, we obtain
\[ x_P + x_{P'} = -a_2 + x_A - x_B - x_C \]
\[ = 2x_A, \]
and hence (4.9) follows.

Now, combining (4.8) and (4.9), we obtain
\[ x_A + (x_A + x_{P + P'}) = \left( \frac{y_P - y_{P'}}{x_P - x_{P'}} \right)^2 - a_2. \tag{4.11} \]
Since
\[ \{A, P + P', P - P'\} = E[2] \setminus O, \]
we have
\[ x_A + x_{P + P'} + x_{P - P'} = -a_2. \tag{4.12} \]
Then, (4.11) and (4.12) show the lemma. $\square$

An immediate corollary of Lemma 4.4 is the following:
Corollary 4.5. For \((P, Q, R) \in S_4(E[4])\), set
\[ P' = P + 2Q, Q' = Q + 2R, R' = R + 2P. \]
Then
\[ \tilde{w}_4(P, Q, R) := \frac{y_P - y_{P'}}{x_P - x_{P'}} - \frac{y_Q - y_{Q'}}{x_Q - x_{Q'}} - \frac{y_R - y_{R'}}{x_R - x_{R'}} \]
is a 4-th root of \(\Delta\), and the map \(\tilde{w}_4 : S_4(E[4]) \to \mu_4 \sqrt[4]{\Delta}\) makes the following diagram commutative:
\[
\begin{array}{ccc}
S_4(E[4]) & \xrightarrow{\tilde{w}_4} & \mu_4 \sqrt[4]{\Delta} \\
\downarrow \pi & & \downarrow \text{squaring} \\
S_2(E[2]) & \xrightarrow{\tilde{w}_2} & \pm \sqrt[4]{\Delta},
\end{array}
\]
where \(\tilde{w}_2 : S_2(E[2]) \to \pm \sqrt[4]{\Delta}\) is a canonical bijection given by
\[ \tilde{w}_2(A, B, C) := 4(x_A - x_B)(x_B - x_C)(x_C - x_A). \]

Remark 4.6. Let the notation be as in Corollary 4.5. Then, we see that
\[ \tilde{w}_4(-P, Q, R) = -\tilde{w}_4(P, Q, R) \]
\[ \tilde{w}_4(P', Q, R) = \tilde{w}_4(P, Q, R) \]
for \((P, Q, R) \in S_4(E[4])\). We also have the analogous properties for \(Q\) and \(R\).

Suppose that we are given two Weierstrass equations defining \(E\) with co-ordinates \((x, y)\) and \((x', y')\). Denote the above maps by \(w_4\) and \(w_4'\), and their discriminants by \(\Delta_4\) and \(\Delta'_4\), respectively.

Lemma 4.7. We have \(\tilde{w}_4 = u^3 \tilde{w}_4'\).

Proof. This is obvious from Remark 2.5 (2). \(\square\)

Lemma 4.7 and \(u^{12} \Delta' = \Delta\) give the following commutative diagram:

\[
\begin{array}{ccc}
S_4(E[4]) & \xrightarrow{\tilde{w}_4} & \mu_4 \sqrt[4]{\Delta} \\
& \downarrow u^3 \times & \\
& \mu_4 \sqrt[4]{\Delta} \\
\end{array}
\]

By the same reason explained at the end of the last subsection, we identify \(\tilde{w}_4\) and \(\tilde{w}_4'\), and we consider them as a map from \(S_4(E[4])\) to the \(\mu_4\)-torsor \(\mu_4 \sqrt[4]{\Delta_E}\). Denote this map simply by \(\tilde{w}_4\).

