Dyadic Torsion of Elliptic Curves

Jeff Yelton

November 11, 2013

Abstract

Let $k$ be an algebraic extension of $\mathbb{Q}$ which contains all 2-power roots of unity, let $g$ be a positive integer, and let $\alpha_1, \ldots, \alpha_{2g+1}$ be algebraically independent transcendental variables over $k$. Let $K$ be the transcendental extension of $k$ obtained by adjoining the elementary symmetric functions of the $\alpha_i$'s. Let $C$ be the hyperelliptic curve defined over $K$ which is given by the equation $y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i)$, and let $J$ be its Jacobian. Then it is well known that $K(J[2]) = K(\alpha_1, \ldots, \alpha_{2g+1})$. We prove that the image of the action of the absolute Galois group of $K(J[2])$ on the 2-adic Tate module $T_2(J)$ is the full principal congruence subgroup $\Gamma(2) \subseteq \text{Sp}(T_2(J))$.

Now let $g = 1$, and let the elliptic curve $E/K$ be defined by the Weierstrass equation $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

1 Introduction

Let $k$ be an algebraic extension of $\mathbb{Q}$ which contains all 2-power roots of unity. Let $K$ be the transcendental extension of $k$ obtained by adjoining the coefficients of the cubic polynomial $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, where $\alpha_1$, $\alpha_2$, and $\alpha_3$ are independent and transcendental over $k$. Fix an algebraic closure $\overline{K}$ of $K$. Suppose that $E$ is the elliptic curve over $K$ given by the Weierstrass equation

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

(1)

For any integer $n \geq 0$, let $E[2^n]$ be the subgroup of $E(\overline{K})$ of $2^n$-torsion points, and let $K_n$ be the extension of $K$ over which they are defined. (Note that $K_0 = K$.) Further, denote by $E[2^\infty]$ the subgroup of all 2-power torsion points and denote by $K_\infty$ the minimal (algebraic) extension of $K$ over which they are defined.

In this paper, $T_2(E) := \lim_{\leftarrow n} E[2^n]$. 

1
will denote the 2-adic Tate module of $E$; it is a free $\mathbb{Z}_2$-module of rank 2. Let 

$$V_2(E) := T_2(E) \otimes \mathbb{Q}_2.$$  

Then $V_2(E)$ is a 2-dimensional vector space over $\mathbb{Q}_2$ which contains the rank-2 $\mathbb{Z}_2$-lattice $T_2(E)$. Clearly, $\mathbb{Q}_2^2$ acts upon the set of all rank-2 $\mathbb{Z}_2$-lattices in $V_2(E)$ as follows: for any such lattice $\Lambda$ and any $a \in \mathbb{Q}_2^2$, then $a\Lambda := \{a\lambda \mid \lambda \in \Lambda\}$, which is also a rank-2 $\mathbb{Z}_2$-lattice in $V_2(E)$. Now let $\mathcal{L}$ be the set of equivalence classes of such lattices, where two lattices $\Lambda$ and $\Lambda'$ are equivalent if there exists $a \in \mathbb{Q}_2^2$ such that $a\Lambda = \Lambda'$. The equivalence class in $\mathcal{L}$ of a lattice $\Lambda$ will be denoted $[\Lambda]$.

We endow $\mathcal{L}$ with the structure of a graph whose vertices are the elements of $\mathcal{L}$ as follows: two vertices are connected by an edge if they can be written as $[\Lambda]$ and $[\Lambda']$, where $\Lambda \subset \Lambda'$ and $\Lambda'/\Lambda \cong \mathbb{Z}/2\mathbb{Z}$. It is easy to see that this relation is symmetric, so the edge set of this graph is well-defined. It is proven in [9] (Chapter II Section 1) that this graph is in fact a 3-regular tree, known as the Bruhat-Tits tree. We may designate $v_0 := [\Lambda_0]$ as the root, and consider the Bruhat-Tits tree as a rooted tree.

Let $|\mathcal{L}|$ denote the set of vertices of $\mathcal{L}$. Since $\mathcal{L}$ is a tree, one may define the “distance” between two vertices in $|\mathcal{L}|$ to be the number of edges in a simple path connecting them. For any integer $n \geq 0$, let $|\mathcal{L}|_n$ (respectively $|\mathcal{L}|_{\leq n}$) denote the subset of vertices of $\mathcal{L}$ which are of distance $n$ (respectively $\leq n$) from the root $[\Lambda_0]$. The fact that $\mathcal{L}$ is a 3-regular tree implies immediately that each vertex $v \in |\mathcal{L}|_n$, for $n \geq 1$ has exactly one “parent”, that is, a unique vertex $\tilde{v} \in |\mathcal{L}|_{n-1}$ of distance 1 from $v$. Furthermore, each $v \in |\mathcal{L}|_n$ for $n \geq 2$ has a “twin”, that is, a unique lattice $v' \in |\mathcal{L}|_n$ different from $v$ with the same parent as $v$. Note that for any $v \in |\mathcal{L}|_n$ with $n \geq 2$, $v \neq v'$ but $(v')' = v$.

Let $v \in |\mathcal{L}|_1$. Then there is a lattice $\Lambda$ representing $v$ such that $\Lambda > \Lambda_0$ and $\Lambda/\Lambda_0 \cong \mathbb{Z}/2\mathbb{Z}$. There are three such lattices $\Lambda$ which represent the three vertices in $|\mathcal{L}|_1$, all contained in $2\Lambda_0$. Then each such $\Lambda$ can be identified with an order-2 subgroup of $E[2]$ via the induced injection $\Lambda/\Lambda_0 \hookrightarrow \frac{1}{2}\Lambda_0/\Lambda_0$ composed with the obvious isomorphisms $\frac{1}{2}\Lambda_0/\Lambda_0 \cong \Lambda_0/2\Lambda_0 = T_2(E)/2T_2(E) \cong E[2]$. For $i = 1, 2, 3$, we denote by $v_i$ the vertex in $|\mathcal{L}|_1$ corresponding in this way to the order-2 subgroup $\langle (\alpha_i, 0) \rangle$ of $E[2]$. We define the “twin” of $v_i$ to be $v_i' := v_{i+1}$, where $i$ is considered as an element of $\mathbb{Z}/3\mathbb{Z}$.

**Definition 1.1.** A decoration on the Bruhat-Tits tree $\mathcal{L}$ is a map $\Psi : |\mathcal{L}|\setminus\{v_0\} \to \bar{K}$ with the following properties:

a) For any vertex $v \in |\mathcal{L}|\setminus\{v_0\}$, $\Psi(v) \neq \Psi(v')$.

b) For $i \in \mathbb{Z}/3\mathbb{Z}$, $\Psi(v_i) = \alpha_{i+1} - \alpha_{i+2}$.

c) For every $v \in |\mathcal{L}|_2$, $\Psi(v)$ is a root of the quadratic polynomial

$$x^2 - 2(2\Psi((\tilde{v})') + \Psi(\tilde{v}))x + \Psi((\tilde{v})')^2 \in \bar{K}[x],$$

(2)

and for every $v \in |\mathcal{L}|_n$ with $n \geq 3$, $\Psi(v)$ is a root of the quadratic polynomial

$$x^2 - 2(\Psi((\tilde{v})') - 2\Psi(\tilde{v}))x + \Psi((\tilde{v})')^2 \in \bar{K}[x].$$

(3)
Proposition 1.2. A decoration on \( \mathcal{L} \) exists.

Proof. For each \( N \geq 1 \), define \( F_N \) to be the set of all functions \( \Psi : |\mathcal{L}|_{\leq N} \setminus \{v_0\} \) that satisfy the conditions of Definition 1.1 for \( n \leq N \). Clearly, each \( F_N \) is finite, and for each \( N < N' \), there is a map from \( F_N \) to \( F_N' \) by restriction, so it will suffice to show that each \( F_N \) is nonempty. By definition, \( F_1 \) is nonempty, and one can explicitly show that \( F_2 \) is nonempty and that any function \( \Psi \in F_2 \) takes nonzero values in \( \bar{K} \). Now we prove inductively that \( F_N \) is nonempty for \( N \geq 3 \) by showing that for each \( N \geq 2 \) and function \( \Psi_N \in F_N \), there is a function \( \Psi_{N+1} \in F_{N+1} \) restricting to \( \Psi_N \). This amounts to showing that for each \( v \in |\mathcal{L}|_n \) with \( n \geq 2 \), the polynomial \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \) has two distinct roots in \( \bar{K} \). It is clear from part (b) of the definition and a little computation that for \( v \in |\mathcal{L}|_2 \), the polynomial \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \) has two distinct, nonzero roots in \( \bar{K} \). Now assume inductively that this claim holds for all \( v \in |\mathcal{L}|_{n-1} \) for some \( n \geq 3 \). Let \( v \in |\mathcal{L}|_n \). If 0 were a root of \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \), then the constant coefficient \( (\Psi(v'))^2 \) would be 0. But \( \Psi(v') \) is a root of the polynomial \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \), which by the inductive assumption, has nonzero roots. Thus, the polynomial \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \) has nonzero roots. Now suppose that its roots are equal. Then its discriminant \( 4(\Psi(v'))^2 - 4(\Psi(v'))^2 = 16\Psi(v)(\Psi(v)-\Psi(v')) \) is 0, implying that either \( \Psi(v) = 0 \) or \( \Psi(v) = \Psi(v') \). But \( \Psi(v) \) and \( \Psi(v') \) are the two roots of the polynomial \( x^2 - 2(\Psi(v')) x + \Psi(v')^2 \), and by the inductive assumption, they are distinct and nonzero, so we have a contradiction. 

Now we may state the main theorem.

Theorem 1.3. Let an elliptic curve \( E/K \) be defined as above, with Weierstrass roots \( \alpha_1, \alpha_2, \) and \( \alpha_3 \). Define the Bruhat-Tits tree \( \mathcal{L} \) associated with this elliptic curve as above, and let \( \Psi \) be a decoration on \( \mathcal{L} \). Set

\[
K'_\infty := K(\{\Psi(v)\}_{v \in |\mathcal{L}|_{\leq N} \setminus \{v_0\}}).
\]

a) Choose \( i, j \in \{1, 2, 3\} \) with \( i \neq j \), and choose an element \( \sqrt{\alpha_i - \alpha_j} \in \bar{K} \) whose square is \( \alpha_i - \alpha_j \). Then we have

\[
K_\infty = K'_\infty(\sqrt{\alpha_i - \alpha_j}).
\]

b) The Galois group of \( K_\infty/K \) is isomorphic to \( SL_2(\mathbb{Z}_2) \), while the subgroup fixing \( K(\alpha_1, \alpha_2, \alpha_3) \) is isomorphic to the congruence subgroup \( \Gamma(2) < SL_2(\mathbb{Z}_2) \). Moreover, the Galois automorphism corresponding to the scalar matrix \( -1 \in \Gamma(2) \) acts on \( K_\infty \) by fixing \( K'_\infty \) and sending \( \sqrt{\alpha_i - \alpha_j} \) to \( -\sqrt{\alpha_i - \alpha_j} \) for \( 1 \leq i, j \leq 3 \), \( i \neq j \).

