The Pennsylvania State University

The Graduate School

The Eberly College of Science

HYPERELLIPTIC JACOBIANS AND THEIR ASSOCIATED ℓ-ADIC GALOIS REPRESENTATIONS

A Dissertation in Mathematics by

Jeffrey S. Yelton

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

August 2015

The dissertation of Jeffrey S. Yelton was reviewed and approved* by the following:

Yuri Zarhin
Professor of Mathematics
Dissertation Adviser
Chair of Committee

Mihran Papikian
Associate Professor of Mathematics

Wen-Ching W. Li
Distinguished Professor of Mathematics

Donald Richards
Professor of Statistics

Yuxi Zheng
Professor of Mathematics
Head of the Department of Mathematics

* Signatures are on file in the Graduate School.

Abstract

First let k be a field of characteristic different from 2, and let K be the extension of k obtained by adjoining the symmetric functions of the independent transcendental elements $\alpha_1, \alpha_2, ..., \alpha_d$ for some $d \geq 3$. For each prime ℓ, we examine the natural ℓ-adic representation of the absolute Galois group of K associated to the "generic" Jacobian J of the hyperelliptic curve over K whose Weierstrass roots are the α_i's. In particular, we show that the image of the absolute Galois group in the group of automorphisms of the ℓ-adic Tate module $T_\ell(J)$ contains the entire symplectic group $\mathrm{Sp}(T_\ell(J))$ when $\ell \neq 2$, and that it contains the level-2 congruence subgroup $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$ when $\ell = 2$. We also derive formulas for generators for the field extension $K(J[4])/K$, as well as formulas for generators of $K(J[8])/K$ in the case that J is an elliptic curve.

We then give a full desription of the infinite algebraic extension of K generated by the coordinates of all 2-power torsion points of J when d is 3, 5, or 6, by giving recursive formulas for the generators. This is done in all of the above cases by associating to J a regular tree and assigning elements of the algebraic closure of K to the vertices of the tree. We also use these constructions to describe several other algebraic extensions of K related to the subgroup of dyadic torsion of J.

Contents

Acknowledgments **vi**

1 Introduction **1**
1.1 Outline and conventions of dissertation 1
1.1.1 Outline 1
1.1.2 Notation 2
1.2 Hyperelliptic Jacobians 3
1.2.1 Definition and construction 3
1.2.2 Fields of 2-torsion of hyperelliptic Jacobians 5
1.2.3 Main results concerning 2-power torsion 7
1.3 Galois actions on ℓ-adic Tate modules 8
1.3.1 Open image theorems 9
1.3.2 Main result concerning images of Galois 11

2 Families of Jacobians **13**
2.1 Topological preliminaries 13
2.1.1 Configuration spaces and braid groups 13
2.1.2 Mapping class groups 15
2.1.3 Dehn twists 17
2.2 A family of hyperelliptic curves over $\mathbb{C}$ 19
2.2.1 Construction of several families 19
2.2.2 The induced monodromy representation 21
2.2.3 Relationship to the mapping class group 22
2.2.4 Image of the monodromy representation 25
2.3 Generic image of Galois 26
2.3.1 Proof of the main theorem 27
2.3.2 Corollaries and applications 31
2.4 Fields of 4-torsion of hyperelliptic Jacobians 32

2.4.1 The case of odd degree 33
2.4.2 The case of even degree 35
2.5 Fields of 8-torsion of elliptic curves 40
2.6 Generalization to other ground fields 43

3 Dyadic torsion of elliptic curves **47**
3.1 Construction of decorations for genus 1 47
3.1.1 Equivalence classes of rank-2 $\mathbb{Z}_2$-lattices 47
3.1.2 A 3-regular tree 49
3.1.3 Decorations on 3-regular trees 50
3.2 Field of dyadic torsion for genus 1 51
3.2.1 Compositions of 2-isogenies of elliptic curves 52
3.2.2 The subfield fixed by the scalar subgroup 58
3.2.3 A general lemma 60
3.3 Description of some subextensions 62
3.3.1 Extensions generated by x-coordinates 62
3.3.2 Bounding each field of 2^n-torsion 63
3.4 Application to the Legendre family 64

4 Dyadic torsion of 2-dimensional hyperelliptic Jacobians **69**
4.1 Construction of decorations for genus 2 69
4.1.1 Preliminary results on the Weil pairing 69
4.1.2 Equivalence classes of isotropic rank-4 $\mathbb{Z}_2$-lattices . . . 73
4.1.3 A 15-regular tree 76
4.1.4 Decorations on 15-regular trees 77
4.2 Field of dyadic torsion for genus 2 79
4.2.1 The Richelot isogeny 80
4.2.2 Compositions of $(2,2)$-isogenies of Jacobians 83
4.2.3 The subfield fixed by the scalar subgroup 87
4.3 Subextensions associated to the Kummer surface 89

Bibliography **91**

Acknowledgments

First and foremost, I would like to thank my adviser Yuri Zarhin, who has been a great source of inspiration as a mathematician, and whose insight and suggestions guided me through my thesis research and have made me a better mathematician as well. I would also like to extend my gratitude to Mihran Papikian and Winnie Li, for their instruction and guidance which was immensely helpful to me throughout my years in graduate school.

As a graduate student in the Penn State math department, I could not have asked for a more supportive and stimulating environment for studying and participating in mathematical research. The graduate students, postdocs, and professors in the department who have continually challenged me and aided me in mathematical struggles are too many to name here. In addition, I am grateful for the opportunities to attend a number of inspiring conferences and workshops, particularly the Arizona Winter School, at which I have had positive interactions with many mathematicians from other departments. I have also benefited from being able to balance my work life with leisure time, and I am grateful for all of the friends I have made over my years as a graduate student, both in the department and out, who have provided me with great memories of my time in State College.

And lastly, I owe a great deal to my parents, who were my first math teachers, and who have played the greatest role in guiding me through the challenges of school as well as life. None of my academic success would have been possible had they not nurtured and encouraged my love of mathematics from a very early age. The love and support of my family has been present throughout my life's journey not only as a student but as a person, and I will be forever grateful for it.

Chapter 1

Introduction

Over the last fifty years, the natural ℓ-adic Galois representations associated to abelian varieties have been objects of great interest to number theorists and algebraic geometers. Descriptions of the images of such representations associated to an abelian variety often determine its endomorphism ring, and shed light on such problems as the Hodge conjecture and the Mumford-Tate conjecture. This dissertation contains results describing the natural Galois action on ℓ-adic Tate modules of Jacobians of hyperelliptic curves, as well as results which give generators for fields of definition of various torsion subgroups of these Jacobians of 2-power order. We will present these results and their proofs, as well as relevant background information, in several chapters.

1.1 Outline and conventions of dissertation

1.1.1 Outline

In this chapter, we will introduce notation used throughout this thesis, the main objects that our results will be concerned with, and several background results. In §1.2 we define the Jacobian of a hyperelliptic curve over a certain function field and completely describe the 2-torsion points of this Jacobian as well as the field over which they are defined. In §1.3 we discuss the natural ℓ-adic Galois representations associated to this Jacobian, describe some background results concerning the images of these representations, and give our result on their images in the "generic" case.

In Chapter 2, we develop some topological constructions which will be needed to prove several results for hyperelliptic Jacobians defined over a field containing $\mathbb{C}$, including descriptions of the ℓ-adic image of Galois for any prime ℓ, the field of definition of 4-torsion of a hyperelliptic Jacobian of any dimension, and the field of definition of 8-torsion of an elliptic curve.

In Chapter 3, we use sequences of 2-isogenies of elliptic curves to derive generators of the field of definition of all 2-power torsion of an elliptic curve. We use this construction to give a description of the field extension obtained by adjoining the x-coordinates of all 2-power torsion points of an elliptic curve, as well as a partial description of the field of definition of the 2^n-power torsion for each positive integer n.