Lemma 4.8. The map \(\tilde{w}_4 : S_4(E[4]) \to \mu_4 \sqrt[4]{\Delta_E}\) factors through the quotient \(T_4(E[4])\).
Proof. We use the notation in Subsection 3.3 and Corollary 4.5. It is obvious that \( \tilde{w}_4 \) is invariant under the action of \( \mathfrak{S}_3 \). We claim that for each \((P, Q, R) \in S_4(E[4])\) we have

\[
\tilde{w}_4([\sigma](P, Q, R)) = \begin{cases} 
-\tilde{w}_4(P, Q, R) & \text{(if } \sigma \in \mathfrak{S}_3 \text{ is even)} \\
\tilde{w}_4(P, Q, R) & \text{(if } \sigma \in \mathfrak{S}_3 \text{ is odd)}.
\end{cases}
\] (4.13)

Since every \([\sigma]\) for even (resp. odd) \(\sigma\) is conjugate to \([id]\) (resp. to \([(12)]\) by an element in \(\mathfrak{A}_3 \subset \text{Aut}(S(E[4]))\), it is enough to check the claim for \([id]\) and \([(12)]\). In these cases, we see that

\[
\tilde{w}_4([id](P, Q, R)) = \tilde{w}_4(P, -Q', R) = -\tilde{w}_4(P, Q, R) \\
\tilde{w}_4([(12)](P, Q, R)) = \tilde{w}_4(P', Q, R) = \tilde{w}_4(P, Q, R)
\]

by Remark 4.6.

Lemma 4.8 gives us a map

\[
w_4 : T_4(E[4]) \longrightarrow \mu_4 \sqrt[4]{\Delta_E} \\
[P, Q, R] \mapsto \tilde{w}_4(P, Q, R)
\]

induced from \(\tilde{w}_4\), which is \(G_K\)-equivariant as in the case \(n = 3\).

Remark 4.9. The commutative diagram in Corollary 4.5 induces a commutative diagram

\[
\begin{array}{ccc}
T_4(E[4]) & \xrightarrow{w_4} & \mu_4 \sqrt[4]{\Delta} \\
\downarrow \pi & & \downarrow \text{squaring} \\
T_2(E[2]) & \xrightarrow{w_2} & \pm \sqrt[2]{\Delta}
\end{array}
\]

of \(G_K\)-sets. Here, \(w_2\) is the map induced from \(\tilde{w}_2\). By Remark 4.6 \(w_4\) is compatible with \(pr_2 : G/H \rightarrow \{\pm 1\}\).

Corollary 4.10. The map \(w_4 : T_4(E[4]) \rightarrow \mu_4 \sqrt[4]{\Delta_E}\) is bijective.

Proof. Fix an element \(X \in T_4(E[4])\). Since \(w_4\) is compatible with \(pr_2 : G/H \rightarrow \{\pm 1\}\),

\[
w_4(T_4(E[4])) = w_4((G/H) \cdot X) = \{\pm w_4(X), \pm w(\sigma X)\}
\]

for any odd permutation \(\sigma \in \mathfrak{S}_3\). The commutativity of the diagram in Remark 4.11 shows that \(\pm w_4(X)\) and \(\pm w(\sigma X)\) belong to distinct fibers of the squaring map \(\mu_4 \sqrt[4]{\Delta} \rightarrow \pm \sqrt[4]{\Delta}\). Thus, we obtain \(#w_4(T_4(E[4])) = 4\) and hence \(w_4\) is bijective.

Remark 4.11. For the same reason as in Remark 4.3 we can define \(T_4(E[4])\) and \(w_4\) for an elliptic curve over a scheme on which \(4\) is invertible.

16
4.3 The Tate curve case

Let $E = E_q$ be the Tate curve over the field $K = \mathbb{Q}((q))$ of Laurent series. By Theorem [2.9] (1), $E[n]$ is canonically an extension of $\mathbb{Z}/(n)$ in the category of $G_K$-modules:

$$0 \to \mu_n \to E[n] \to \mathbb{Z}/(n) \to 0.$$ 

For this extension, we use the notations and results in Subsection 3.3 by setting $V = E[n]$. In our Tate curve case, we identify

$$L = \mu_n,$$

$$T = \mu_n \sqrt[2]{q},$$

$$\epsilon = e_n^{-1} : L \xrightarrow{\sim} \bigwedge^2 E[n],$$

the last equality of which is due to Remark [2.10].