In Section 2, we will study families of hyperelliptic curves of odd degree \( 2g+1 \) parametrized by their sets of Weierstrass roots. (Note that an elliptic curve will be considered to be simply a hyperelliptic curve of genus 1.) In this context, the extensions of \( K(\alpha_1, \alpha_2, \alpha_3) \) over which \( E[2^n] \) is defined for \( n = 1, 2, 3, \ldots \)
will be viewed as function fields of covers of the configuration space of sets of Weierstrass roots. This will enable us to argue that \( \text{Gal}(K_\infty/K(\alpha_1, \alpha_2, \alpha_3)) \) is isomorphic to the level 2 congruence subgroup of \( \text{SL}_2(\mathbb{Z}_2) \). Then, in Section 3, we will construct \( K_\infty' \) as a compositum of fields of definition of certain elliptic curves that have a 2-power isogeny to \( E \). It will be shown that \( K_\infty \) is only a quadratic extension of \( K_\infty' \), which will lead to a proof of the above theorem. We will obtain additional results (Corollary 3.10 and Theorem 3.11) which relate each \( K_n \) with \( K_n' \) and with the field generated by the \( x \)-coordinates of the points in \( E[2^n] \).

We fix the following notation. Let \( R \) be a commutative ring with unity (such as \( \mathbb{Z}_2 \)), and let \( G \) be a multiplicative group of (invertible) matrices over \( R \). If \( 2 \) is not invertible in \( R \), for any integer \( n \geq 0 \), we will denote by 
\[
\Gamma(2^n) := \{ g \in G \mid g \equiv 1 \mod 2^n \} \triangleleft G
\]
the level \( 2^n \) congruence subgroup of \( G \). It will be clear from context which matrix group has \( \Gamma(2^n) \) as a subgroup. In some cases, for a free module \( M \) over \( R \), without specifying a basis for \( M \), we will write \( \Gamma(2^n) \triangleleft \text{Aut}(M) \) for the subgroup of automorphisms of \( M \) which act trivially on the quotient module \( M/2^n M \).

2 Families of Hyperelliptic Jacobians

Fix a positive integer \( g \). An affine model for an affine hyperelliptic curve over \( \mathbb{C} \) of genus \( g \) may be given by
\[
y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i), \tag{4}
\]
with \( \alpha_i \)'s distinct complex numbers. Now let \( \alpha_1, ..., \alpha_{2g+1} \) be independent transcendental variables, and let \( L \) be the subfield of \( \mathbb{C}(\alpha) := \mathbb{C}(\alpha_1, ..., \alpha_{2g+1}) \) generated over \( \mathbb{C} \) by the elementary symmetric functions of the \( \alpha_i \)'s. For each \( n \geq 0 \), let \( L_n \) denote the extension of \( L \) over which the \( 2^n \)-torsion of \( J \) is defined, and let
\[
L_\infty := \bigcup_{n=1}^{\infty} L_n.
\]
Note that \( \mathbb{C}(\alpha_1, ..., \alpha_{2g+1}) \) is Galois over \( L \) with Galois group isomorphic to \( S_{2g+1} \). It is well known (5, Corollary 2.11) that \( \mathbb{C}(\alpha_1, ..., \alpha_{2g+1}) = L_1 \), so \( \text{Gal}(L_1/L) \cong S_{2g+1} \). Fix an algebraic closure \( \bar{L} \) of \( L \), and write \( G_L \) for the absolute Galois group \( \text{Gal}(\bar{L}/L) \).

Let \( C \) be the curve defined over \( L \) by equation (4), and let \( J/L \) be its Jacobian. Write \( \text{SL}(T_2(J)) \) (resp. \( \text{Sp}(T_2(J)) \)) for the subgroup of automorphisms of the 2-adic Tate module \( T_2(J) \) with determinant 1 (resp. automorphisms of \( T_2(J) \) which preserve the Weil pairing). The main theorem of this section is the following.
Theorem 2.1. Let $\rho_2 : G_L \rightarrow \text{Sp}(T_2(J))$ be the continuous homomorphism induced by the natural Galois action on the 2-adic Tate module of $J$. Then the image under $\rho_2$ of the Galois subgroup fixing $L_1$ is the principal congruence subgroup $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$.

Before setting out to prove this theorem, we state some easy corollaries.

Corollary 2.2. Let $G$ denote the image under $\rho_2$ of all of $G_L$. Then we have the following:

a) $G$ contains $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$, and $G/\Gamma(2) \cong S_{2g+1}$.

b) In the case that $g = 1$, $G = \text{Sp}(T_2(J)) = \text{SL}(T_2(J))$.

c) For each $n \geq 1$, the homomorphism $\rho_2$ induces an isomorphism

$$\tilde{\rho}_2^{(n)} : \text{Gal}(L_n/L_1) \sim \rightarrow \text{Gal}(\tilde{L}/L_2).$$

via the restriction map $\text{Gal}(\tilde{L}/L_2) \rightarrow \text{Gal}(L_n/L_1)$.

Proof. Since $\text{Gal}(L(2)/L) \cong S_{2g+1}$, part (a) immediately follows from the theorem. If $g = 1$, then fix a basis of $T_2(J)$ so that we may identify $\text{Sp}(T_2(J))$ (resp. $\text{SL}(T_2(J))$) with $\text{Sp}(Z_2)$ (resp. $\text{SL}(Z_2)$). Then it is well known that $\text{Sp}(Z_2) = \text{SL}(Z_2)$, and that $\text{SL}(Z_2)/\Gamma(2) \cong \text{SL}(Z/2Z) \cong S_3$. Since, by part (a), $G/\Gamma(2) \cong S_3$ when $g = 1$, the linear subgroup $G$ must be all of $\text{Sp}(T_2(J)) = \text{SL}(T_2(J))$, which is the statement of (b). To prove part (c), note that for any $n \geq 0$, the image under $\rho_2$ of the Galois subgroup fixing the $2^n$-torsion points is clearly $G \cap \Gamma(2^n)$. But $G > \Gamma(2)$, so for any $n \geq 1$, the image under $\rho_2$ of $\text{Gal}(\tilde{L}/L(2^n))$ is $\Gamma(2^n)$. Then part (c) immediately follows by the definition of $\tilde{\rho}_2^{(n)}$.

In order to prove Theorem 2.1 we study a family of hyperelliptic curves parametrized by all (unordered) subsets $T = \{\alpha_i\} \subset \mathbb{C}$ of cardinality $2g + 1$ whose generic fiber is $C$. Let $e_1(\alpha), e_2(\alpha), \ldots, e_{2g+1}(\alpha)$ be the elementary symmetric functions of the variables $\alpha_i$, and let $\Delta(\alpha)$ be the discriminant function of these variables. Then the base of this family is the affine variety over $\mathbb{C}$ given by

$$X := \text{Spec}(\mathbb{C}[e_1(\alpha), e_2(\alpha), \ldots, e_{2g+1}(\alpha), \Delta(\alpha)^{-1}]).$$

(5)

This complex affine scheme may be viewed as the configuration space of subsets of cardinality $2g + 1$ of $\mathbb{C}$ (see the discussion in Section 6 of [12]). Thus, we consider each point $T \in X(\mathbb{C})$ to be a subset of $\mathbb{C}$ of cardinality $2g + 1$. The (topological) fundamental group of $X$ is $\pi_1(X) \cong B_{2g+1}$, the braid group on $2g + 1$ strands. Note that the function field of $X$ is $L$.

We also define the complex affine scheme

$$Y := \text{Spec}(\mathbb{C}[\alpha_1, \alpha_2, \ldots, \alpha_{2g+1}, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq 2g+1}]).$$

(6)

As a complex manifold, $Y$ is the ordered configuration space of ordered subset of $\mathbb{C}$ of cardinality $2g + 1$, whose points may be identified with ordered subsets.
of \( \mathbb{C} \) of cardinality \( 2g + 1 \). The (topological) fundamental group of \( Y \) is \( \pi_1(Y) \cong P_{2g+1} \triangleleft B_{2g+1} \), the pure braid group on \( 2g + 1 \) strands.

Now denote by \( C \to X \) the family whose fiber at any point \( T \in X \) is the hyperelliptic curve over \( \mathbb{C} \) defined by the equation

\[
y^2 = \prod_{z \in T} (x - z).
\]

(7)

Clearly, \( C/L \) is the generic fiber of \( C \). Fix a basepoint \( T_0 \) of \( X \), and a basepoint \( P_0 \) of \( C_{T_0} \). Then we have a short exact sequence of fundamental groups

\[
1 \to \pi_1(C_{T_0}, P_0) \to \pi_1(C, P_0) \to \pi_1(X, T_0) \to 1.
\]

(8)

We may define a continuous section \( s : X \to C \) as in [12], Lemma 6.1. This section defines the monodromy action of \( \pi_1(X) \cong B_{2g+1} \) on \( \pi_1(C_{T_0}) \), given by \( \sigma \in \pi_1(X) \) acting as conjugation by \( s(\sigma) \) on \( \pi_1(C_{T_0}) \). This induces an action of \( B_{2g+1} \) on the abelianization of \( \pi_1(C_{T_0}) \), the homology group \( H_1(C_{T_0}, \mathbb{Z}) \), which is isomorphic to \( \mathbb{Z}^{2g} \). We denote this action by \( R : B_{2g+1} \to \text{Aut}(H_1(C_{T_0}, \mathbb{Z})) \).

(9)

This action respects the intersection pairing on \( C_T \), so the image of \( R \) is actually contained in the subgroup of symplectic automorphisms \( \text{Sp}(H_1(C_T, \mathbb{Z})) \).

The following theorem is proven in [1] (Théorème 1), as well as in [5] (Lemma 8.12).

**Theorem 2.3.** In the representation \( R : B_{2g+1} \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) \), the image of \( P_{2g+1} \) is exactly \( \Gamma(2) \).

We are now ready to prove the main theorem of this section.

**Proof (of Theorem 2.1).** We proceed in five steps.

**Step 1:** We switch from the affine curve \( C \) to a smooth compactification of \( C \), which is defined as follows. Let \( C' \) be the (smooth) curve defined over \( L \) by the equation

\[
y'^2 = x'^{2g+1} \prod_{i=1}^{2g+1} (1 - \alpha_i x').
\]

(10)

We glue the open subset of \( C \) defined by \( x \neq 0 \) to the open subset of \( C' \) defined by \( x' \neq 0 \) via the mapping

\[
x' \mapsto \frac{1}{x}, \quad y' \mapsto \frac{y}{x^{2g+1}},
\]

and denote the resulting smooth, projective scheme by \( \bar{C} \). Let \( \infty \in \bar{C}(L) \) denote the “point at infinity” given by \( (x', y') = (0, 0) \in C' \). The curve \( \bar{C} \) has smooth reduction over every point \( T \in X \) and therefore can be extended in an obvious way to a family \( \bar{C} \to X \) whose generic fiber is \( \overline{C/L} \). Note that \( \bar{C}_T \) is a smooth compactification of \( C_T \) for each \( T \in X \). There is a surjective
map \( \pi_1(C_{T_0}, P_0) \to \pi_1(\bar{C}_{T_0}, \infty_{T_0}) \) induced by the inclusion \( C \to \bar{C} \). Note also that the section \( s : X \to \bar{C} \subset C \) can be continuously deformed to the “constant section” \( \bar{s} : X \to \bar{C} \) sending each \( T \in X \) to the point at infinity \( \infty_T \in C_T \). Therefore, \( \bar{s}_* : \pi_1(X, T_0) \to \pi_1(\bar{C}_{T_0}, \infty_{T_0}) \) is the composition of \( s_* \) with the map \( \pi_1(C_T) \to \pi_1(\bar{C}_T) \). In this way, we may view the action of \( \pi_1(X, T_0) \) on \( \pi_1(\bar{C}_{T_0}, P_0)^{ab} = \pi_1(\bar{C}_{T_0}, \infty_{T_0})^{ab} \) as being induced by \( \bar{s}_* \).