In Chapter 4, we use sequences of $(2,2)$-isogenies of Jacobians of genus-2 hyperelliptic curves to derive generators of the field of all 2-power torsion of the Jacobian of a genus-2 hyperelliptic curve. We use this construction to give a description of the field extension obtained by adjoining the coordinates of the images of all 2-power torsion points in the corresponding Kummer surface.

1.1.2 Notation

We adhere to the following notational conventions throughout this dissertation.

If S is a set, we write $|S|$ for the cardinality of S.

If N is a group or a module containing elements $a_1, a_2, ..., a_m \in N$, we write $\langle a_1, a_2, ..., a_m \rangle$ for the subgroup or submodule of N which they generate. We often use the symbols "$<$" and "$>$" to indicate inclusion of subgroups or sublattices.

For any group G of automorphisms of a free R-module, where the ring R is $\mathbb{Z}$, $\mathbb{Z}_2$, or $\mathbb{Z}/2^n\mathbb{Z}$ with $n \in \mathbb{Z}_{\geq 0}$, and for any integer $r \in \mathbb{Z}$, we write $r \in G$ for the scalar automorphism corresponding to the image of r under the obvious ring homomorphism $\mathbb{Z} \to R$. In particular, $1 \in G$ denotes the identity automorphism, and $-1 \in G$ denotes the automorphism of G which sends each element to its additive inverse.

For any group G of automorphisms of a free R-module, where the ring R is $\mathbb{Z}$ or $\mathbb{Z}_\ell$ for a prime ℓ, and for any integer $N \geq 1$, we write $\Gamma(N) \lhd G$ for the kernel of reduction modulo N (which we call "the level-N congruence

subgroup of G"); in other words,

$$\Gamma(N) = \{\sigma \in G \mid \sigma \equiv 1 \pmod{N}\}.$$

We fix, once and for all, a complex number $\sqrt{-1} \in \mathbb{C}$ whose square is -1.

Given a field k and an algebraic closure $\bar{k}$ of k, we fix, once and for all, a compatible system of Nth roots of unity $\zeta_N \in \bar{k}$ for $N = 1, 2, 3, ...$; that is, we have $\zeta_{N'}^{N'/N} = \zeta_N$ for any positive integers N and N'. If $k \subset \mathbb{C}$, then we put $\zeta_N = \{e^{2\pi\sqrt{-1}/N}\}$ for $N = 1, 2, 3, ...$ For any prime ℓ, let $\mu_\ell \subset \bar{k}^\times$ denote the subgroup generated by $\{\zeta_{\ell^n}\}_{n \geq 1}$. We write $T_\ell(\mu)$ for the inverse limit of the system of subgroups $\langle \zeta_{\ell^n} \rangle \subset \bar{k}^\times$ under the ℓth-power homomorphism $[\ell] : \langle \zeta_{\ell^{n+1}} \rangle \to \langle \zeta_{\ell^n} \rangle$; although $T_\ell(\mu)$ is a free $\mathbb{Z}_\ell$-module of rank 1, we will consider it as a multiplicative group.

Let X be a complex manifold (resp. a scheme over a field k), and let t be a point (resp. a k-point) of X. Then if $\mathcal{F} \to X$ is a family, we denote the fiber over t by $\mathcal{F}_t$.

1.2 Hyperelliptic Jacobians

The main object of study in this dissertation is the Jacobian of a hyperelliptic curve. Most of the results will concern the Jacobian of the "generic" hyperelliptic curve of degree $d \geq 3$; therefore, we will start by defining this object over a ground field in which the Weierstrass roots are transcendental over its prime subfield. Since some of the results concern the fields of 2-power torsion of these Jacobians, we will then give a full description of their 2-torsion subgroups, and state the main results which describe their fields of higher 2-power torsion.

1.2.1 Definition and construction

Let k be any field of characteristic different from 2. Fix an integer $d \geq 3$; let $\alpha_1, \alpha_2, ..., \alpha_d$ be transcendental and independent over k; and let K be the subfield of $k(\alpha_1, ..., \alpha_d)$ generated over k by the symmetric functions of the α_i's. We fix an algebraic closure $\bar{K}$ of K. Then

$$y^2 = \prod_{i=1}^{d} (x - \alpha_i) \tag{1.1}$$

is an equation for an affine hyperelliptic curve C' of degree d over K. We construct a smooth, projective model C of this curve as follows. Let C'' be the curve defined over K given by the equation

$$y'^2 = x' \prod_{i=1}^{d} (1 - \alpha_i x') \tag{1.2}$$

if d is odd, and by the equation

$$y'^2 = \prod_{i=1}^{d} (1 - \alpha_i x') \tag{1.3}$$

if d is even. 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

$$x' \mapsto \frac{1}{x}, \; y' \mapsto \frac{y}{x^{\lfloor (d+1)/2 \rfloor}},$$

and denote the resulting (smooth, projective) curve by C. If d is odd, C has one "point at infinity" given by $(x', y') = (0, 0) \in C''(K)$, which we denote by ∞; if d is even, C has two "points at infinity" given by $(x', y') = (0, \pm 1) \in C''(K)$, which we denote by $\infty_1 := (0, -1)$ and $\infty_2 := (0, 1)$. (See [18], §1 for more details of this construction.) It is well known that the genus of C is $g := \lfloor (d-1)/2 \rfloor$; i.e. $d = 2g + 1$ or $d = 2g + 2$. (Note that our definition of a hyperelliptic curve will include the case where $d = 3$ or $d = 4$ and the curve is an elliptic curve.)

There is an obvious degree-2 morphism $C \to \mathbb{P}^1_K$ defined over K, which is defined on C' by projection onto the x-coordinate, and which sends the point(s) at infinity to $\infty \in \mathbb{P}^1_K$. By the Hurwitz formula, this morphism is ramified over exactly $2g + 2$ points in $\mathbb{P}^1_{\bar{K}}$, which we call the *branch points* of C. We denote this $(2g + 2)$-element set of branch points by B. It is easy to see that if d is odd, then $B = \{\alpha_i\}_{i=1}^d \cup \{\infty\} \in \mathbb{P}^1_{\bar{K}}$, and if d is even, then $B = \{\alpha_i\}_{i=1}^d \in \mathbb{P}^1_{\bar{K}}$.

For any algebraic extension $K' \supset K$, we denote by $\mathrm{Div}^0(C)(K')$ the group of degree-0 divisors on C which are fixed by $\mathrm{Gal}(\bar{K}/K')$, and we denote by $\mathrm{Pic}^0(C)(K')$ the quotient group of $\mathrm{Div}^0(C)(K')$ modulo divisors of functions in $K'(C)^\times$. (When the field K' is clear from context, we will denote these groups simply by $\mathrm{Div}^0(C)$ and $\mathrm{Pic}^0(C)$.) There is an abelian variety J defined over K which represents the assignment $K' \mapsto \mathrm{Pic}^0(C)(K')$; i.e. J is a

projective group variety such that for any extension $K' \supset K$, $J(K')$ and $\mathrm{Pic}^0(C)(K')$ are isomorphic as abstract groups (see §1 of [14]). We call J the *Jacobian* of C; it is an abelian variety over K of dimension g. An explicit construction of the Jacobian of a hyperelliptic curve is given in [18], §2.

For any integer $N \geq 1$, let $J[N]$ denote the N-torsion subgroup of $J[\bar{K}]$; by the results in §6 of [16], $J[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank $2g$. We let $K(J[N])$ denote the (finite algebraic) extension of K obtained by adjoining the coordinates of all $\bar{K}$-points of $J[N]$.