Note that the action of $G_K$ on $E[n]$ gives rise to an isomorphism

$$g : \text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n)) \xrightarrow{\sim} M.$$ 

We also remark that the composite map $f \circ g : \text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n)) \xrightarrow{\sim} M \xrightarrow{\sim} L = \mu_n$ is the Kummer character $h_1$ mapping $\sigma \in \text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n))$ to $\sigma(\sqrt[2]{q})/\sqrt[2]{q}$.

**Proposition 4.12.** The composition $w_n \circ \tau : T \to \mu_n \sqrt[2]{\Delta_E}$ is an isomorphism of $L = \mu_n$-torsors over $K$.

**Proof.** It is obvious from the constructions that $w_n \circ \tau$ is $G_K$-equivariant. We show that it is also $\mu_n$-equivariant. By definition, the action of $L$ on $T$ is identified with the action of $M$ on $T$ via the isomorphism $\tilde{\phi} : L \xrightarrow{\sim} M$, which is also identified with the action of $\text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n))$ on $T$ via $g : \text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n)) \xrightarrow{\sim} M$. On the other hand, the action of $G_K$ on $\mu_n \sqrt[2]{\Delta}$ induces an action of $\text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n))$ on $\mu_n \sqrt[2]{\Delta}$, which is identified with a canonical action of $\mu_n$ on $\mu_n \sqrt[2]{\Delta}$ via the Kummer character $h_2 : \text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n)) \xrightarrow{\sim} \mu_n$ mapping $\sigma$ to $\sigma(\sqrt[2]{\Delta})/\sqrt[2]{\Delta}$. Since $w_n \circ \tau$ is $G_K$-equivariant, it is also $\text{Gal}(K(\mu_n, \sqrt[2]{q})/K(\mu_n))$-equivariant. These arguments imply that the map $w_n \circ \tau : T \to \mu_n \sqrt[2]{\Delta_E}$ is compatible with $h_2 \circ (f \circ g)^{-1} = h_2 \circ h_1^{-1} : L \to \mu_n$, which is the identity map since $\sqrt[2]{\Delta}/\sqrt[2]{q} \in K(\mu_n)^\times$ by (2.3). Therefore, $w_n \circ \tau$ is $L = \mu_n$-equivariant. \( \square \)

**Corollary 4.13.** The map $w_n$ is compatible with the normalized Weil pairing $\epsilon_n$.

**Proof.** This immediately follows from Corollary [3.14] (2) (3), Proposition [4.12] and $\epsilon_n = \epsilon^{-1}$. \( \square \)

Next we consider the following canonical isomorphism

$$\delta : T \to \mu_n \sqrt[2]{\Delta_E}$$

$$z \mapsto z \prod_{m \geq 1} (1 - q^m)^{2q/n}$$

of $L = \mu_n$-torsors over $K$. 

17
Proposition 4.14. We have $w_4 \circ \tau = \delta$.

Proof. By Proposition 4.12, the composite map $\sigma := (w_n \circ \tau) \circ \delta^{-1}$ is an automorphism of the $\mu_n$-torsor $\mu_n \sqrt{\Delta_E}$ over $K$, and hence $\sigma$ belongs to $\mu_n(K) \subset \text{Aut}(\mu_n \sqrt{\Delta_E})$. Because $\mu_n(K) = \{1\}, \{\pm 1\}$ for $n = 3, 4$ respectively, the assertion for $n = 3$ is proved, but there remains a possibility of $w_4 \circ \tau = -\delta$.

To determine the sign of $\sigma$ for $n = 4$, we check that the first coefficient of $w_4(\tau(z))$, which belongs to $\mathbb{Q}(i)((z))$, coincides with that of $\delta(z) = z \prod_{m>1}(1-\varphi^m)^6$; that is, $\tau$. Note that, if $(P, Q, R) = \tau(z) = (z, i(z)^{-1})$ and if $P', Q', R'$ are as in Corollary 4.13 then we obtain $(P', Q', R') = (-z, -iz^2, -iz)$.