**Step 2:** We switch from (topological) fundamental groups to étale fundamental groups. Since \( X \) and \( \bar{C} \), as well as \( C_T \) for each \( T \in X \), can be viewed as a scheme over the complex numbers, Riemann’s Existence Theorem implies that the étale fundamental groups of \( X, \bar{C}, \) and each \( C_T \) (defined using a choice of geometric base point \( T_0 \) over \( T_0 \)) are isomorphic to the profinite completions of their respective topological fundamental groups. Taking profinite completions induces a sequence of étale fundamental groups

\[
1 \to \pi_1^{et}(\mathcal{J}_{T_0}, 0_{T_0}) \to \pi_1^{et}(\mathcal{J}, 0_{T_0}) \to \pi_1^{et}(X, T_0) \to 1,
\]

which is a short exact sequence by \([4], \text{Corollaire X.2.2}\). Moreover, the section \( \bar{s} : X \to \bar{C} \) similarly gives rise to an action of \( \pi_1^{et}(X, T_0) \) on \( \pi_1^{et}(\bar{C}_{T_0}, \infty_{T_0})^{ab} \).

**Step 3:** We switch from \( \bar{C} \) to its Jacobian. Define \( \mathcal{J} \to X \) to be the family of abelian varieties such that \( \mathcal{J}_T \) is the Jacobian of \( C_T \) for each \( T \in X \). Then the generic fiber of \( \mathcal{J} \) is \( J/L \), the Jacobian of \( C/L \). Let \( f_\infty : \bar{C} \to J \) be the morphism (defined over \( L \)) given by sending each point \( P \in \Omega(C/L) \) to the divisor class \( [(P) - (\infty)] \) in \( Pic^0_0(\bar{C}) \), which is identified with \( J(L) \). By \([3] \) (“Jacobian Varieties”, Proposition 9.1), the induced homomorphism of étale fundamental groups \( f_\infty_* : \pi_1^{et}(\bar{C}, \infty) \to \pi_1^{et}(J, 0) \) factors through an isomorphism \( \pi_1^{et}(\bar{C}, \infty)^{ab} \cong \pi_1^{et}(J, 0) \). This induces an isomorphism \( \pi_1^{et}(C_T, \infty_T)^{ab} \cong \pi_1^{et}(\mathcal{J}_T, 0_T) \) for each \( T \in X \). Note that the composition of the section \( \bar{s} : X \to \bar{C} \) with \( f_\infty \) is the “zero section” \( o : X \to \mathcal{J} \) mapping each \( T \) to the identity element \( 0_T \in \mathcal{J}_T \). Thus, the action of \( \pi_1^{et}(X, T_0) \) on \( \pi_1^{et}(\bar{C}_{T_0}, \infty_{T_0})^{ab} \) coming from the splitting of \([9]\) is the same as the action of \( \pi_1^{et}(X, T_0) \) on \( \pi_1^{et}(\mathcal{J}_{T_0}, 0_{T_0}) \) coming from the splitting of \([11]\) induced by the section \( o_* : \pi_1^{et}(X, T_0) \to \pi_1^{et}(\mathcal{J}, 0_{T_0}) \).

**Step 4:** We now want to show that this action can be viewed as a Galois action on \( \pi_1^{et}(J_L, 0) \) (and therefore on its \( \ell \)-adic quotient \( T_\ell(J) \)). Let \( J_L = \text{Spec}(L) \to X \) denote the generic point of \( X \). Note that we may identify \( \pi_1^{et}(L, \bar{L}) \) with \( G_L \), and that \( \eta : G_L \to \pi_1^{et}(X, \bar{\eta}) \) is a surjection (in fact, it is the restriction homomorphism of Galois groups corresponding to the maximal algebraic extension of \( L \) unramified at all points of \( X \)). Also, the point \( 0 \in J_L \) may be viewed as a morphism \( 0 : \text{Spec}(L) \to J_L \) which induces \( 0_* : G_L = \pi_1^{et}(L, \bar{L}) \to \pi_1^{et}(J_L, 0) \). Let \( T_0 \) and \( \bar{\eta} \) be geometric points over \( T_0 \) and \( \eta \) respectively. Then we have \([4], \text{Corollaire X.1.4}\) an exact sequence of étale fundamental groups

\[
\pi_1^{et}(\mathcal{J}, 0_{\eta}) \to \pi_1^{et}(\mathcal{J}, 0_{\bar{\eta}}) \to \pi_1^{et}(X, \bar{\eta}) \to 1.
\]

Changing the geometric basepoint of \( X \) from \( T_0 \) to \( \bar{\eta} \) (resp. changing the geometric basepoint of \( \mathcal{J} \) from \( 0_\eta \) to \( 0_{\bar{\eta}} \)) non-canonically induces an isomorphism \( \pi_1^{et}(X, \bar{\eta}) \cong \pi_1^{et}(X, T_0) \) (resp. an isomorphism \( \pi_1^{et}(\mathcal{J}, 0_{\bar{\eta}}) \cong \pi_1^{et}(\mathcal{J}, 0_{T_0}) \)). Fix
such an isomorphism $\varphi : \pi_1^\et(X, \eta) \xrightarrow{\sim} \pi_1^\et(X, \bar{T}_0)$. Then we have the following commutative diagram, where all horizontal rows are exact:

\[
\begin{array}{cccccc}
1 & \xrightarrow{} & \pi_1^\et(J_L, 0) & \xrightarrow{} & \pi_1^\et(J_L, 0) & \xrightarrow{} & \pi_1(L, \bar{L}) & \xrightarrow{} & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\pi_1^\et(J_{\eta}, 0_{\eta}) & \xrightarrow{\sigma^*} & \pi_1^\et(J, 0_{\eta}) & \xrightarrow{\sigma^*} & \pi_1^\et(X, \bar{\eta}) & \xrightarrow{\sigma^*} & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \xrightarrow{\text{sp}} & \pi_1^\et(J_{\bar{T}_0}, 0_{\bar{T}_0}) & \xrightarrow{\sigma^*} & \pi_1^\et(J, 0_{\bar{T}_0}) & \xrightarrow{\sigma^*} & \pi_1^\et(X, \bar{T}_0) & \xrightarrow{\sigma^*} & 1
\end{array}
\]

Here the vertical arrow from $\pi_1^\et(J, 0_{\eta})$ to $\pi_1^\et(J, 0_{\bar{T}_0})$ is a change-of-basepoint isomorphism chosen to make the lower right square commute, and $\text{sp} : \pi_1^\et(J_{\bar{T}_0}, 0_{\bar{T}_0}) \rightarrow \pi_1^\et(J_{\bar{T}_0}, 0_{\bar{T}_0})$ is the surjective homomorphism induced by a diagram chase on the bottom two horizontal rows. Grothendieck’s Specialization Theorem ([1], Corollaire X.3.9) states that $\text{sp}$ is an isomorphism, which implies that the second row is also a short exact sequence. Thus, the image of the action of $\pi_1^\et(X, \bar{T}_0)$ on $\pi_1^\et(J_{\bar{T}_0}, 0_{\bar{T}_0})$ arising from the splitting of the lower row by $\sigma^*$ is identified with the image of the action of $\pi_1^\et(X, \bar{T}_0)$ on $\pi_1^\et(J_{\bar{T}_0}, 0_{\bar{T}_0})$ arising from the splitting of the middle row by $\sigma^*$. In turn, a simple diagram chase confirms that this may be identified with the image of the action of $\pi_1^\et(L, \bar{L})$ on $\pi_1^\et(J_L, 0)$ arising from the splitting of the top row by $\sigma^*$. So, by abuse of notation, we may write $R : G_L = \pi_1^\et(L, \bar{L}) \rightarrow \text{Aut}(\pi_1^\et(J_L, 0))$. Since for any prime $\ell$, the Tate module $T_\ell(J)$ may be identified with the maximal pro-$\ell$ quotient of $\pi_1^\et(J_L, 0)$, $R$ induces an action of $G_L$ on $T_\ell(J)$, which we denote by $R_\ell : G_L \rightarrow \text{Aut}(T_\ell(J))$. One can identify the symplectic pairing on $\pi_1(J_{\bar{T}_0}, 0_{\bar{T}_0})$ with the Weil pairing on $T_\ell(J)$ via the results in [1], Chapter IV, §24. Therefore, the image of $R_\ell$ is a subgroup of $\text{Sp}(T_\ell(J))$.

Note that $P_{2g+1}$ is the normal subgroup of $B_{2g+1} \cong \pi_1(X, T_0)$ corresponding to the cover $Y \rightarrow X$, and the function field of $Y$ is $C(\alpha_1, \ldots, \alpha_{2g+1}) = L(2)$, so the image of $\text{Gal}(L/L(2))$ under $\eta_1$ is $P_{2g+1} \triangleleft B_{2g+1} \cong \pi_1^\et(X, T_0)$. Therefore, the statement of Theorem 2.3 implies that the image of $\text{Gal}(L/L(2))$ under $R_2$ is $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$.

Step 5: We show that $R_\ell = \rho_\ell$, from which the statement of the theorem will follow by taking $\ell = 2$. To determine $R_\ell$, we are interested in the action of $G_L$ on the group $\text{Aut}_{J_L}(Z)$ for each $\ell$-power-degree covering $Z \rightarrow J_L$. But each such covering is a subcovering of $[\ell^n] : J_L \rightarrow J_L$, so it suffices to determine the action of $G_L$ on the group of translations $\{t_P|P \in J[\ell^n]\}$ for each $n$. Recall that $0_\ast : G_L \rightarrow \pi_1^\et(J_L, 0)$ is induced by the inclusion of the $L$-point $0 \in J_L$. Thus, for any $\sigma \in G_L$, $0_\ast(\sigma)$ acts on any connected étale cover of $J_L$ via $\sigma$ acting on the coordinates of the points. Since $R(\sigma)$ is conjugation by $0_\ast(\sigma)$ on $\pi_1^\et(J_L, 0)$, one sees that for each $n$, $0_\ast(\sigma)$ acts on $\{t_P|P \in J[\ell^n]\}$ by sending each $t_P$ to $\sigma^{-1}t_P\sigma = t_{P'\ast}$. Thus, $G_L$ acts on the Galois group of the
covering \([\ell^n] : J_L \to J_L\) via the usual Galois action on \(J[\ell^n]\). This lifts to the usual action of \(G_L\) on \(T_\ell(J)\), and we are done.