1.2.2 Fields of 2-torsion of hyperelliptic Jacobians

Note that the extension $K(\{\alpha_i\}_{i=1}^d)/K$ is Galois, and we may canonically identify the Galois group $\mathrm{Gal}(K(\{\alpha_i\}_{i=1}^d)/K)$ with S_d, the symmetric group on d objects. For any subgroup $H \subset S_d$, let $K(\{\alpha_i\}_{i=1}^d)^H$ denote the subfield of $K(\{\alpha_i\}_{i=1}^d)$ fixed by $H \subset \mathrm{Gal}(K(\{\alpha_i\}_{i=1}^d)/K)$.

We now describe completely the subgroup $J[2]$ as well as the field extension $K(J[2])/K$ for any degree $d \geq 3$. This result is already well-known; for instance, the description below of the elements of $J[2]$ is given in [18] (the statement and proof of Corollary 2.11) for hyperelliptic Jacobians over $\mathbb{C}$.

Proposition 1.2.1. *a) The 2-torsion subgroup $J[2]$ consists of all elements of $\mathrm{Pic}^0(C)(\bar{K})$ represented by elements of the form*

$$e_U := \sum_{\alpha \in U} (\alpha, 0) - |U| \cdot (\infty) \in \mathrm{Div}^0(C)(\bar{K})$$

if d is odd, and of the form

$$e_U := \sum_{\alpha \in U} (\alpha, 0) - \frac{|U|}{2} \cdot ((\infty_1) + (\infty_2)) \in \mathrm{Div}^0(C)(\bar{K})$$

if d is even, where $U \subset B$ is a subset of even cardinality. For two subsets $U, U' \subset B$ of even cardinality, $e_U, e_{U'} \in \mathrm{Div}^0(C)(\bar{K})$ represent the same element of $J[2]$ if and only if $U' = U$ or $U' = B \setminus U$.

b) The Galois group $\mathrm{Gal}(K\{\alpha_i\}_{i=1}^d)/K)$ acts on the representative of each such divisor e_U through its action on $B \subset \mathbb{P}^1_{\bar{K}}$ (where the points at infinity are fixed by all Galois elements).

c) If $d \neq 4$, we have

$$K(J[2]) = K(\{\alpha_i\}_{i=1}^d) \tag{1.4}$$

and $\mathrm{Gal}(K(J[2])/K) \cong S_d$. *If* $d = 4$, *we have*

$$K(J[2]) = K(\{\alpha_i\}_{i=1}^4)^V \tag{1.5}$$

and $\mathrm{Gal}(K(J[2])/K) \cong S_4/V \cong S_3$, *where* V *is the unique normal order-*4 *subgroup of* S_4.

Proof. We first note that for each α_i, the divisor of the function $x - \alpha_i \in K(C)^\times$ is $2(\alpha_i, 0) - 2(\infty) \in \mathrm{Div}^0(C)(\bar{K})$ (resp. $2(\alpha_i, 0) - (\infty_1) - (\infty_2) \in \mathrm{Div}^0(C)(\bar{K})$) if d is odd (resp. if d is even). It follows that for any subset $U \subset B$ of even cardinality, $2e_U$ is a principal divisor. Thus, each e_U represents an element of $J[2]$.

Now assume that $U, U' \subset B$ are subsets of even cardinality and that e_U and $e_{U'}$ represent the same element in $J[2]$. Then $e_U - e_{U'}$ is a principal divisor. But clearly $e_U - e_{U'}$ represents the same element as $e_{U \circ U'}$ in $J[2]$, where $U \circ U' = (U \cup U') \setminus (U \cap U')$, so it will suffice to show that e_U is a principal divisor if and only if $U = \varnothing$ or $U = B$. It is easy to see that e_B is the divisor of $y \in \bar{K}(C)^\times$. It follows that e_U represents the same element as $e_U + e_B$, which is clearly equivalent to $e_{B \setminus U}$. So by possibly replacing U with $B \setminus U$, we may assume that U consists of K-points of $\mathbb{P}^1_{\bar{K}} \setminus \{\infty\}$ and $|U| \leq g$. If e_U is the divisor of a function g, clearly this function has no poles at any $\bar{K}$-point of C', so g must be a polynomial in x and y. Since the divisor of poles of y has degree d and the divisor of poles of g has degree $\leq g = \lfloor (d-1)/2 \rfloor$, g must be a polynomial in x only. Then if U is nonempty, $(x - \alpha) | g$ for some $\alpha \in U$. But the order of $(x - \alpha)$ is 2 at the point $\alpha \in C'(\bar{K})$, and $g/(x - \alpha)$ can have no poles on C', which contradicts the fact that the divisor of g is e_U. Therefore, $U = \varnothing$, as desired.

By what has been proved above, the set of points in $J[2]$ represented by divisors of the form e_U for $U \subset B$ a subset of even cardinality is parametrized by the partitions of B into 2 even subsets. By an easy combinatorial argument, there are 2^{2g} such partitions. But $|J[2]| = |(\mathbb{Z}/2\mathbb{Z})^{\oplus 2g}| = 2^{2g}$, so these divisors represent all elements in $J[2]$. Thus, part (a) is proved.

Part (b) is clear from the definition of e_U for each of the subsets $U \subset B$.

Since each element e_U is clearly a divisor in $\mathrm{Div}^0(C)(K(\{\alpha_i\}_{i=1}^d))$, we have the inclusion $K(J[2]) \subseteq K(\{\alpha_i\}_{i=1}^d)$. If $d \neq 4$, then clearly the only permutation in $S_d \cong \mathrm{Gal}(K(\{\alpha_i\}_{i=1}^d))$ which fix all partitions of B into 2 even subsets is the identity, and it follows that $K(J[2]) = K(\{\alpha_i\}_{i=1}^d)$. One checks that the subgroup of permutations in S_4 which fix all partitions of a

4-element set into 2 even subsets coincides with $V \lhd S_4$, and thus, if $d = 4$, we have $K(J[2]) = K(\{\alpha_i\}_{i=1}^4)^V$. This proves part (c).

□

1.2.3 Main results concerning 2-power torsion

Since the extension $K(J[2])$ has such a nice description, it is natural to ask for a description of $K(J[2^n])/K$ for $n = 2, 3, ...$ In §2.4, we present and prove a result (which is a generalization of Proposition 3.1 of the author's paper [32]) that gives generators for $K(J[4])$ over $K(J[2])$.

Theorem 1.2.2.
(a) If $d = 2g + 1$, then

$$K(J[4]) = K(J[2])(\zeta_4, \{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i < j \leq d}). \tag{1.6}$$

(b) If $d = 2g + 2$, then

$$K(J[4]) = K(J[2])(\zeta_4, \{\sqrt{\alpha_i - \alpha_j} \prod_{\substack{1 \leq l \leq d-1 \\ l \neq i,j}} \sqrt{\alpha_l - \alpha_d}\}_{1 \leq i < j \leq d}). \tag{1.7}$$

In §2.5, we present and prove a result that gives generators for $K(J[8])$ over $K(J[4])$ in the case that J is an elliptic curve.

Theorem 1.2.3. *Assume that $d = 3$ or $d = 4$ (i.e. $g = 1$). For $i = 1, 2, 3$, considering i as an element of $\mathbb{Z}/3\mathbb{Z}$, choose an element $A_i \in K(J[4])$ such that $A_i^2 = \alpha_{i+1} - \alpha_{i+2}$ (resp. $A_i^2 = (\alpha_i - \alpha_4)(\alpha_{i+1} - \alpha_{i+2})$) if $d = 3$ (resp. if $d = 4$). Then*

$$K(J[8]) = K(J[4])(\zeta_8, \{\sqrt{A_i(A_{i+1} + \zeta_4 A_{i+2})}\}_{1 \leq i \leq 3}). \tag{1.8}$$

We are not able to explicitly describe the extensions generated by 2-power torsion points for higher powers of 2. However, in Chapters 3 and 4, we give recursive formulas for generators of the full extension $K(J[2^\infty])/K$ generated all 2-power torsion points of J when $d = 3$ (Theorem 3.2.1) and when $d = 5, 6$ (Theorem 4.2.1) respectively. Moreover, in the $g = 1$ case, we are able to use these recursive formulas to completely describe a particular biquadratic extension of $K(J[2^n])$ for each $n \geq 2$ (Theorem 3.3.2). These results can also be found in the author's preprints [30] and [31] respectively.