Change variables of $E$ as

$$X = x \quad \text{and} \quad Y = y + \frac{1}{2}x$$

to make the Weierstrass equation of $E$ into the form

$$Y^2 = X^3 + A_2X^2 + A_4X + A_6.$$

Then, it follows from Theorem 2.9 that

$$K^x/\mathbb{Q} \xrightarrow{\sim} \left\{ \text{$\bar{K}$-valued points on } y^2 + xy = x^3 + a_4x + a_6 \right\} \xrightarrow{\sim} \left\{ \text{$\bar{K}$-valued points on } Y^2 = X^3 + A_2X^2 + A_4X + A_6 \right\}$$

with

$$u \quad \mapsto \quad (x(u, q), y(u, q)) \quad \mapsto \quad (x(u, q), y(u, q) + \frac{1}{2}x(u, q))$$

We have

$$x(u) := x(u, z^4) = f(u) + \sum_{n \geq 1} \frac{z^{4n}u}{(1 - z^{4n}u)^2} + \frac{z^{4n}u^{-1}}{(1 - z^{4n}u^{-1})^2} - 2z^{4n}u \quad \text{mod } z^3,$$

where $f(u) = \frac{u}{(1 - u)} \equiv u + 2u^2 \quad \text{mod } z^3$. Also, set

$$Y(u) := y(u, z^4) + \frac{1}{2}x(u, z^4) = \frac{1}{2} \sum_{n \in \mathbb{Z}} \frac{z^{4n}u(1 + z^{4n}u)}{(1 - z^{4n}u)^2} - 1 \left( \frac{1}{z^{4n}u^{-1} - 1} \right)^3 - \frac{z^{4n}u(1 + z^{4n}u)}{(1 - z^{4n}u)^3},$$

where $g(u) = u(1 + u)/2(1 - u)^3 \equiv \frac{1}{2}u + 2u^2 \quad \text{mod } z^3$. Note that the second term of $x(u)$ and $Y(u)$ is congruent to 0 (mod $z^3$) whenever the degree of $u \in \mathbb{Q}(i)((z))$ in $z$ is of 0, ±1, ±2, and that $f(u) = f(u^{-1})$ and $g(u) = -g(u^{-1})$. Then, the computation goes as follows:

$$w_4([z, i, iz]) = 2 \frac{Y(z) - Y(-z)}{x(z) - x(-z)} \cdot \frac{Y(i) - Y(-iz^2)}{x(i) - x(-iz^2)} \cdot \frac{Y(i(z^{-1}) - Y(-iz)}{x((iz)^{-1}) - x(-iz)}$$

$$\equiv 2 \left( \frac{g(z) - g(-z)}{f(z) - f(-z)} \cdot \frac{g(i) - g(-iz^2)}{f(i) - f(-iz^2)} \cdot \frac{g((iz)^{-1}) - g(-iz)}{f((iz)^{-1}) - f(-iz)} \right) \quad \text{mod } z^3. \quad (4.14)$$

For each factor in the right hand side of (4.14), we see that

$$\frac{g(z) - g(-z)}{f(z) - f(-z)} \equiv \frac{z}{2z} \quad \text{mod } z^2$$

$$\equiv \frac{1}{2} \quad \text{mod } z^2,$$
\[
g(i) - g(-iz^2) \equiv g(i) \pmod{z^2}
\]
\[
f(i) - f(-iz^2) \equiv \frac{i}{2} \pmod{z^2},
\]
and
\[
g((iz)^{-1}) - g(-iz) = -g(iz) - g(-iz)
\]
\[
f((iz)^{-1}) - f(-iz) \equiv \frac{2z}{i} \pmod{z^2}.
\]
Therefore,
\[
w_4([z, i, (iz)^{-1}]) \equiv 2 \cdot \frac{1}{2} \cdot \frac{i}{2} \cdot \frac{2z}{i} \pmod{z^2}
\]
\[
\equiv z \pmod{z^2}.
\]
Therefore, we have \(w_4([z, i, (iz)^{-1}]) = z \prod_{m \geq 1}(1 - q^m)^6\).