One application of Theorem 2.1 is that it allows us to obtain an explicit description of \(L_2\). We will follow Yu’s argument in [12].

**Proposition 2.4.** We have

\[
L_2 = L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i < j \leq 2g+1}).
\]

**Proof.** For \(n \geq 1\), let \(B_n\) denote the set of bases of the free \(\mathbb{Z}/2^n\mathbb{Z}\)-module \(\mathcal{J}_{T_0}[2^n]\). Then it was shown in the proof of Theorem 2.1 that \(G_L\) acts on \(B_n\) through the map \(R : \pi_1(X, T_0) \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) = \text{Sp}(H_1(\mathcal{J}_{T_0}, \mathbb{Z}))\) in the statement of Theorem 2.3 and the subgroup fixing all elements of \(B_n\) corresponds to \(R^{-1}(\Gamma(2^n)) \triangleleft \pi_1(X, T_0)\). Hence, by covering space theory, there is a connected cover \(X_n \to X\) corresponding to an orbit of \(B_n\) under the action of \(\pi_1(X, T_0)\), and the function field of \(X_n\) is the extension of \(L\) fixed by the subgroup of \(G_L\) which fixes all bases of \(J[2^n]\). Clearly, this extension is \(L_n\). Thus, the Galois cover \(X_n \to X\) is an unramified morphism of connected affine schemes corresponding to the inclusion \(L \to L_n\) of function fields.

Note that, setting \(n = 1\), we get that \(X_1\) is the Galois cover of \(X\) whose étale fundamental group can be identified with \(R^{-1}(\Gamma(2))\). Theorem 2.3 implies that \(R^{-1}(\Gamma(2))\) is isomorphic to \(\hat{P}_{2g+1}\), the profinite completion of \(P_{2g+1}\). For \(n \geq 1\), the étale morphism \(X_n \to X_1\) corresponds to the function field extension \(L_n \supset L_1\), which by Corollary 2.2(c) has Galois group isomorphic to \(\Gamma(2)/\Gamma(2^n)\). Therefore, \(X_n\) is the cover of \(X_1\) whose étale fundamental group can be identified with a normal subgroup of \(\hat{P}_{2g+1}\) with quotient isomorphic to \(\Gamma(2)/\Gamma(2^n)\).

In the proof of Corollary 2.2 of [8], it is shown that \(\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}\), and thus,

\[
\text{Gal}(L_2/L_1) \cong \Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}.\tag{13}
\]

It is also clear from looking at a presentation of the pure braid group \(P_{2g+1}\) (see for instance [2], Lemma 1.8.2) that the abelianization of \(P_{2g+1}\) is a free abelian group of rank \(2g^2 + g\). Therefore, its maximal abelian quotient of exponent 2 is isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2g^2+g}\). Thus, \(\hat{P}_{2g+1}\) has a unique normal subgroup inducing a quotient isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2g^2+g}\). It follows that there is only one Galois cover of \(X_1\) with Galois group isomorphic to \(\Gamma(2)/\Gamma(4)\), namely \(X_2\). The field extension \(L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{i < j}) \supset L_1\) is unramified except over primes of the form \((\alpha_i - \alpha_j)\) with \(i \neq j\) and is obtained from \(L_1\) by adjoining \(2g^2 + g\) independent square roots of elements in \(L_1^2\). Therefore, \(L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{i < j})\) is the function field of a Galois cover of \(X(2)\) with Galois group isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2g^2+g} \cong \Gamma(2)/\Gamma(4)\). It follows that this cover of \(X_1\) is \(X_2\), and that \(L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{i < j})\) is \(L_2\), the function field of \(X_2\).
As in Section 1, let \( k \) be an algebraic extension of \( \mathbb{Q} \) which contains all 2-power roots of unity, and let \( K \) be the transcendental extension obtained by adjoining the coefficients of (4) to \( k \). We will also fix the following notation. Let \( C_k \) be the hyperelliptic curve defined over \( K \) given by the equation (4), and let \( J_K \) be its Jacobian. For each \( n \geq 0 \), let \( K_n \) be the extension of \( K \) over which the \( 2^n \)-torsion of \( J_K \) is defined. Note that, analogous to the situation with \( C/L \), the extension \( K_2 \) is \( k(\alpha_1, \ldots, \alpha_{2g+1}) \), which is Galois over \( K \) with Galois group isomorphic to \( S_{2g+1} \). Let \( \rho_{2,K} : \text{Gal}(K_\infty/K) \to \text{Sp}(T_2(J_K)) \) be the homomorphism arising from the Galois action on the Tate module of \( J_K \).

We now investigate what happens to the Galois action when we descend from working over \( \mathbb{C} \) to working over \( k \).

**Proposition 2.5.** The statements of Theorem [2.1], Corollary [2.2], and Proposition [2.4] are true when \( L \) and \( p_2 \) are replaced by \( K \) and \( \rho_{2,K} \) respectively.

**Proof.** For any \( n \geq 0 \), let \( \theta_n : \text{Gal}(L_\infty/L_n) \to \text{Gal}(K_\infty/K_n) \) be the composition of the obvious inclusion \( \text{Gal}(L_\infty/L_n) \hookrightarrow \text{Gal}(L_\infty/K_n) \) with the obvious restriction map \( \text{Gal}(L_\infty/K_n) \to \text{Gal}(K_\infty/K_n) \). Let \( \tilde{\rho}_2(\infty) \) (resp. \( \tilde{\rho}_{2,K}(\infty) \)) be the representation of \( \text{Gal}(L_\infty/L) \) (resp. \( \text{Gal}(K_\infty/K) \)) induced from \( \rho_2 \) (resp. \( \rho_{2,K} \)) by the restriction homomorphism of the Galois groups. It is easy to check that \( \rho^{(\infty)} = \tilde{\rho}_{2,K}(\infty) \circ \theta_0 \). It will suffice to show that \( \theta_0 \) is an isomorphism.

Fix \( n \geq 0 \). First, observe that \( L_\infty = K_\infty \mathbb{C} \) and \( L_n = K_n \mathbb{C} \), and that therefore, \( K_\infty L(2^n) = K_\infty \mathbb{C} = L_\infty \). Choose any \( \sigma \in \text{Gal}(L_\infty/L_n) \) such that \( \theta_n(\sigma) \) acts trivially on \( K_\infty \). Then \( \sigma \) acts trivially on \( K_\infty \) as well as on \( L_n \), so it acts trivially on their compositum \( K_\infty L_n = L_\infty \). Thus, \( \theta_n \) is injective.

Now suppose that \( n \geq 1 \). Then, as in the proof of [2.2] the image under \( \tilde{\rho} \) of \( \text{Gal}(L_\infty/L_n) \) is the entire congruence subgroup \( \Gamma(2^n) \). Therefore, since \( \theta_n \) is injective, the image under \( \tilde{\rho}_K \) of \( \text{Gal}(K_\infty/K_n) \) contains \( \Gamma(2^n) \). But since \( K \) contains all 2-power roots of unity, the Weil pairing is Galois invariant, and so the image of \( \text{Gal}(K_\infty/K_n) \) must also be contained in \( \Gamma(2^n) \). Therefore, \( \theta_n \) is an isomorphism for \( n \geq 1 \). Now, using [2.2]a and the fact that \( \text{Gal}(K(\alpha_1, \ldots, \alpha_{2g+1})/K) \cong S_{2g+1} \), we get the commutative diagram below, whose top and bottom rows are short exact sequences.

\[
\begin{array}{cccccc}
1 & \longrightarrow & \text{Gal}(L_\infty/L_1) & \longrightarrow & \text{Gal}(L_\infty/L) & \longrightarrow & S_{2g+1} & \longrightarrow & 1 \\
& & \downarrow \theta_1 & & \downarrow \theta_0 & & \\
1 & \longrightarrow & \text{Gal}(K_\infty/K_1) & \longrightarrow & \text{Gal}(K_\infty/K) & \longrightarrow & S_{2g+1} & \longrightarrow & 1
\end{array}
\]

By the Short Five Lemma, since \( \theta_1 \) is an isomorphism, so is \( \theta_0 \).

**Remark 2.6.** a) Suppose we drop the assumption that \( k \) contains all 2-power roots of unity. Then \( \rho_{2,K}(G_K) \) is no longer contained in \( \text{Sp}(T_2(J)) \) in general. However, the Galois equivariance of the Weil pairing forces the image of \( \rho_{2,K} \) to be contained in the group of symplectic similitudes

\[
\text{GSp}(T_2(J)) := \{ \sigma \in \text{Aut}(T_2(J)) \mid e_2(P^n, Q^n) = \chi_2(\sigma)e_2(P, Q) \ \forall P, Q \in T_2(J) \},
\]

10
where \( e_2 : T_2(J) \times T_2(J) \to \lim_{\kappa} \mu_2^\infty \cong \mathbb{Z}_2 \) is the Weil pairing on the 2-adic Tate module of \( J \), and \( \chi_2 : G_K \to \mathbb{Z}_2^\times \) is the cyclotomic character on the absolute Galois group of \( K \). Galois equivariance of the Weil pairing also implies that \( K_\infty \) contains all 2-power roots of unity. Thus, \( K_\infty \supset K(\mu_2^\infty) \), and the statements referred to in Proposition 2.5 still hold when we replace \( K \) with \( K(\mu_2^\infty) \).

b) In addition, suppose that \( k \) is a number field. We may specialize by identifying each coefficient of the degree-2\( g+1 \) polynomial in \([4]\) with an element of \( k \), and defining the corresponding Jacobian \( J_k/k \) and Galois representation \( \rho_{2,k} : G_k \to \text{Sp}(T_2(J_k)) \). Then we may use Proposition 1.3 of \([7]\) and its proof (see also \([10]\)) to see that for infinitely many choices of \( e_1(\alpha), \ldots, e_{2g+1}(\alpha) \in k \), \( \rho_{2,k}(G_k) \) can be identified with \( \rho_{2,k}(G_k) \) from part (a). We have \( \rho_{2,k}(\text{Gal}(k/k(\mu_2^\infty))) = \rho_{2,k}(G_k) \cap \text{Sp}(T_2(J_k)) \), and therefore, the statements referred to in Proposition 2.5 still hold over \( k(\mu_2^\infty) \).

## 3 Results on elliptic curves via 2-isogenies

The main goal of this section is to prove Theorem 1.3. We resume the notation used in Section 1: let \( k \) be an algebraic extension of \( \mathbb{Q} \) which contains all 2-power roots of unity, let \( \alpha_1, \alpha_2, \alpha_3 \) be (independent) transcendental variables over \( k \), and let \( K \) be obtained by adjoining the elementary symmetric functions of the \( \alpha_i \)'s to \( k \). Let \( E \) be the elliptic curve defined over \( K \) with Weierstrass equation

\[
y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).
\]

Define \( E[2^n] \) and \( K_n \) for \( n \geq 0 \) as in Section 1. Clearly, \( K_0 = K \) and \( K_1 = K(\alpha_1, \alpha_2, \alpha_3) \).

We will often use “<” and “>” to indicate inclusion of \( \mathbb{Z}_2 \)-lattices inside \( V_2(E) \), or to indicate inclusion of subgroups of \( E[K] \).