1.3 Galois actions on ℓ-adic Tate modules

This dissertation largely deals with the action of the absolute Galois group of K on the torsion subgroups of J. Fix an algebraic closure $\bar{K}$ of K. Note in particular that for any integer N, the multiplication-by-N map on J is defined over K, and therefore, the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ acts on the torsion subgroup $J[N]$. In particular, for any prime ℓ and integer $n \geq 0$, $\mathrm{Gal}(\bar{K}/K)$ acts on $J[\ell^n]$. Moreover, this action commutes with the multiplication-by-ℓ map $[\ell] : J[\ell^{n+1}] \to J[\ell^n]$ for each $n \geq 0$. Let

$$T_\ell(J) := \lim_{\leftarrow n} J[\ell^n]$$

denote the inverse limit of the projective system $\{J[\ell^{n+1}] \xrightarrow{[\ell]} J[\ell^n]\}$. We refer to $T_\ell(J)$ as the *ℓ-adic Tate module* of J; it is a free $\mathbb{Z}_\ell$ module of rank $2g$. It follows from the above discussion that the action of $\mathrm{Gal}(\bar{K}/K)$ on $J[\ell^n]$ for each n induces an action of $\mathrm{Gal}(\bar{K}/K)$ on $T_\ell(J)$. We write $\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J))$ for the homomorphism induced by this action; ρ_ℓ is a continuous homomorphism from the profinite Galois group $\mathrm{Gal}(\bar{K}/K)$ to the ℓ-adic algebraic group $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J))$. We denote the image of $\mathrm{Gal}(\bar{K}/K)$ under ρ_ℓ by G_ℓ.

Since J is the Jacobian of a curve, it comes equipped with a canonical principal polarization. For any prime ℓ and any $n \geq 0$, the principal polarization on J induces a canonical skew-symmetric alternating pairing

$$\bar{e}_\ell^{(n)} : J[\ell^n] \times J[\ell^n] \to \mu_{\ell^n},$$

known as the *Weil pairing* on $J[\ell^n]$. It is known ([13], Lemma 16.1) that for $n \geq 0$ and $P, Q \in J[\ell^{n+1}]$, $\bar{e}_\ell^{(n+1)}(P,Q)^m = \bar{e}_\ell^{(n)}([\ell]P, [\ell]Q)$. It follows that the system of Weil pairings $\{\bar{e}_\ell^{(n)}\}$ induces a skew-symmetric alternating pairing

$$e_\ell : T_\ell(J) \times T_\ell(J) \to T_\ell(\mu),$$

similarly known as the *Weil pairing* on $T_\ell(J)$. (See [16], §20 or [13], §16 for more details.)

It is well known that the Weil pairing e_ℓ is equivariant with respect to the Galois action ρ_ℓ; i.e.

$$e_\ell(P^\sigma, Q^\sigma) = e_\ell(P,Q)^\sigma \tag{1.9}$$

for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. It follows that G_ℓ is contained in the *group of symplectic similitudes*

$$\mathrm{GSp}(T_\ell(J)) := \{\sigma \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \mid e_\ell(P^\sigma, Q^\sigma) = e_\ell(P,Q)^{\chi_\ell(\sigma)}\ \forall P, Q \in T_2(J)\},$$

where $\chi_\ell : \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \to \mathrm{Aut}(T_\ell(\mu))$ is a homomorphism which induces the ℓ-adic cyclotomic character of the Galois group $\mathrm{Gal}(\bar{K}/K)$. If k contains all ℓ-power roots of unity, then e_ℓ is Galois invariant and G_ℓ is contained in the *symplectic group*

$$\mathrm{Sp}(T_\ell(J)) := \{\sigma \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \mid e_\ell(P^\sigma, Q^\sigma) = e_\ell(P,Q)\ \forall P, Q \in T_2(J)\}.$$

In the case that $g = 1$, the group $\mathrm{GSp}(T_\ell(J))$ (resp. the group $\mathrm{Sp}(T_\ell(J))$) coincides with the group $\mathrm{GL}(T_\ell(J)) := \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J))$ (resp. the group $\mathrm{SL}(T_\ell(J))$) of automorphisms of $T_\ell(J)$ of determinant 1).

For each $n \geq 0$, we define $\mathrm{GSp}(J[\ell^n])$ and $\mathrm{Sp}(J[\ell^n])$ similarly. We denote the action of $\mathrm{Gal}(\bar{K}/K)$ on $J[\ell]$ by $\bar{\rho}_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(J[\ell])$; similarly, the image $\bar{G}_\ell$ of $\mathrm{Gal}(\bar{K}/K)$ under $\bar{\rho}_\ell$ is contained in $\mathrm{GSp}(J[\ell])$, and if $\zeta_\ell \in k$, then $\bar{G}_\ell$ is contained in $\mathrm{Sp}(J[\ell])$.

1.3.1 Open image theorems

In this subsection, we assume that J is the Jacobian of a hyperelliptic curve defined by an equation of the form in (3.1) but that each α_i is an element of k, so that J is defined over k. We observe that, by Proposition 1.2.1(c), the image $\bar{G}_2$ of $\bar{\rho}_2$ in $\mathrm{GSp}(J[2]) = \mathrm{Sp}(J[2])$ is isomorphic to a subgroup of S_d (resp. to a subgroup of $S_4/V \cong S_3$) if $d \neq 4$ (resp. if $d = 4$).

It is expected that for "most" hyperelliptic Jacobians J over a field k of characteristic 0 which is finitely generated over its prime subfield, the image of the absolute Galois group under ρ_ℓ is "large", i.e. open with finite index in $\mathrm{GSp}(T_\ell(J))$. It is clear that there exist hyperelliptic Jacobians with endomorphism ring $\mathbb{Z}$, and that in many cases (such as that of elliptic curves, by Theorem 1.3.4 below), this implies a "large" Galois image, but it has been shown (see §4 of [15] and §1 of [20]) that this implication does not always hold for abelian varieties of dimension $g = 4$. On the other hand, the following theorems show that there exist many families of Jacobians over a given number field k for which this is the case for all (or almost all) fibers, which immediately implies that the Galois image is "large" in the "generic" case of §1.1.

Theorem 1.3.1. *(Zarhin, [34], Theorem 2.5)*

With the above notation, assume that k is finitely generated over $\mathbb{Q}$ and that the degree is $d \geq 5$. If $\bar{G}_2$ is isomorphic to S_d or A_d, then G_ℓ is open with finite index in $\mathrm{Sp}(T_\ell(J))$ for each prime ℓ.

Theorem 1.3.2. *(Zarhin, [35], Theorem 8.3)*

With the above notation, assume that k is finitely generated over $\mathbb{Q}$ and that $f(x) = (x-t)h(x)$ for some $t \in k$ and such that the degree of h is $d-1 \geq 9$. If $\bar{G}_2$ is isomorphic to S_{d-1} or A_{d-1}, then G_ℓ is open with finite index in $\mathrm{Sp}(T_\ell(J))$ for each prime ℓ.

Theorem 1.3.3. *(Cadoret-Tamagawa, [6], Theorem 1.1 and Theorem 5.1)*

With the above notation, assume that k is finitely generated over $\mathbb{Q}$. Let X be a smooth, geometrically connected, separated curve over k, and let $\mathcal{A} \to X$ be an abelian scheme. For each $t \in X(k)$, we denote the fiber at t by $\mathcal{A}_t$, the corresponding ℓ-adic Galois representation by $\rho_{\ell,t} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{GSp}(T_\ell(\mathcal{A}_t))$, and the image of $\mathrm{Gal}(\bar{k}/k)$ under this map by $G_{\ell,t}$; we denote the analogous ℓ-adic Galois image associated to a generic fiber by $G_{\ell,X}$. Then

a) the subset $S_{\ell,\mathcal{A}} \subset X(k)$ of $t \in X(k)$ such that $G_{\ell,t}$ is not of finite index in $G_{\ell,X}$ is finite; and

b) there exists an integer $B_{\ell,\mathcal{A}} \geq 1$ such that the index of $G_{\ell,t}$ in $G_{\ell,X}$ is bounded by $B_{\ell,\mathcal{A}}$ for each $t \in X(k) \setminus S_{\ell,\mathcal{A}}$.