5 The main theorem

Combining the results of the previous two sections, we now state our main theorem. In the following statement, we consider \(T_n(E[n])\) as a \(\mu_n\)-torsor via the action of \(\bigwedge^2 V\) on \(T_n(E[n])\) by the identification \(e_n : \bigwedge^2 V \cong \mu_n\) with \(e_n\) the normalized Weil pairing.

Theorem 5.1. Let \(n\) be 3 or 4.

1. The family of maps

\[
(w_n : T_n(E[n]) \longrightarrow \mu_n \sqrt{\Delta_E})_{E/S}
\]

defined in Section 3 with \(E\) an elliptic curve over a scheme \(S\) on which \(n\) is invertible satisfies the following properties:

(a) Each map \(w_n\) is an isomorphism of \(\mu_n\)-torsors over \(S\).

(b) The maps \(w_n\)'s are compatible with arbitrary base change.

(c) If \(E = E_q\) is the Tate curve over \(K = \mathbb{Q}((q))\), then the map \(w_n\) coincides with \(\delta \circ \tau^{-1}\).

(2) If \(n = 3\), then there exists a unique family of maps \((T_3(E[3]) \cong \mu_3 \sqrt{\Delta_E})_{E/S}\) satisfying (a) and (b) with \(E\) an elliptic curve over a scheme \(S\) with 3 invertible. Hence it coincides with \((w_3 : T_3(E[3]) \rightarrow \mu_3 \sqrt{\Delta_E})_{E/S}\) and automatically satisfies the property (c).

(3) If \(n = 4\), then \((w_4)_{E/S}\) and \((-w_4)_{E/S}\) are the only families of maps \(T_n(E[4]) \rightarrow \mu_4 \sqrt{\Delta_E}\) satisfying (a) and (b) with \(E\) an elliptic curve over a scheme \(S\) with 4 invertible. Also, \((w_4)_{E/S}\) is the only family which satisfies the properties (a), (b), and (c).

Proof. (1) Since (b) is obvious from our construction of \(w_n\) and (c) follows from Proposition 4.14, we have only to show (a) for \(w_n\). To do this, we may assume that \(E[n]\) (and hence \(\mu_n\)) is constant over \(S\). Let \(e_n\) be the conjugation

\[
\text{Aut}(T_n(E[n])) \cong \text{Aut}(\mu_n \sqrt{\Delta_E})
\]
by \( w_n \). We consider \( \Lambda^2 E[n] \) as a subgroup of \( \text{Aut}(T_n(E[12])) \) by (3.1) and (3.3). We also consider \( \mu_n \) as a subgroup of \( \text{Aut}(\mu_n \sqrt{\Delta_E}) \) by the canonical action of \( \mu_n \) on \( \mu_n \sqrt{\Delta_E} \). For the proof, we first show the following lemma:

**Lemma 5.2.** (1) The restriction of the map \( c_n \) to \( \Lambda^2 E[n] \) induces an isomorphism \( c'_n : \Lambda^2 E[n] \to \mu_n \).

(2) The isomorphism \( c'_n : \Lambda^2 E[n] \to \mu_n \) is the unique map with which \( w_n \) is compatible.

**Proof.** (1) If \( n = 3 \), then the claim follows from the fact that \( \text{Aut}(T_3(E[3])) \cong \text{Aut}(\mu_3 \sqrt{\Delta_E}) \cong \mathfrak{S}_3 \) has the unique subgroup of order 3; the alternating group.