We now want to set up, for any \( n \geq 1 \), a bijection between \( |L|_n \) and the set of all cyclic subgroups of \( E[2^n] \) of order \( 2^n \). First, we will show that each vertex \( v \in |L|_n \) has a unique representative lattice \( \Lambda \) containing \( \Lambda_0 \) such that \( \Lambda/\Lambda_0 \cong \mathbb{Z}/2^{n-1}\mathbb{Z} \) is an isomorphism of \( \mathbb{Z}_2 \)-modules, and that conversely, each such \( \Lambda \) represents a vertex in \( |L|_n \). This statement is trivial for \( n = 0 \). Now let \( n \geq 1 \), and assume inductively that the statement holds for \( n - 1 \). Let \( v \in |L|_n \). Then \( \tilde{v} \in |L|_{n-1} \), and there is a unique lattice \( \Lambda \) representing \( \tilde{v} \) which contains \( \Lambda_0 \) and such that \( \Lambda/\Lambda_0 \cong \mathbb{Z}/2^{n-1}\mathbb{Z} \). Then, since there is an edge connecting \( \tilde{v} \) and \( v \), there is a lattice \( \Lambda > \tilde{\Lambda} \) such that \( \Lambda/\tilde{\Lambda} \cong \mathbb{Z}/2\mathbb{Z} \). So \( \Lambda > \Lambda_0 \) and the \( \mathbb{Z}_2 \)-module \( \Lambda/\Lambda_0 \) is an extension of \( \mathbb{Z}/2\mathbb{Z} \) by \( \mathbb{Z}/2^{n-1}\mathbb{Z} \). If \( \Lambda/\Lambda_0 \) is not cyclic, then \( \Lambda/\Lambda_0 \cong \mathbb{Z}/2^{n-1}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \). It is easy to check that in this case, \( 2\Lambda > \Lambda_0 \), and \( 2\Lambda/\Lambda_0 \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \). Then by the inductive assumption, \( [2\Lambda] \in |L|_{n-2} \), but this is a contradiction since \( [\Lambda] = [2\Lambda] \). Conversely, let \( \Lambda \) be a lattice containing \( \Lambda_0 \) such that \( \Lambda/\Lambda_0 \cong \mathbb{Z}/2^{n}\mathbb{Z} \). Then there is a Jordan-Holder sequence of lattices \( \Lambda_0 < \Lambda_1 < \ldots < \Lambda_{n-1} < \Lambda_n \) such that \( \Lambda_i/\Lambda_{i-1} \cong \mathbb{Z}/2\mathbb{Z} \) for \( 1 \leq i \leq n \), and by checking that the quotient of any \( \Lambda_i/\Lambda_j \) for \( 1 \leq j < i \leq n \) is cyclic, it is clear that none of these lattices are scalar multiples of each other. Thus, there
Let \( \Lambda \in |L| \) which never backtracks. It follows immediately that \( \Lambda \) is a path in \( L \) isomorphisms of \( Z \).

By construction, this \( \Lambda \) is uniquely determined by \( |L| \). Hence, a bijection between \( \Lambda \) and the set of all cyclic \( 2^n \)-subgroups of \( E[2^n] \) for any \( n \geq 0 \), and hence, a bijection between \( |L| \) and the set of all cyclic \( 2 \)-power torsion subgroups of \( E(K) \).

For each \( v \in |L| \), write \( N_v \) for the \( 2 \)-power torsion subgroup corresponding to \( v \) under this bijection. Note that, according to the definition from Section 1 of \( v_i \) for \( i = 1, 2, 3 \), we have \( N_{v_i} = \langle (\alpha_i, 0) \rangle \).

Next we will assign to each \( v \in |L| \) an elliptic curve \( E_{N_v^+} \) and a \( 2^n \)-isogeny \( \phi_{N_v^+} : E \to E_{N_v^+} \), whose kernel is \( N_v \), which we will later show (Proposition 3.6(b)) is defined over \( K(N_v^+) \). We will do this using a well-known isogeny of degree 2 \( (11) \), Chapter III, example 4.5) which is defined over the field of definition of its kernel. (Note that it is well known, as in exercise 3.13(e) of \( (11) \), that for any finite subgroup \( N \subseteq E(K) \), there is an elliptic curve \( E' \cong E/N \) and an isogeny \( E \to E' \) with kernel \( N \) which is defined over the extension \( K(N) \supseteq K \). However, the proof for this is not constructive.) In the following, for \( \alpha_i \in \{ \alpha_1, \alpha_2, \alpha_3 \} \), we will write \( \alpha_{i+1} \) or \( \alpha_{i+2} \) as though \( i \in \mathbb{Z}/3\mathbb{Z} \).

Set \( E_{v_0} := E \), and let \( \phi_{v_0} : E \to E_{v_0} \) be the identity isogeny.

For any \( z \in K \), denote by \( E_z \) the elliptic curve with Weierstrass equation given by

\[
y^2 = (x - \alpha_1 - z)(x - \alpha_2 - z)(x - \alpha_3 - z).
\]

Let \( t_z \) the isomorphism \( E \to E_z \) sending \( (x, y) \rightarrow (x + z, y) \). Define, for any \( \beta, \gamma \in K_1 \), the elliptic curves \( E_{\beta, \gamma} \) and \( E'_{\beta, \gamma} \) given by the following Weierstrass equations:

\[
E_{\beta, \gamma} : y^2 = x(x - \beta)(x - \gamma),
\]

\[
E'_{\beta, \gamma} : y^2 = x^3 - 2(\beta + \gamma)x^2 + (\beta - \gamma)^2x = x(x - (\beta + \gamma + 2\sqrt{\beta\gamma}))(x - (\beta + \gamma - 2\sqrt{\beta\gamma})).
\]

Let \( \phi_{\beta, \gamma} : E_{\beta, \gamma} \to E'_{\beta, \gamma} \) be the isogeny of degree 2 given by

\[
\phi_{\beta, \gamma} : (x, y) \rightarrow (x - (\beta + \gamma) + \frac{\beta\gamma}{x}, y(1 - \frac{\beta\gamma}{x^2})).
\]
Note that the kernel of $\phi_{\beta, \gamma}$ has as its only nontrivial element the 2-torsion point $(0, 0) \in E_{\beta, \gamma}$. Now define, for $i \in \mathbb{Z}/3\mathbb{Z}$,

$$\phi_{N_{v_i}} : E \to E'_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i}, \quad \phi_i := \phi_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i} \circ t_{-\alpha_i}. \quad (20)$$

We assign $E_{N_{v_i}} := E'_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i}$. Note that for each $i$, $\phi_{N_{v_i}} : E \to E_{N_{v_i}}$ is an isogeny whose kernel is the cyclic subgroup $N_{v_i} = \langle (\alpha_i, 0) \rangle$ of order 2.

For each $i \in \mathbb{Z}/3\mathbb{Z}$, we may write the Weierstrass equation for $E_{N_{v_i}}$ as

$$y^2 = x^3 - 2((\alpha_{i+2} - \alpha_i) - (\alpha_i - \alpha_{i+1}))x^2 + (\alpha_{i+1} - \alpha_{i+2})^2x$$

$$= x^3 - 2(2(\alpha_{i+2} - \alpha_i) + (\alpha_{i+1} - \alpha_{i+2}))x^2 + (\alpha_{i+1} - \alpha_{i+2})^2x$$

$$= x^3 - 2(2a_{v_i} + a_{v_i})x^2 + a_{v_i}^2x. \quad (21)$$

Since 0 is a root of the cubic in the above equation, we know that $(0, 0) \in E_{N_{v_i}}[2]$, and it is easy to verify that in fact, $(0, 0)$ is the image of both points in $E[2]\setminus N_{v_i}$. It follows that the inverse image of $\langle (0, 0) \rangle < E_{N_{v_i}}[2]$ under $\phi_{N_{v_i}}$ is $E[2]$. Then the inverse images of the other two order-2 subgroups of $E_{N_{v_i}}(\bar{K})$ under $\phi_{N_{v_i}}$ are the two cyclic order-4 subgroups of $E(\bar{K})$ which contain $N_{v_i}$. It follows that these cyclic order-4 subgroups must be $N_v$ and $N_{v'}$, where $v$ and $v'$ are twin vertices in $|L_2|$ whose parent vertex is $v_j$. Let $a_v$ (resp. $a_{v'}$) be the (nonzero) root of the cubic in the above equation such that $\phi_{N_{v'}}$ takes $N_v$ (resp. $N_{v'}$) to the subgroup $\langle (a_v, 0) \rangle$ (resp. $\langle (a_{v'}, 0) \rangle$) of $E_{N_{v_j}}(\bar{K})$. Now, using the notation of above, we have the elliptic curve $E'_{-a_v, a_v-a_v}$ and the isogeny $\phi_{-a_v, a_v-a_v} \circ t_{-a_v} : E_{N_{v_j}} \to E'_{-a_v, a_v-a_v}$. Its kernel is $\langle a_v, 0 \rangle$. Therefore, if we assign $E_{N_v} := E'_{-a_v, a_v-a_v}$ and

$$\phi_{N_{v}} := \phi_{-a_v, a_v-a_v} \circ t_{-a_v} \circ \phi_{N_{v_j}} : E \to E_{N_v}, \quad (22)$$

then $\phi_{N_{v}}$ has kernel $N_v$. Its Weierstrass equation can be written as

$$y^2 = x^3 - 2((-a_v) + (a_v-a_v))x^2 + ((-a_v) - (a_v-a_v))^2x$$

$$= x^3 - 2(a_{v'} - 2a_v)x^2 + a_{v'}^2x. \quad (23)$$

Thus, we have defined the desired $E_{N_v}$ and $\phi_{N_v}$ for all $v \in \mathcal{L}_2$.

Now we will define the desired $\phi_{N_v}$ and $E_{N_v}$ for any $v \in \mathcal{L}\setminus\{v_0\}$ using induction. Choose any vertex $v \in \mathcal{L}_n$ for $n \geq 2$, and suppose (inductively) that we have assigned elements $a_v, a_{v'} \in \bar{K}$, as well as an elliptic curve $E_{N_v}$ and an isogeny $\phi_{N_v} : E \to E_{N_v}$ whose kernel is $N_v$. Assume further the existence of an elliptic curve $E_{N_{v_j}}$ and an isogeny $\phi_{N_{v_j}} : E \to E_{N_{v_j}}$ whose kernel is $N_{v_j}$.