The above theorem says that when k is finitely generated over $\mathbb{Q}$, for any one-parameter family of Jacobians over k, all but finitely many of the fibers will have the property that the ℓ-adic image of Galois is uniformly "large" in the generic image of Galois. Theorem 1.3.2 provides a one-parameter family of Jacobians of hyperelliptic curves of degree $d \geq 10$ for which this finite subset is empty.

Meanwhile, it is known exactly for which elliptic curves the Galois image is "large", as in the following celebrated theorem of Serre.

Theorem 1.3.4. *(Serre's Open Image Theorem, [24], Chapter IV, §2.2) With the above notation, suppose that J is an elliptic curve. Then G_ℓ is open with finite index in $\mathrm{GSp}(T_\ell(J)) = \mathrm{GL}(T_\ell(J))$ if and only if J has no complex multiplication.*

Thus, "most" elliptic curves have a "large" Galois image G_ℓ for each prime ℓ. It is also known for elliptic curves (for instance by an application of Proposition 1.3 of [19] to Corollary 1 of Chapter 6, §3 of [12]) that the ℓ-adic

image of Galois may coincide with the full automorphism group of its ℓ-adic Tate module.

1.3.2 Main result concerning images of Galois

We resume the notation of §1.2, where J is once again the "generic" hyperelliptic Jacobian over K. The results listed in §1.2 show that G_ℓ has finite index in $\mathrm{GSp}(T_\ell(J))$. However, they do not (except in the case of elliptic curves) provide any bound for G_ℓ in $\mathrm{GSp}(T_\ell(J))$. It is natural to ask exactly how "large" G_ℓ is in $\mathrm{GSp}(T_\ell(J))$. Suppose that k contains all ℓ-power roots of unity, so that $G_\ell \subseteq \mathrm{Sp}(T_\ell(J))$. Then if $\ell \neq 2$, *a priori* it is possible for G_ℓ to coincide with $\mathrm{Sp}(T_\ell(J))$. For $\ell = 2$, we note that the order of the symplectic group over $\mathbb{F}_2$ is given by

$$|\mathrm{Sp}_{2g}(\mathbb{F}_2)| = 2^{g^2}(2^{2g}-1)(2^{2g-2}-1)...(2^2-1) \tag{1.10}$$

(see Chapter III, §6 of [2]). Thus, by Proposition 1.2.1(c), for $d \neq 3, 4, 6$, G_2 cannot coincide with $\mathrm{Sp}(J[2])$.

The image under ρ_2 of $\mathrm{Gal}(\bar{K}/K(J[2]))$ is clearly contained in the kernel $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$ of the obvious reduction map $\mathrm{Sp}(T_2(J)) \to \mathrm{Sp}(J[2])$. Thus, *a priori* the largest possible image of ρ_2 is all of $\mathrm{Sp}(T_2(J)) = \mathrm{SL}(T_2(J))$ if $d = 3$ or $d = 4$ and an extension of S_d by $\Gamma(2)$ if $d \geq 5$. The following result, which is in the author's paper [32] (Theorem 1.1 with the results of §4) and which we prove in Chapter 2, says that the image of ρ_2 is actually "as large as possible" in this sense if $k \subseteq \mathbb{C}$.

Theorem 1.3.5. *With the above notation, assume that k is a subfield of $\mathbb{C}$. Then the image under ρ_2 of $\mathrm{Gal}(\bar{K}/K(J[2])(\mu_2))$ coincides with $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. For any prime $\ell \neq 2$, the image under ρ_ℓ of $\mathrm{Gal}(\bar{K}/K(J[2])(\mu_\ell))$ coincides with $\mathrm{Sp}(T_\ell(J))$.*

Corollary 1.3.6. *With the above notation, assume that k is a subfield of $\mathbb{C}$.*

a) We have

$$|\mathrm{Sp}(T_2(J)) : G_2 \cap \mathrm{Sp}(T_2(J))| = \frac{2^{g^2}(2^{2g}-1)(2^{2g-2}-1)...(2^2-1)}{d!} \tag{1.11}$$

if $d \neq 4$ and $G_2 \supseteq \mathrm{Sp}(T_2(J)) = \mathrm{SL}(T_2(J))$ if $d = 4$.

b) For any choice of $(f_1, f_2, ..., f_d) \in k^d$ such that $f(x) := x^d + \sum_{i=1}^{d} f_i x^{d-i} \in k[x]$ has nonzero discriminant, let J_f/k be the Jacobian of the hyperelliptic curve defined by $y^2 = f(x)$. For each prime ℓ, let $\rho_{\ell,f} : \mathrm{Gal}(\bar{k}/k) \to$

$\mathrm{GSp}(T_\ell(J_f))$ *be the natural* ℓ*-adic Galois representation associated to* J_f*, and let* $G_{\ell,f}$ *denote its image. Then if* $d \neq 4$*, we have*

$$|\mathrm{Sp}(T_2(J_f)) : G_{2,f} \cap \mathrm{Sp}(T_2(J_f))| \geq \frac{2^{g^2}(2^{2g}-1)(2^{2g-2}-1)...(2^2-1)}{d!} \quad (1.12)$$

for all such choices of $(f_1, f_2, ..., f_d)$*, and we have equality in infinitely many cases. If* $\ell \neq 2$*, or if* $\ell = 2$ *and* $d = 4$*, we have* $G_{\ell,f} \supseteq \mathrm{Sp}(T_\ell(J_f))$ *for infinitely many such choices of* $(f_1, f_2, ..., f_d)$*.*

Proof. Part (a) follows directly from the fact that if $d \neq 4$ (resp. if $d = 4$), then $|\bar{G}_2| = d!$ (resp. $|\bar{G}_2| = 6$) and from (1.10). Since we have obtained each Jacobian J_f by assigning elements of k to elementary symmetric functions of the α_i's, it is clear that there is an injection of Galois images $G_{\ell,f} \hookrightarrow G_\ell$ for each prime ℓ, and part (a) implies the inequality in part (b). The fact that equality holds in infinitely many cases follows from applying a suitable form of Hilbert's Irreducibility Theorem given by Proposition 1.3 of [19] and its proof (see also [23]).

□

Chapter 2

Families of Jacobians

The goal of this chapter is to study a family of hyperelliptic Jacobians over $\mathbb{C}$ in order to obtain results concerning the ℓ-adic image of Galois, as well as some 2-power torsion fields associated to the "generic" hyperelliptic Jacobian given in §1.2. We develop the necessary topological background material in §2.1 and §2.2, and use it to prove Theorems 1.3.5 (in §2.3), 1.2.2 (in §2.4), and 1.2.3 (in §2.5) in the case that $k = \mathbb{C}$. Finally, in §2.6, we generalize these results to cases where k is a subfield of $\mathbb{C}$ or where k is any field of characteristic different from 2.

2.1 Topological preliminaries

In this section, we develop some well-known topological constructions involving configuration spaces, braid groups, and mapping class groups, which will be needed for the rest of the chapter.