If \( n = 4 \), by Proposition 3.10, we have \( \Lambda^2 E[4] = C(-1) \subset \text{Aut}(T_4(E[4])) \) and \( \mu_4 = C(-1) \subset \text{Aut}(\mu_4 \sqrt{\Delta_E}) \). Thus, it suffices to check that \( c_4 \) maps \(-1 \in \text{Aut}(T_4(E[4]))\) to \(-1 \in \text{Aut}(\mu_4 \sqrt{\Delta_E})\); that is, \( w_4(-X) = -w_4(X) \) for \( X \in T_4(E[4]) \). This follows from Remark 4.6.

(2) The compatibility is obvious from the definition, and the uniqueness follows because \( \mu_n \to \text{Aut}(\mu_n \sqrt{\Delta_E}) \) is injective.

We continue the proof of the theorem. To show the claim (1), we check that \( e_n = e'_n \).

Denote \( A := \Gamma(Y(n), O) \) and let \( (E_0/A, (P_0, Q_0)) \) be the universal object of \( \mathcal{M}(n) \) (see Theorem 2.4). Then the point \( e'_n(P_0 \land Q_0) \in \mu_n(A) \) defines a morphism \( Y(n) \to \mu_n = \text{Spec}[X, 1/n](X^n - 1) \) of schemes over \( \mathbb{Z}[1/n] \), which we also denote by \( e'_n \). This morphism satisfies the following property: If \( E_0 \) is a field and \( x = (E_0/K, (P, Q)) \in Y(n)(K), \) then \( e'_n(x) = e'_n(P \land Q) \). In the same way, the point \( e_n(P_0 \land Q_0) \in \mu_n(A) \) also defines a morphism \( e_n : Y(n) \to \mu_n \) of schemes over \( \mathbb{Z}[1/n] \), which satisfies \( e_n(x) = e_n(P \land Q) \) for any \( x \) as above.

Since \( Y(n) \) is connected by Theorem 2.6, the morphism \( e_n/e'_n : Y(n) \to \mu_n \) factors through a connected component \( U \) of the scheme \( \mu_n \) over \( \mathbb{Z}[1/n] \).

Corollary 1.13 and Lemma 5.2 (2) imply that \( c_n/e'_n(E_{2^m}, (\zeta_n, z)) = 1 \) for the Tate curve \( E_{2^m}/\mathbb{Q}(\zeta_n)((z)) \). Therefore, \( U \) must be the connected component \( \mu_1 = \text{Spec}[X, 1/n]/(X - 1) \) of \( \mu_n \). This completes the proof of (1).

(2), (3) Suppose that we are given two maps \( W_i : T_n(E[12]) \to \mu_n \sqrt{\Delta_E} \) for each elliptic curve \( E/S \) which satisfy the condition (a) and (b) in the theorem. Then \( W_1/W_2 \) defines a morphism \( W : \mathcal{M} \to \mu_n \) of functors \( \text{Sch}/\mathbb{Z}[1/n] \to \text{Sets} \), where \( \mathcal{M} \) is the functor defined in Theorem 2.6 (1). By Theorem 2.6 (1), there exists a unique morphism \( W' : \mathbb{A}^1_{\mathbb{Z}[1/n]} \to \mu_n \) of schemes over \( \mathbb{Z}[1/n] \) satisfying \( W' \circ j = W : \mathcal{M} \to \mu_n \), where \( j : \mathcal{M} \to \mathbb{A}^1_{\mathbb{Z}[1/n]} \) is given by taking the \( j \) invariant. The morphism \( W' \) corresponds to an element of \( \mu_n(\mathbb{Z}[1/n], j) = 1, \{ \pm 1 \} \) for \( n = 3, 4 \), respectively. This proves the assertions.

**Remark 5.3.** When \( \text{char}(k) \nmid 12 \), we define \( T_{12}(E[12]) = T_3(E[3]) \times T_4(E[4]). \) Then, \( T_{12}(E[12]) \) admits an action of \( \Lambda^2 E[12] \cong \Lambda^2 E[3] \times \Lambda^2 E[4] \), and Theorem 5.1 for \( n = 3, 4 \) immediately gives the analogous result for \( n = 12 \).
6 An isogeny of an elliptic curve and the 12-th roots of its discriminant

The following corollary gives a variant of a Coates’ result [2, appendix]. The original result assumed that the characteristic of the base field is 0.