Suppose that $E_{N_v}$ has Weierstrass equation

$$y^2 = (x - a_v)(x - a_{v'}), \quad (24)$$

that $E_{N_v}$ has Weierstrass equation

$$y^2 = x^3 - 2(a_{v'} - 2a_v)x^2 + a_{v'}^2x, \quad (25)$$
and that \( \phi_{N_v} = \phi_{-a_v,a_v';-a_v} \circ t_{-a_v} \circ \phi_{N_v} \). Then as above, \((0,0) \in E_{N_v}[2] \), and it is easy to verify that, again as above, the inverse image of \( \langle (0, 0) \rangle < E_{N_v}[2] \) under \( \phi_{-a_v,a_v';-a_v} \circ t_{-a_v} \) is \( E_{N_v}[2] \). The inverse image of \( \langle (0, 0) \rangle < E_{N_v}[2] \) under \( \phi_{N_v} \) therefore contains \( E[2] \) and is not a cyclic subgroup of \( E(K) \). The inverse images under \( \phi_{N_v} \) of the other two order-2 subgroups of \( E_{N_v}(K) \) therefore correspond to the two order-2\( n+1 \) cyclic subgroups of \( E(K) \) which contain the order-2\( n \) cyclic subgroup \( N_v \). Therefore, these inverse images are \( N_u \) and \( N_u' \), where \( u \) is a vertex in \( |\mathcal{L}|_{n+1} \) such that \( \bar{u} = v \). Let \( a_u \) (resp. \( a_{u'} \)) be the (nonzero) root of the cubic in the above equation such that \( \phi_{N_v} \) takes \( N_u \) (resp. \( N_u' \)) to the subgroup \( \langle (a_u,0) \rangle \) (resp. \( \langle (a_{u'},0) \rangle \)) of \( E_{N_v}(K) \). Now, using the notation of above, we have the elliptic curve \( E'^{\prime}_{a_u,a_{u'}-a_u} \) and the isogeny \( \phi_{-a_u,a_{u'}-a_u} \circ t_{-a_u} : E_{N_v} \to E'^{\prime}_{a_u,a_{u'}-a_u} \). Its kernel is \( \langle (a_u,0) \rangle \). Therefore, if we assign \( E_{N_v} := E'^{\prime}_{a_u,a_{u'}-a_u} \) and
\[
\phi_{N_u} := \phi_{-a_u,a_{u'}-a_u} \circ t_{-a_u} \circ \phi_{N_v} : E \to E_{N_v},
\]
then \( \phi_{N_u} \) has kernel \( N_u \). Its Weierstrass equation can be written as
\[
y^2 = x^3 - 2((-a_v) + (a_{v'} - a_v))x^2 + ((-a_v) - (a_{v'} - a_v))^2 x
= x^3 - 2(a_{v'} - 2a_u)x^2 + a_u^2 x.
\] (26)
Since the parent of every vertex \( |\mathcal{L}|_{n+1} \) is a vertex in \( |\mathcal{L}|_n \), it follows that through the method described above, we have defined the desired \( E_{N_v} \) and \( \phi_{N_v} \) for all \( v \in |\mathcal{L}|_{n+1} \). In this way, \( E_{N_v}, \phi_{N_v}, \) and \( a_v \in K \) are defined for all \( v \in |\mathcal{L}| \setminus \{v_0\} \). Furthermore, for all \( v \in |\mathcal{L}| \setminus \{v_0\} \), we define \( K_{N_v} \) to be the extension of \( K \) obtained by adjoining the coefficients of the Weierstrass equation of \( E_{N_v} \) given above.

**Remark 3.1.** With the above notation, for any \( v \in |\mathcal{L}|_n \) with \( n \geq 2 \), let \( a_v \) and \( a_{v'} \) be the two distinct nonzero roots of the cubic in \( \{25\} \). Then we have shown above that the isogeny
\[
\phi_{a_v,a_{v'}} \circ \phi_{-a_v,a_{v'}-a_v} \circ t_{-a_v} : E_{N_v} \to E'_{a_v,a_{v'}}
\] (27)
has kernel \( E_{N_v}[2] \). In fact, one can compute that it takes
\[
E_{N_v} : y^2 = x(x - a_v)(x - a_{v'})
\] (28)
to
\[
E'_{a_v,a_{v'}} : y^2 = x(x - 4a_v)(x - 4a_{v'}).
\] (29)
These two elliptic curves are easily seen to be isomorphic over \( K \); for instance, one can define an isomorphism \( E_{N_v} \to E'_{a_v,a_{v'}} \) by \( (x, y) \mapsto (4x, 8y) \).

**Lemma 3.2.** Using the above notation, define \( \Psi : |\mathcal{L}| \setminus \{v_0\} \to K \) by setting \( \Psi(v) = a_v \) for \( v \in |\mathcal{L}| \setminus \{v_0\} \). Then \( \Psi \) is a decoration on \( |\mathcal{L}| \).

**Proof.** The assignments of \( a_v \) for \( i \in \mathbb{Z}/3\mathbb{Z} \) satisfy part (b) of Definition \[1.1\]. For \( v \in |\mathcal{L}|_2, a_v \) and \( a_{v'} \) are, by definition, the two nonzero roots of the cubic in \( \{21\} \). It follows immediately they are the two roots of the quadratic polynomial
\[
x^2 - 2(\Psi((\bar{v})') + 2\Psi(\bar{v}))x + \Psi((\bar{v})')^2 \in K[x].
\] (30)
Similarly, for \( v \in |\mathcal{L}|_n \) with \( n \geq 3 \), \( a_v \) and \( a_{v'} \) are, by definition, the two nonzero roots of the cubic in (23). It follows immediately that they are the two roots of the quadratic polynomial

\[
x^2 - 2(\Psi((\tilde{v})') - 2\Psi(\tilde{v}))x + \Psi((\tilde{v})')^2 \in \bar{K}[x].
\]

(31)

Thus, part (c) of Definition 1.1 is satisfied. Finally, as in the proof of Proposition 1.2, the roots of the above quadratics must be distinct, fulfilling part (a) of Definition 1.1.

\[\square\]

**Definition 3.3.** For any integer \( n \geq 0 \), define the extension \( K'_n \) of \( K \) to be the compositum of the fields \( K_{N_v} \) for all \( v \in |\mathcal{L}|_n \setminus \{v_0\} \). Define the extension \( K'_\infty \) of \( \bar{K} \) to be the infinite compositum

\[
K'_\infty := \bigcup_{n \geq 0} K'_n.
\]

In this way, we obtain a tower of field extensions

\[
K = K'_0 \subset K'_1 \subset K'_2 \subset ... \subset K'_n \subset ...,
\]

(32)

with \( K'_\infty = \cup_{n \geq 0} K'_n \).

**Lemma 3.4.** For each \( v \in |\mathcal{L}|_n \) with \( n \geq 1 \), let \( \{v_0 = v^0, v^1, ..., v^n = v\} \) be the sequence of vertices in the path of length \( n \) from \( v_0 \) to \( v \). Let \( \bar{K}_{N_v} \) denote the compositum of the fields \( K_{N_v} \) for all \( v \in \{v^0, v^1, ..., v^n\} \). Then

\[
\bar{K}_{N_v} = K(\alpha_1, \alpha_2, \alpha_3, \{a_v\}_{v \in \{v^2, ..., v^n\}}).
\]

**Proof.** This is trivial for \( n = 1 \). Now assume inductively that the statement holds for some \( n \geq 1 \) and all \( v \in |\mathcal{L}|_n \). Choose any \( v \in |\mathcal{L}|_{n+1} \). We may apply the inductive assumption to \( \tilde{v} \), since \( \tilde{v} \in |\mathcal{L}|_n \). We know that \( E_{N_v} \) is given by a Weierstrass equation of the form (21) or (23) and is therefore defined over \( K(a_v, a_{v'}) \). But \( a_v a_{v'} \) is a coefficient of \( E_{N_v} \), and so the only element that we need to adjoin to \( \bar{K}_{N_v} = K(\alpha_1, \alpha_2, \alpha_3, \{a_v\}_{v \in \{v^2, ..., v^n\}}) \) to obtain \( \bar{K}_{N_v} \) is \( a_v \). Moreover, \( a_v \) does lie in this extension, since \(-\alpha_v \) is a coefficient in the equation for \( E_{N_v} \) and \( 2(a_{v'} - 2a_v) \) (resp. \( 2(2a_{v'} + a_v) \)) is a coefficient of \( E_{N_v} \) if \( n = 1 \) (resp. \( n \geq 2 \)). Thus, we have proved the claim for \( n + 1 \).

\[\square\]

**Proposition 3.5.** a) For any \( n \geq 1 \), \( K'_n = K(\{\Psi(v)\}_{v \in |\mathcal{L}|_{n+1} \setminus \{v_0\}}) \) for any decoration \( \Psi \) on \( \mathcal{L} \).

b) As in the statement of Theorem 1.3, \( K'_\infty = K(\{\Psi(v)\}_{v \in |\mathcal{L}| \setminus \{v_0\}}) \) for any decoration \( \Psi \) on \( \mathcal{L} \).

(In particular, the extensions \( K(\{\Psi(v)\}_{v \in |\mathcal{L}|_{n+1} \setminus \{v_0\}}) \) and \( K(\{\Psi(v)\}_{v \in |\mathcal{L}| \setminus \{v_0\}}) \) do not depend on the choice of decoration \( \Psi \).)
Proof. Keeping in mind that $K(a_{v_1}, a_{v_2}, a_{v_3}) = K(\alpha_1, \alpha_2, \alpha_3)$, it follows directly from the definition of $K'_n$ and the statement of Lemma 3.4 that
\[
K'_n = K(\{a_v\}_{v \in |L|_n \setminus \{v_0\}}),
\] (33)
from which it follows that
\[
K'_\infty = K(\{a_v\}_{v \in |L| \setminus \{v_0\}}).
\] (34)
Therefore, it suffices to show that for any decoration $\Psi$, $\tilde{K}(\{\Psi(v)\}_{v \in |L|_n \setminus \{v_0\}}) = K(\{a_v\}_{v \in |L|_n \setminus \{v_0\}})$. Choose any decoration $\Psi$. By 1.1(b), $\Psi(v) = a_v$ for any $v \in |L|_1$, so the above claim is true for $n = 1$. Now assume inductively that for some $n \geq 1$, there is a permutation $\sigma$ on $|L|_n$ which preserves distances between vertices (in particular, it acts on each $|L|_i$ for $1 \leq i \leq n$), such that $\Psi(v) = a_{\sigma(v)}$ for all $v \in |L|_n$. For any $i \in \{1, \ldots, n\}$, two vertices in $|L|_i$ are of distance 2 apart if and only if they are twins, so it is clear that $\sigma(v') = \sigma(v')'$ for all $v \in |L|_n$. Now choose any $v \in |L|_{n+1}$. Since $\Psi(v)$ is a root of the quadratic polynomial $x^2 - 2(\Psi(\tilde{v}) + 2\Psi(\tilde{v}'+i))x + \Psi(\tilde{v})x + \Psi(\tilde{v'})x = x^2 - 2(a_{\sigma(\tilde{v})} + 2a_{\sigma(\tilde{v}')})x + a_{\sigma(\tilde{v})}^2$ (resp. $x^2 - 2(\Psi(\tilde{v}') - 2\Psi(\tilde{v}))x + \Psi(\tilde{v})x + \Psi(\tilde{v'})x = x^2 - 2(a_{\sigma(\tilde{v})'} - 2a_{\sigma(\tilde{v})})x + a_{\sigma(\tilde{v})'}^2$) if $n = 1$ (resp. $n \geq 2$), there must exist $u \in |L|_{n+1}$ with $\tilde{u} = \sigma(\tilde{v})$ such that $\Psi(v) = a_u$. Extend $\sigma$ to be a permutation on $|L|_{n+1}$ by assigning $\sigma$ to take each $v \in |L|_{n+1}$ to the vertex $u$ obtained in this way. Then this extension $\sigma$ is clearly a permutation on $|L|_{n+1}$, and one can easily check that $\sigma$ preserves distances between vertices. Therefore, we have the equalities
\[
K(\{\Psi(v)\}_{v \in |L|_{n+1} \setminus \{v_0\}}) = K(\{a_{\sigma(v)}\}_{v \in |L|_{n+1} \setminus \{v_0\}}) = K(\{a_v\}_{v \in |L|_{n+1} \setminus \{v_0\}}),
\] (35)
and we are done.

\[\square\]

Proposition 3.6. With the above notation,
\begin{itemize}
  \item[a)] the isogeny $\phi_{N_v}$ is defined over $K(N_v)$, and $K_{N_v} \subseteq K(N_v)$,
  \item[b)] for all $n \geq 0$, $K'_n \subseteq K_n$, and equality holds for $n = 0, 1$.
\end{itemize}

Proof. First of all, for $i \in \mathbb{Z}/3\mathbb{Z}$, $E_{N_v}$ and $\phi_{N_v}$ are defined over $K(\alpha_{i+1} - \alpha_i, \alpha_{i+2} - \alpha_i) = K(\alpha_1, \alpha_2, \alpha_3) = K_1$. This implies the equality in the $n = 1$ case of the statement in part (b) (the equality in the $n = 0$ case is trivial). It also proves part (a) for $v \in |L|_1$, since $K(N_v) = K(\alpha_1, \alpha_2, \alpha_3) = K_1$ for all $i \in \mathbb{Z}/3\mathbb{Z}$.