2.1.1 Configuration spaces and braid groups

For any integer $d \geq 3$, we define Y_d to be the complex manifold $\mathbb{C}^d \setminus \bigcup_{1 \leq i < j \leq d} \Delta_{i,j}$, where each $\Delta_{i,j}$ is the "weak diagonal" subspace of $\mathbb{C}^d$ consisting of points $(z_1, z_2, ..., z_d)$ with $z_i = z_j$. We endow $Y_d \subseteq \mathbb{C}^d$ with the subspace topology and call it the *ordered configuration space* of d-element subsets of $\mathbb{C}$. Each point $(z_1, z_2, ..., z_d) \in Y_d$ may be identified with the ordered d-element subset $\{z_1, z_2, ..., z_d\} \subset \mathbb{C}$.

The symmetric group S_d acts on Y_d by $\sigma \cdot (z_1, z_2, ..., z_d) = (z_{\sigma(1)}, z_{\sigma(2)}, ..., z_{\sigma(d)})$

for any permutation $\sigma \in S_d$. Let $X_d := Y_d/S_d$ be the corresponding quotient space, which we call the *(unordered) configuration space* of d-element subsets of $\mathbb{C}$. Each point in X_d coming from a point $(z_1, z_2, ..., z_d) \in Y_d$ may be identified with the (unordered) d-element subset $\{z_1, z_2, ..., z_d\} \subset \mathbb{C}$. It is easy to see that the quotient map $Y_d \to X_d$ is an unramified cover of degree $d!$.

The fundamental groups of the ordered and unordered configuration spaces are well known and are given in [4]. Fix $T_0 := (0, 1, 2, ..., d-1)$ as a basepoint of Y_d; we denote its image in X_d by T_0 as well. Then the fundamental group $\pi_1(X_d, T_0)$ may be identified with the *braid group on d strands*, denoted B_d. The group B_d is generated by elements $\beta_1, \beta_2, ..., \beta_{d-1}$, where each β_i is the braid wrapping the $(i+1)$th point over the ith point in a semicircle counterclockwise. A full set of relations is given by

$$\begin{aligned} \beta_i\beta_j &= \beta_j\beta_i, & |i-j| \geq 2 \\ \beta_i\beta_{i+1}\beta_i &= \beta_{i+1}\beta_i\beta_{i+1}, & 1 \leq i \leq d-2. \end{aligned} \tag{2.1}$$

There is an obvious surjective homomorphism $B_d \twoheadrightarrow S_d$ given by mapping each braid in B_d to the permutation it induces on the d-element subset corresponding to T_0, or more explicitly, by mapping each generator β_i to the transposition $(i, i+1) \in S_d$. It is clear that the fundamental group of the covering space Y_d of X_d with respect to the basepoint $T_0 \in Y_d$ is canonically identified with the normal subgroup $P_d \lhd B_d = \pi_1(X_d, T_0)$, where P_d is the kernel of the above homomorphism $B_d \twoheadrightarrow S_d$. We call P_d the *pure braid group on d strands*; it consists of all braids in B_d which return each of the points $0, 1, ..., d-1 \in \mathbb{C}$ to their original positions. The group P_d is generated by elements $\{A_{i,j}\}_{1 \leq i < j \leq d}$, where each $A_{i,j}$ is the braid wrapping the jth point in a full circle counterclockwise around the ith point only and passing underneath the points in-between. We have

$$A_{i,j} = \beta_{j-1}\beta_{j-2}...\beta_{i+1}\beta_i^2\beta_{i+1}^{-1}...\beta_{j-2}^{-1}\beta_{j-1}^{-1} \tag{2.2}$$

for $1 \leq i < j \leq d$, and a full set of relations is given in Lemma 1.8.2 of [4].

The following fact is shown in Corollary 1.8.4 of [4] and its proof.

Proposition 2.1.1. *The centers of B_d and P_d are both generated by the element*

$$(\beta_1\beta_2...\beta_{d-1})^d = (A_{1,2})(A_{1,3}A_{2,3})...(A_{1,d}A_{2,d}...A_{d-1,d}),$$

which is of infinite order in $P_d \lhd B_d$.

2.1.2 Mapping class groups

For any $i \geq 0$, let $\mathcal{X}_i$ denote the groups of self-homeomorphisms of the complex plane which fix the subset $\{0, 1, ..., i-1\} \subset \mathbb{C}$; and let $\mathcal{Y}_i \subset \mathcal{X}_i$ denote the subgroup of self-homeomorphisms which fix each element $0, 1, ..., i-1 \in \mathbb{C}$. Note that we have the inclusions of subgroups $\mathcal{Y}_d \subset \mathcal{X}_d \subset \mathcal{X}_0 = \mathcal{Y}_0$; we write $\iota : \mathcal{Y}_d \hookrightarrow \mathcal{Y}_0$ for this composition of inclusions. We endow these groups of homeomorphisms with the compact-open topology and consider them as topological groups. Note that two homeomorphisms f and g are in the same connected component of $\mathcal{X}_0 = \mathcal{Y}_0$ if and only if there is a continuous transformation $H : [0,1] \times \mathbb{C} \to \mathbb{C}$ such that for all $t \in [0,1]$, $H(t, \cdot)$ is a homeomorphism $\mathbb{C} \to \mathbb{C}$ and with $H(0, \cdot) = f$ and $H(1, \cdot) = g$; furthermore, f and g are in the same connected component of $\mathcal{X}_d$ or $\mathcal{Y}_d$ if and only if H can be chosen such that for all $t \in [0,1]$ and $z = 0, 1, ..., d-2, \infty$, $H(t, z) = f(z) = g(z)$.

The *(full) mapping class group (of the plane)* $\pi_0(\mathcal{X}_d, \mathrm{id})$ (resp. the *pure mapping class group (of the plane)* $\pi_0(\mathcal{Y}_d, \mathrm{id})$) is the quotient of the topological group $\mathcal{X}_d$ (resp. $\mathcal{Y}_d$) modulo the path component of the identity id. We will use the abbreviated notations $\pi_0\mathcal{X}_d$ and $\pi_0\mathcal{Y}_d$ for the full and pure mapping class groups respectively. Note that since the ordered configuration space Y_d is path connected, $\pi_0 Y_d := \pi_0(Y_d, T_0)$ is a singleton set and may be identified with the trivial group 1.

Let $\epsilon : \mathcal{Y}_0 \to Y_d$ be the *evaluation map* defined by sending any homeomorphism $f \in \mathcal{Y}_d$ to $(f(0), f(1), ..., f(d-1)) \in Y_d$. Clearly, the inverse image of $T_0 = (0, 1, ..., d-1) \in Y_d$ under ϵ is $\mathcal{Y}_d$.

Proposition 2.1.2. *The evaluation map $\epsilon : \mathcal{Y}_0 \to Y_d$ is a fibration.*

Proof. In [4], Birman defines the configuration spaces $Y_d(S)$ and the spaces $\mathcal{Y}_0(S)$ of self-homeomorphisms of the Riemann sphere $S := \mathbb{C} \cup \{\infty\}$ analogously to how we have defined them for the complex plane. Similarly, we also have an evaluation map $\epsilon(S) : \mathcal{Y}_0(S) \to Y_d(S)$. Theorem 4.1 of [4] states that this evaluation map is a fibration. Note that Y_d is the subspace of $Y_{d+1}(S)$ consisting of ordered cardinality-$(d+1)$ subsets of S whose last element is ∞; $\mathcal{Y}_0$ is the topological subgroup of $\mathcal{Y}_0(S)$ consisting of homeomorphisms which fix ∞; and ϵ is the restriction of $\epsilon(S)$ to $\mathcal{Y}_0 \subset \mathcal{Y}_0(S)$. The desired statement follows.