Corollary 6.1. Let $E$ and $E'$ be elliptic curves over a field $K$ of characteristic $\text{char}(K) \neq 2, 3$, and $\varphi : E \to E'$ be an isogeny over $K$. If $d = \deg \varphi$ is prime to 12, then we have $\Delta_E = (\Delta_{E'})^d$ in $K^\times/(K^\times)^{12}$.

Proof. By Theorem 5.1, we have the following commutative diagram:

$$
\begin{array}{ccc}
\mu_{12} \times \mu_{12} \sqrt[12]{\Delta_E} & \longrightarrow & \mu_{12} \sqrt[12]{\Delta_E} \\
\downarrow e_{12} \times w_{12} & & \downarrow w_{12} \\
\wedge^2 E[12] \times T(E[12]) & \longrightarrow & T(E[12]) \\
\downarrow \wedge^2 \varphi \times T \varphi & & \downarrow T \varphi \\
\wedge^2 E'[12] \times T(E'[12]) & \longrightarrow & T(E'[12]) \\
\downarrow e_{12} \times w_{12}' & & \downarrow w_{12}' \\
\mu_{12} \times \mu_{12} \sqrt[12]{\Delta_{E'}} & \longrightarrow & \mu_{12} \sqrt[12]{\Delta_{E'}} \\
\downarrow (\cdot)^{12} \times (\cdot)^{12} & & \downarrow (\cdot)^{12} \\
\mu_{12} \times \mu_{12} \sqrt[12]{\Delta_{E'}} & \longrightarrow & \mu_{12} \sqrt[12]{\Delta_{E'}}.
\end{array}
$$

Here, $(\cdot)^{12}$ denotes the 12-th power map, and the horizontal maps are the action map. Also, the vertical maps in the above diagram are all bijective and $G_K$-equivariant. Since $e_{12} \circ \wedge^2 \varphi \circ e_{12}^{-1} = (\cdot)^d : \mu_{12} \to \mu_{12}$ (for example, see [8, III, Proposition 8.2]) and $d^2 \equiv 1 \pmod{12}$, the outside rectangle in the above diagram becomes

$$
\begin{array}{ccc}
\mu_{12} \times \mu_{12} \sqrt[12]{\Delta_E} & \longrightarrow & \mu_{12} \sqrt[12]{\Delta_E} \\
\downarrow \sigma \times 1 & & \downarrow (\cdot)^{12} \circ w_{12} \circ T \varphi \circ w_{12}^{-1} \\
\mu_{12} \times \mu_{12} \sqrt[12]{\Delta_{E'}} & \longrightarrow & \mu_{12} \sqrt[12]{\Delta_{E'}}.
\end{array}
$$

This implies that $\mu_{12} \sqrt[12]{\Delta_E}$ and $\mu_{12} \sqrt[12]{\Delta_{E'}}$ are isomorphic as $\mu_{12}$-torsors over $K$. Hence the assertion holds. \qed

References

[1] P.Deligne, M.Rapoport, Les schemas de modules de courbes elliptiques, Modular functions of one variables, II (Proc Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 143-316. Lecture Notes in Math., Vol.349, Springer, Berlin, 1973.

[2] J.Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bulletin of the LMS 23(1991) 321-350.
[3] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Math. studies, Princeton Univ. Press 151 (1994).

[4] S. Lang, H. Trotter, Frobenius Distributions in \( GL_2 \)-Extensions, Lecture Notes in Math. 504 (Springer-Verlag, 1976).

[5] T. Saito, Fermat’s Last Theorem (in Japanese), Iwanami-shoten (2009).

[6] J.-P. Serre, Abelian \( \ell \)-adic representations and Elliptic curves, Benjamin (1968).

[7] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. Invent. Math., 15(1972), 259-331.

[8] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer (1986), 106.