Now assume inductively that for some $n \geq 1$ and all $v \in |L|_n$, $\phi_{N_v}$ is defined over $K(N_v)$ and $K_{N_v} \subseteq K(N_v)$. Choose any $v \in |L|_{n+1}$. We may apply the inductive assumption to $\tilde{v}$, since $\tilde{v} \in |L|_n$. Let $P$ be a generator of the cyclic order-$2^{n+1}$ subgroup $N_v$. Then $P$ has coordinates in $K(N_v)$ and $\phi_{N_v}$ is defined over $K(N_v) \subseteq K(N_v)$, and it follows that $\phi_{N_v}(P) = (a_v, 0)$ has coordinates in $K(N_v)$. Thus, $a_v \in K(N_v)$. But $a_v a_v'$ is a coefficient of $E_{N_{\tilde{v}}}$ and $K_{N_v} \subseteq K(N_{\tilde{v}})$, so $a_v' \in K(N_v)$ also. By construction, $\phi_{-a_v, a_v', -a_v} \circ t_{-a_v}$ is defined over $K(a_v, a_v')$, so $\phi_{N_v} = \phi_{-a_v, a_v', -a_v} \circ t_{-a_v} \circ \phi_{N_v}$ is defined over
therefore restricts to an action on 

If \( \text{SL}_2 \) has an action of \( \text{Aut}_Z \), then \( \text{SL}_2 \) has an action of \( \text{Aut}_Z \). Thus, for any \( v \) in \( |L| \), \( \text{SL}_2 \) acts on \( |L| \) by left multiplication, and this action restricts to an action on \( |L| \). This action clearly preserves edge pairings, and therefore restricts an action on \( |L| \) for each \( n \geq 1 \). We will denote this action \( \text{SL}_2(Z_2) \times |L| \rightarrow |L| \) by \( (s, v) \mapsto s \cdot v \). Note that this action of \( \text{SL}_2(Z_2) \), when restricted to \( |L| \), factors through \( \text{SL}_2(Z/2^nZ) \), which we similarly denote by \( \text{SL}_2(Z/2^nZ) \times |L| \rightarrow |L|, (s, v) \mapsto s \cdot v \).

Meanwhile, the choice of basis of \( T_2(E) \) also determines a homomorphism \( \rho_2 : \text{Gal}(K/K) \rightarrow \text{SL}_2(Z_2) \), and for each \( n \geq 0 \), a homomorphism \( \rho_2^{(n)} : \text{Gal}(K_n/K) \rightarrow \text{SL}_2(Z/2^nZ) \), arising from the natural Galois action on \( T_2(E) \).

For any Galois element \( \sigma \in \text{Gal}(K/K) \) and vertex \( v \in |L| \), let \( \sigma := \rho_2(\sigma) \cdot v \).

If \( \sigma \in |L| \), then \( \sigma := \rho_2(n) \cdot v \). Note that it follows from the above construction of the bijection \( v \mapsto N_v \) that \( N_v = N_v \), and that if \( v \in |L| \), then \( N_v < E[2^n] \) and \( N_v \subseteq N_{v,\sigma} \).

**Lemma 3.7.** For any \( \sigma \in \text{Gal}(K/K_1) \) and vertex \( v \in |L| \), we have \( a_v^\sigma = a_v^{\cdot\sigma} \). If \( v \in |L| \), then \( a_v^{\sigma|\sigma} = a_v^{\cdot\sigma} \).

**Proof.** Choose any \( \sigma \in \text{Gal}(K/K_1) \). We will prove that \( a_v^\sigma = a_v^{\cdot\sigma} \) for all \( v \in |L| \), for each \( n \geq 1 \). The claim is trivially true for \( n = 1 \). Moreover, in the \( n = 1 \) case, \( E_{N_v} \) and \( \phi_{N_v} \) are clearly defined over \( K_1 \) and are therefore fixed by \( \sigma \). Now choose \( v \in |L|_1 \). Then \( a_v \) is a nonzero root of \( |L|_1 \), which is the Weierstrass cubic for \( E_{N_v} \). Let \( P \) be a generator of the cyclic order-4 subgroup \( N_v \); then \( \phi_{N_v}(P) = (a_v, 0) \in E_{N_v}[2] \), by the above construction of \( a_v \). So we have

\[
\phi_{N_v}(P^\sigma) = \phi_{N_v}(P^\sigma) = (\phi_{N_v}(P))^\sigma = (a_v^\sigma, 0). \tag{36}
\]

But \( P^\sigma \) generates \( E_{N_v}^\sigma = N_v^{\cdot\sigma} \). Since \( v^\sigma = \tilde{v} \), by the above construction, we have \( \phi_{N_v}(P^\sigma) = (a_v^{\cdot\sigma}, 0) \). Then (36) implies that \( a_v^\sigma = a_v^{\cdot\sigma} \).

Now assume inductively that for some \( n \geq 2 \) and \( \sigma \in |L|_n \), \( a_v^\sigma = a_v^{\cdot\sigma} \), \( E_{N_v}^\sigma = E_{N_v^{\cdot\sigma}} \), and \( \phi_{N_v}^\sigma = \phi_{N_v^{\cdot\sigma}} \). Choose any \( v \in |L|_{n+1} \). We may apply the induction assumption to \( \tilde{v} \), since \( \tilde{v} \in |L|_n \). Then \( a_v \) is a nonzero root of the cubic polynomial \( [23] \), which is the Weierstrass cubic for \( E_{N_v} \). Let \( P \) be a generator.
of the cyclic order-\(2^{n+1}\) subgroup \(N_v\); then \(\phi_{N_v}(P) = (a_v, 0) \in E_{N_v}[2]\), by the above construction of \(a_v\). Then we have
\[
\phi_{N_v}(P^\sigma) = \phi_{N_v}^\sigma(P^\sigma) = (\phi_{N_v}(P))^\sigma = (a_v^\sigma, 0).
\]
(37)

But since \(P^\sigma\) generates \(N_v^\sigma = N_v^\sigma\), again we have \(\phi_{N_v}(P^\sigma) = (a_v^\sigma, 0)\). Then
(37) implies that \(a_v^\sigma = a_v^\sigma\), and so the first statement is proven.

Now let \(v \in |L|_{\leq n}\). Then \(v_v \in K_n\) by 3.6(b), and one easily checks from the definitions that \(v^\sigma = v^\sigma|_{K_n}\) for any \(\sigma \in \text{Gal}(K/K)\). Thus, the second statement follows from the first.

By Proposition 2.5 we may identify \(\text{Gal}(K_n/K_1)\) with \(\text{Gal}(L_n/L_1)\) from Section 2, which Proposition 2.2(c) says is isomorphic to \(\Gamma(2)/\Gamma(2^n)\). It is an immediate corollary of Proposition 3.6(b) that \(\text{Gal}(K'_n/K_1)\) is a quotient of \(\text{Gal}(K_n/K_1)\), for all \(n \geq 1\). The following key lemma characterizes the kernel \(\text{Gal}(K_n/K'_n)\).

**Proposition 3.8.** Fix a basis of the free, rank-2 \(\mathbb{Z}/2^n\mathbb{Z}\)-module \(E[2^n]\), so that via Corollary 2.2(c), we have the canonical isomorphism \(\tilde{\rho}_2^{(n)} : \text{Gal}(K_n/K) \to \text{SL}_2(\mathbb{Z}/2^n\mathbb{Z})\). For all \(n \geq 1\), the image of \(\text{Gal}(K_n/K'_n)\) under \(\tilde{\rho}_2^{(n)}\) coincides with the subgroup of scalar matrices in \(\text{SL}_2(\mathbb{Z}/2^n\mathbb{Z})\).

**Proof.** Fix \(n \geq 1\). Since \(K'_n \supseteq K_1\) for each \(n \geq 1\), we only need to consider the Galois subgroup \(\text{Gal}(K_n/K_1)\). Part (a) of proposition 3.5 with the help of Lemma 5.2 implies that \(K'_n\) is generated over \(K_1\) by the elements \(a_v\) for all \(v \in |L|_{\leq n}\setminus\{v_0\}\). Therefore, the elements of \(\text{Gal}(K_\infty/K_1)\) which fix \(K'_n\) are exactly those which fix all of the elements \(a_v\) for \(v \in |L|_{\leq n}\setminus\{v_0\}\). By Lemma 3.7 for any \(\sigma \in \text{Gal}(K/K_1)\), \(a_v^\sigma = a_v^\sigma\), where \(v^\sigma = \rho_2(\sigma) \cdot v\). Thus, by the construction of \(\tilde{\rho}_2^{(n)}\), we have \(v^\sigma = \tilde{\rho}_2^{(n)}(\sigma|_{K_n}) \cdot v\) for any \(\sigma \in \text{Gal}(K/K_1)\). Therefore, the Galois automorphisms in \(\text{Gal}(K_n/K_1)\) which fix \(a_v\) for all \(v \in |L|_{\leq n}\) are the ones sent by \(\tilde{\rho}_2^{(n)}\) to the matrices that fix all vertices in \(|L|_{\leq n}\). But it was shown in the construction of the bijection \(v \mapsto N_v\) above that the set of such vertices \(v\) corresponds to the set of lattices \(\Lambda \geq \Lambda_0\) with the property that \(\Lambda/\Lambda_0 \cong \mathbb{Z}/2^i\mathbb{Z}\) for some \(i \in \{1, \ldots, n\}\). Clearly, a matrix in \(\text{SL}_2(\mathbb{Z}/2^n\mathbb{Z})\) will fix all such lattices \(\Lambda\) if and only if it is a scalar, hence the claim.