□

It follows (see [5], Chapter VII, Theorem 6.7) that ϵ induces a long exact sequence of fundamental groups

$$... \xrightarrow{\iota_*} \pi_1(\mathcal{Y}_0, \mathrm{id}) \xrightarrow{\epsilon_*} \pi_1(Y_d, T_0) \xrightarrow{\partial} \pi_0\mathcal{Y}_d \xrightarrow{\iota_*} \pi_0\mathcal{Y}_0 \xrightarrow{\epsilon_*} \pi_0 Y_d = 1. \tag{2.3}$$

Note that the map $\partial : P_d = \pi_1(Y_d, \mathrm{id}) \to \pi_0\mathcal{Y}_d$ can be described explicitly as follows. Let $\gamma : [0,1] \to Y_d$ be a loop, with $\gamma(0) = \gamma(1) = T_0$, and let $[\gamma] \in P_d$ be the corresponding equivalence class. Then γ lifts to a loop $\tilde{\gamma} : [0,1] \to \mathcal{Y}_d$ with $\tilde{\gamma}(0) = \mathrm{id}$, via the evaluation map $\epsilon : \mathcal{Y}_d \to Y_d$. Note that the self-homeomorphism $\tilde{\gamma}(1) : \mathbb{C} \to \mathbb{C}$ fixes the points $0, 1, ..., d-1$ since $\gamma(1) = (0, 1, ..., d-1)$, so $\tilde{\gamma}(1) \in \mathcal{Y}_d$. Then $\partial([\gamma]) \in \pi_0\mathcal{Y}_d$ is the path component of $\tilde{\gamma}(1)$.

Proposition 2.1.3. *In the long exact sequence above, the image of $\epsilon_* : \pi_1(\mathcal{Y}_0, \mathrm{id}) \to \pi_1(Y_d, T_0) = P_d$ coincides with the center of P_d.*

Proof. The proof is analogous to the proofs of Lemmas 4.2.1 and 4.2.4 of [4]. Choose any element of P_d which is in the image of ϵ_*. Then there is a loop $\Gamma : [0,1] \to \mathcal{Y}_0$ with $\Gamma(0) = \Gamma(1) = \mathrm{id} : \mathbb{C} \to \mathbb{C}$ whose image in $\pi_1(\mathcal{Y}_0, \mathrm{id})$ is mapped to by ϵ_*. By the definition of ϵ, $\epsilon_*(\Gamma)$ is represented by a loop $\gamma : [0,1] \to Y_d$ such that $\gamma(t) = (\Gamma(t)(0), \Gamma(t)(1), ..., \Gamma(t)(d-1)) \in Y_d$ for $t \in [0,1]$. Let $\beta : [0,1] \to Y_d$ be any other loop with $\beta(0) = \beta(1) = T_0 \in Y_d$ and $\beta(t) = (\beta_0(t), \beta_1(t), ..., \beta_{d-1}(t)) \in Y_d$ for some $\beta_i : [0,1] \to \mathbb{C}$. Let $H : [0,1] \times [0,1] \to Y_d$ be the continuous map given by $H(s,t) = (\Gamma(s)(\beta_1(t)), \Gamma(s)(\beta_2(t)), ..., \Gamma(s)(\beta(d-1)(t))) \in Y_d$ for $(s,t) \in [0,1] \times [0,1]$. Since $H(\cdot, 0) = H(\cdot, 1) = \gamma$ and $H(0, \cdot) = H(1, \cdot) = \beta$, H gives a continuous deformation from the concatination of γ with β to the concatination of β with γ. Thus, $[\beta]$ and $[\gamma]$ commute in $P_d = \pi_1(Y_d, T_0)$. Since $[\beta]$ was chosen as an arbitrary element in P_d, it follows that $\mathrm{im}(\epsilon_*)$ is contained in the center of P_d.

To prove the reverse inclusion, note that by Proposition 2.1.1, the center of P_d is generated by the element $(\beta_1\beta_2...\beta_{d-1})^d$. Since $\mathrm{im}(\epsilon_*) = \ker(\partial)$ by the exactness of the sequence in (2.3), it therefore suffices to show that $(\beta_1\beta_2...\beta_{d-1})^d$ is in the kernel of ∂. The braid $(\beta_1\beta_2...\beta_{d-1})^d$ can be represented by the loop $\gamma : [0,1] \to Y_d$ given by $\gamma(t) = (0, e^{2\pi\sqrt{-1}t}, ..., (d-1)e^{2\pi\sqrt{-1}t}) \in Y_d$ for $t \in [0,1]$. This can be lifted to the loop $\Gamma : [0,1] \to \mathcal{Y}_d$ given by $\Gamma(t)(z) = e^{2\pi\sqrt{-1}t}z$ for $t \in [0,1]$ and $z \in \mathbb{C}$. Since $\Gamma(0) = \Gamma(1) = \mathrm{id}$, it follows from the explicit description of ∂ given above that $\partial((\beta_1\beta_2...\beta_{d-1})^d) = 1$.

□

Proposition 2.1.4. *The mapping class group $\pi_0\mathcal{Y}_0$ is trivial.*

Proof. Since $\mathbb{C}$ is the Riemann sphere with one point removed, this is given in the statement of Theorem 4.4 of [4].

□

Corollary 2.1.5. *The map $\partial : P_d \to \pi_0\mathcal{Y}_d$ is a surjection whose kernel coincides with the central cyclic subgroup generated by $(\beta_1\beta_2...\beta_{d-1})^d \in P_d$.*

Proof. This follows directly from Propositions 2.1.1, 2.1.3, and 2.1.4, and the fact that the sequence in (2.3) is exact.

□

2.1.3 Dehn twists

Let $\gamma : [0,1] \to \mathbb{C}$ be a simple loop whose image does not contain any of the points $0, 1, ..., d-1 \in \mathbb{C}$; we also write γ for its image in $\mathbb{C}$. The simple loop $\gamma \subset \mathbb{C}$ is homeomorphic to the unit circle $S^1 := \{z \in \mathbb{C} \ : \ |z| = 1\}$, and this homeomorphism can be chosen such that the image of $\gamma(t)$ is $e^{2\pi\sqrt{-1}t} \in S^1$ for $t \in [0,1]$. Take a small tubular neighborhood around γ on $\mathbb{C}$, which is homeomorphic to $S^1 \times [-\varepsilon, \varepsilon]$ for some $\varepsilon > 0$. By abuse of notation, we identify this neighborhood with $S^1 \times [-\varepsilon, \varepsilon]$; the outer edge is $S^1 \times \{\varepsilon\}$, and the inner edge is $S^1 \times \{-\varepsilon\}$. We define the *Dehn twist* $D_\gamma : \mathbb{C} \to \mathbb{C}$ to be the self-homeomorphism of $\mathbb{C}$ which acts as the identity on $\mathbb{C} \setminus S^1 \times [-\varepsilon, \varepsilon]$, and which takes $(e^{2\pi\sqrt{-1}t}, s) \in S^1 \times [-\varepsilon, \varepsilon]$ to $(e^{\pi\sqrt{-1}(t+1-s/\varepsilon)}, s)$. We may visualize D_γ as a self-homeomorphism of $\mathbb{C}$ that keeps the outer edge of the tubular neighborhood fixed while twisting the inner edge one full rotation counterclockwise. Clearly, $D_\gamma \in \mathcal{Y}_d$; we also denote its path component in $\pi_0\mathcal{Y}_d$ by D_γ.

We will now derive formulas for braids in P_d that map to Dehn twists corresponding to certain closed loops on $\mathbb{C}$. For any subset $I \subset \{0, 1, ..., d-1\} \subset \mathbb{C}$, let $\gamma_I : [0,1] \to \mathbb{C}$ be the loop defined as follows. Let $d' \leq d$ be the cardinality of I, and write the elements of I in order from least to greatest as $n_1, n_2, ..., n_{d'}$. For $1 \leq i \leq d'$, choose positive numbers $r_i \in \mathbb{R}$ small enough that the set of balls of radius r_i centered at each n_i is pairwise disjoint. For $1 \leq i \leq d'$, let $\gamma_{I,i} : [0,1] \to \mathbb{C}$ given by $t \mapsto n_i + r_i e^{2\pi\sqrt{-1}t}$; furthermore, let $\gamma'_{I,i} : [0,1] \to \mathbb{C}$ be the path given by $t \mapsto -\sqrt{-1}(1-t) + (n_i + r_i)t$; and let $\gamma''_{I,i} : [0,1] \to \mathbb{C}$ be the loop whose basepoint is $-\sqrt{-1} \in \mathbb{C}$ given by concatinating $\gamma'_{I,i}$, $\gamma_{I,i}$, and $\gamma'^{-1}_{I,i}$. Then γ_I is defined to be the concatination

of the loops $\gamma''_{I,i}$ for i decreasing from d' to 1. It is clear that γ_I can be deformed to a simple counterclockwise loop such that I is contained in the simply connected component of $\mathbb{C} \setminus \gamma_I$ and $\{0, 1, ..., d-1\} \setminus I$ is contained in the other component of $\mathbb{C} \setminus \gamma_I$.