From now on, for ease of notation, we set \(a_i := a_{v_i} = \alpha_{i+1} - \alpha_{i+2}\) for \(i \in \mathbb{Z}/3\mathbb{Z}\). For each \(a_i\), choose an element \(\sqrt{a_i} \in \bar{K}\) whose square is \(a_i\). Also, for \(r \in \bar{Z}_2\), we will write \(r \in \text{SL}_2(\mathbb{Z}_2)\) (resp. \(r \in \text{SL}_2(\mathbb{Z}/2^n)\) for some \(n\)) for the scalar matrix corresponding to \(r\) (resp. \(r\) modulo \(2^n\)). The following proposition, together with Proposition 3.5(b), gives essentially the statement of Theorem 1.3.

**Proposition 3.9.** The Galois group of the field extension \(K_\infty \supseteq K\) is isomorphic to \(\text{SL}_2(\mathbb{Z}_2)\), and the subextension \(K'_n \supseteq K\) corresponds to the subgroup
\[ \{\pm 1\} < SL_2(\mathbb{Z}_2). \] In fact, 
\[ K_\infty = K'_\infty(\sqrt{a_1}), \] 
and the Galois element corresponding to \(-1\) acts by sending \(\sqrt{a_1}\) to \(-\sqrt{a_1}\). (The same statements are true with \(\sqrt{a_1}\) replaced by \(\sqrt{a_2}\) or \(\sqrt{a_3}\).)

**Proof.** The fact that \(\text{Gal}(K_\infty/K) \cong SL_2(\mathbb{Z}_2)\) is clear from \(2.2\) b). Now let \(\sigma\) be a Galois automorphism of \(K_\infty\) over \(K'_\infty\), written as a matrix in \(SL_2(\mathbb{Z}_2)\). By Proposition \(3.8\) it must be a scalar matrix modulo \(2^n\) for every \(n\) and therefore must be a scalar matrix in \(SL_2(\mathbb{Z}_2)\). But the only nonidentity scalar matrix in \(SL_2(\mathbb{Z}_2)\) is \(-1\). Conversely, Proposition \(3.8\) implies that \(-1 \in \text{Gal}(K_\infty/K'_\infty)\), hence the first part of the claim.

It immediately follows that \(K_\infty\) is generated over \(K'_\infty\) by any element of \(K_\infty\) which is not fixed by the Galois automorphism identified with \(-1 \in SL_2(\mathbb{Z}_2)\). This Galois automorphism restricted to \(K_2\) is identified with \((-1) \in \Gamma(2)/\Gamma(4)\). But setting \(n = 2\) in the statement of Proposition \(3.8\) implies that
\[ \text{Gal}(K_2/K'_2) \cong \{\pm 1\} < \Gamma(2)/\Gamma(4), \] so any element in \(K_2 \setminus K'_2\) will not be fixed by \(-1\). One checks using the formulas for \(a_v\) with \(v \in \mathcal{L}_2\) and using Proposition \(3.5\) a) for \(n = 2\) that
\[ K'_2 = K_1(\sqrt{a_1a_2}, \sqrt{a_2a_3}, \sqrt{a_3a_1}). \] Therefore, \(\sqrt{a_1} \notin K'_2\), although \(\sqrt{a_1} \in K_2\) by Proposition \(2.4\). So \(\sqrt{a_1} \in K_\infty \setminus K'_\infty\) and can be used to generate \(K_\infty\) over \(K'_\infty\). Since \(-1\) does not fix \(\sqrt{a_1}\) but does fix its square \(a_1 \in K_1 \subset K'_\infty\), it follows that \(-1\) acts by sending \(\sqrt{a_1}\) to \(-\sqrt{a_1}\). (Of course, the same arguments work for \(\sqrt{a_2}\) and \(\sqrt{a_3}\).)

**Corollary 3.10.** Write \(K(x(E[2^n]))\) (resp. \(K(x(E[2^\infty]))\)) for the extension of \(K\) obtained by adjoining the \(x\)-coordinates of all elements of \(E[2^n]\) (resp. \(E[2^\infty]\)). Then 
\begin{enumerate}
  \item \(K_n = K(x(E[2^n]))(\sqrt{a_i})\) for all \(n \geq 2\) and \(i = 1, 2, 3\);
  \item \(K'_n \subseteq K(x(E[2^n]))\) for all \(n \geq 1\); and
  \item \(K'_\infty = K(x(E[2^\infty]))\).
\end{enumerate}

**Proof.** For any \(n \geq 1\), the subgroup of the Galois group \(\text{Gal}(K_n/K)\) which fixes the \(x\)-coordinates of the points in \(E[2^n]\) can be identified with the elements of \(SL_2(\mathbb{Z}_2)\) which send each point \(P \in E[2^n]\) either to \(P\) or to \(-P\). The only such matrices are the scalar matrices \(\pm 1\). Thus, \(K(x(E[2^n]))\) is the subextension of \(K_n\) corresponding to the subgroup \(\{\pm 1\} < SL_2(\mathbb{Z}/2^n\mathbb{Z})\), and similarly, \(K(x(E[2^\infty]))\) is the subextension of \(K_\infty\) corresponding to the subgroup \(\{\pm 1\} < SL_2(\mathbb{Z}_2)\). Therefore, \(K_n\) is a quadratic extension of \(K(x(E[2^n]))\), and a generator is any element in \(K_n\) which is not fixed by \(-1\). It is shown in the proof of Proposition \(3.9\) that \(\sqrt{a_1}\) lies in \(K_2 \subseteq K_n\) and is not fixed by \(-1\) (and of course this is also true of \(\sqrt{a_2}\) and \(\sqrt{a_3}\)), hence the statement of part (a). Part (b) follows from the fact that \(K'_n\) is the fixed field corresponding to the
subgroup of scalars in $\text{SL}_2(\mathbb{Z}_2)$ by Proposition 3.8 and that $\{\pm 1\}$ is contained in this subgroup of scalars. Part (c) then follows from the fact that $K'_\infty$ is the fixed field corresponding to the subgroup $\{\pm 1\} < \text{SL}_2(\mathbb{Z}_2)$.

The description of $K'_\infty$ given in the statement of Theorem 1.3 provides us with recursive formulas for the generators of $K'_n$ for each $n \geq 0$. We will not similarly obtain formulas for the generators of each extension $K_n$, but the above results do give us a way of “bounding” each $K_n$, as follows:

**Theorem 3.11.** For each $n \geq 2$,

$$K'_n(\sqrt{a_1}) \subseteq K_n \subsetneq K'_{n+1}(\sqrt{a_1}),$$

where the first inclusion is an equality if and only if $n = 2$. Furthermore, $[K_n : K'_n(\sqrt{a_1})] = 2$ for $n \geq 3$, and $[K'_{n+1}(\sqrt{a_1}) : K_n] = 4$ for $n \geq 2$.

**Proof.** Fix $n \geq 2$. By Proposition 3.6(b), $K'_n \subseteq K_n$, and by Proposition 2.4, $\sqrt{a_1} \in K(4) \subset K_n$, thus implying the first inclusion. For $n = 2$, it has already been shown in the proof of Proposition 3.9 that the inclusion is an equality. Since $\sqrt{a_1} \notin K'_\infty$, it follows that $\sqrt{a_1} \notin K(2^i)$ for any positive integer $i$. Note that by Proposition 3.8 for $n \geq 3$, $\text{Gal}(K_n/K'_n)$ is identified with the subgroup $\{\pm 1, \pm(2^{n-1}+1)\} < \text{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$, which is of order 4. So for $n \geq 3$, $K_n$ is an extension of degree 4 over $K'_n$, of which $K'_n(\sqrt{a_1})$ is a quadratic extension, and thus the degree of the first inclusion is 2 in this case. Similarly, for all $n \geq 2$, $K_{n+1} \supseteq K'_{n+1}(\sqrt{a_1})$ is an extension of degree 2. We have (via $\rho_2^{(n+1)}$) the following identifications:

$$\text{Gal}(K_{n+1}/K) = \Gamma(2)/\Gamma(2^{n+1}),$$

$$\text{Gal}(K_{n+1}/K'_n) = (-1, 2^n + 1) \triangleleft \Gamma(2)/\Gamma(2^{n+1}).$$

These imply that $\text{Gal}(K_{n+1}/K'_n(\sqrt{a_1}))$ is a subgroup of $(-1, 2^n + 1)$ of order 2. Since $2^n + 1$ fixes all of $K(4)$, which includes the element $\sqrt{a_1}$, the aforementioned subgroup is $\langle 2^n + 1 \rangle$. But this subgroup also leaves $K_n$ fixed, whence the second inclusion $K_n \subset K'_{n+1}(\sqrt{a_1})$. We now show that this extension has degree 4. Note that, for $n \geq 1$, $\text{Gal}(K_{n+1}/K_n) \cong \Gamma(2^n)/\Gamma(2^{n+1}) \cong (\mathbb{Z}/2\mathbb{Z})^3$, which has order 8. From this we get

$$[K'_{n+1}(\sqrt{a_1}) : K'_n(\sqrt{a_1})] = [K'_{n+1} : K'_n] = 8$$

for $n \geq 2$ and

$$[K'_{n+1}(\sqrt{a_1}) : K'_n(\sqrt{a_1})] = [K'_{n+1} : K'_n] = 4$$

for $n = 1$. Using (43), (44) and the fact that $[K_n : K'_n(\sqrt{a_1})]$ is 2 for $n \geq 2$ and 1 for $n = 1$, it is clear that in both cases, $[K'_{n+1}(\sqrt{a_1}) : K_n] = 4$ as desired.
Acknowledgements

The author would like to thank Yuri Zarhin and Mihran Papikian for their patience, and for insightful discussions which were extremely helpful in producing this work.

References

[1] Norbert A’Campo. Tresses, monodromie et le groupe symplectique. Commentarii Mathematici Helvetici, 54(1):318–327, 1979.

[2] Joan S Birman. Braids, links, and mapping class groups, volume 82. Princeton University Press, 1974.

[3] Gary Cornell, Joseph H Silverman, and Michael Artin. Arithmetic geometry. Springer New York et al., 1986.

[4] A. Grothendieck et al. Revêtements étales et groupe fondamental, Lecture Notes in Mathematics, 224. Springer-Verlag, 1971. arXiv preprint math/0206203, 2002.

[5] David Mumford. Tata lectures on theta. II: Jacobian theta functions and differential equations. with the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura. Progress in Mathematics, 43, 1984.

[6] David Mumford. Abelian varieties, 2nd edition. Oxford Univ Press, 1974.

[7] Rutger Noot. Abelian varieties-galois representations and properties of ordinary reduction. Compositio Mathematica, 97(1):161–172, 1995.

[8] Masatoshi Sato. The abelianization of the level d mapping class group. Journal of Topology, 3(4):847–882, 2010.

[9] Jean-Pierre Serre. Trees. Translated from the french original by John Stillwell. Corrected 2nd printing of the 1980 English translation. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003.

[10] Jean-Pierre Serre. Lettres à Ken Ribet du 1/1/1981 et du 29/1/1981, Collected Papers, vol. IV. Springer-Verlag, Berlin-Heidelberg, 1996, pp. 1-20.

[11] Joseph H Silverman. The arithmetic of elliptic curves, volume 106. Springer, 2009.

[12] Jiu-Kang Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. preprint, 1997.