Lemma 2.1.6. *We have the following relations in B_d:*

$$\begin{aligned} A_{i,j+1} &= \beta_j A_{i,j} \beta_j^{-1}, & 1 \leq i < j \leq d-1, \\ A_{i+1,j} &= \beta_i A_{i,j} \beta_i^{-1}, & 1 \leq i < j-1 \leq d-1. \end{aligned} \tag{2.4}$$

Proof. This can be verified directly using (2.2) and the braid relations (2.1). □

Proposition 2.1.7. *Let $I \subset \{0, 1, ..., d-1\}$ be a subset of cardinality $d' \leq d$, and assume all of the above notation. Let*

$$\Sigma_{[d']} = (\beta_1 \beta_2 ... \beta_{d'-1})^{d'} = (A_{1,2})(A_{1,3}A_{2,3})...(A_{1,d'}A_{2,d'}...A_{d'-1,d'}).$$

Then the element $B_I \Sigma_{[d']} B_I^{-1} \in P_d$ is mapped by ∂ to the Dehn twist $D_{\gamma_I} \in \pi_0 \mathcal{Y}_d$, where

$$B_I = (\beta_1 ... \beta_{n_1-1})(\beta_2 ... \beta_{n_2-1})...(\beta_{d'} ... \beta_{n_{d'}-1}).$$

Proof. As above, we identify γ_I with the unit circle S^1; furthermore, we identify the simply connected component of $\mathbb{C} \setminus S^1$ with $\{z \in \mathbb{C} \mid |z| < 1\}$. Taking a sufficiently small $\varepsilon > 0$, we may consider the points n_1, n_2, ... , $n_{d'}$ to lie inside the inner circle of the annulus $S^1 \times \{-\varepsilon, \varepsilon\}$ at the points 0, $\frac{1}{d'}$, ... , $\frac{d'-1}{d'}$ respectively. Let $\tilde{\gamma} : [0, 1] \to \mathcal{Y}_0$ be the path defined as follows: for every $t \in [0, 1]$, $\tilde{\gamma}(t)$ acts on $S^1 \times \{-\varepsilon, \varepsilon\}$ by keeping the outer circle fixed while twisting the inner circle counterclockwise by an angle of $2\pi t$; $\tilde{\gamma}(t)$ acts on $\{z \in \mathbb{C} \mid |z| < 1 - \varepsilon\}$ by rotating counterclockwise by an angle of $2\pi t$; and $\tilde{\gamma}(t)$ acts as the identity on the rest of the plane. Then $\tilde{\gamma}(0) = \mathrm{id}$ and $\tilde{\gamma}(1) = D_{\alpha_I}$. Let $\Sigma_I \in P_d$ be the braid represented by the path that rotates the points 0, $\frac{1}{d'}$, ... , $\frac{d'-1}{d'}$ counterclockwise by an angle of $2\pi t$ for $t \in [0, 1]$. Then it is clear from the description of ∂ given in §2.1.2 that $\partial(\Sigma_I) = D_{\alpha_I}$, so it will suffice to show that $\Sigma_I = B_I \Sigma_{[d']} B_I^{-1}$.

For $2 \leq i \leq d'$, the full rotation of the ith point n_i around the points n_1, n_2, ... , n_{i-1} is given by the braid $A_{n_1,n_{d'}} A_{n_2,n_{d'}} ... A_{n_j,n_{d'}}$. Thus, from the description of Σ_I above, we get that

$$\Sigma_I = (A_{n_1,n_2})(A_{n_1,n_3}A_{n_2,n_3})...(A_{n_1,n_{d'}}A_{n_2,n_{d'}}...A_{n_{d'-1},n_{d'}}). \tag{2.5}$$

The fact that $\Sigma_I = B_I \Sigma_{[d']} B_I^{-1}$ then follows from repeated applications of Lemma 2.1.6.

□

It is also possible to define Dehn twists D_γ for simple loops γ on a compact Riemann surface C in the same manner; here D_γ lies in the group of path components of self-homeomorphisms of C. There is an obvious action of D_γ on the first homology group $H_1(C, \mathbb{Z})$. Let $\omega : H_1(C, \mathbb{Z}) \times H_1(C, \mathbb{Z}) \to \mathbb{Z}$ be the intersection pairing on the homology of C. Then this action can be described by the following proposition (which is Proposition 6.3 of [8]).

Proposition 2.1.8. *Let γ be a simple oriented loop on C, and let $[\gamma]$ be its respective class in $H_1(C, \mathbb{Z})$. Then the Dehn twist D_γ acts on $H_1(C, \mathbb{Z})$ as the transvection with respect to $[\gamma]$, that is, by $b \mapsto b + \omega(b, [\gamma])[\gamma]$ for all $b \in H_1(C, \mathbb{Z})$.*

2.2 A family of hyperelliptic curves over $\mathbb{C}$

We retain the above notation, and fix $d \geq 3$. We will now define several families of one-dimensional varieties over $\mathbb{C}$ whose base spaces are X_d and Y_d. Although their definitions will characterize these families as affine schemes over $\mathbb{C}$, for the entirety of this section, we will consider them as complex manifolds and be concerned only with their topological properties. Using results from §2.1, we will show that an induced symplectic representation factors through a certain mapping class group and prove an important theorem about the image of this representation.

2.2.1 Construction of several families

Let α_1, α_2, ... , α_d be transcendental and independent over $\mathbb{C}$. Then the ordered configuration space Y_d is the affine scheme over $\mathbb{C}$ given by

$$\mathrm{Spec}(\mathbb{C}[\alpha_1, \alpha_2, ..., \alpha_d, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq d}]).$$

More explicitly, we identify each $\mathbb{C}$-point $T = (\alpha_1, \alpha_2, ..., \alpha_d)$ of Y_d with ordered subset $(\alpha_1, \alpha_2, ..., \alpha_d)$ of $\mathbb{C}$.

Let $f_1 := \sum_{i=1}^{d} \alpha_i, ..., f_d := \prod_{i=1}^{d} \alpha_i$ be the elementary symmetric functions of the variables α_i; and let Δ be the discriminant function of these

variables. Then the (unordered) configuration space X_d is the affine scheme over $\mathbb{C}$ given by

$$\mathrm{Spec}(\mathbb{C}[f_1, f_2, ..., f_d, \Delta^{-1}]).$$

More explicitly, we identify each $\mathbb{C}$-point $T = (f_1, f_2, ..., f_d)$ of X_d with the set of roots of the squarefree degree-d polynomial $z^d - f_1 z^{d-1} + ... + (-1)^d f_d \in \mathbb{C}[z]$, which is a d-element subset of $\mathbb{C}$. Accordingly, in what follows, given a $\mathbb{C}$-point T of X_d, we will often use T to denote the corresponding subset of $\mathbb{C}$.

Let $\mathcal{O}_{Y_d}$ (resp. $\mathcal{O}_{X_d}$) denote the coordinate ring of Y_d (resp. of X_d); the covering map $Y_d \to X_d$ induces an injection of rings $\mathcal{O}_{X_d} \hookrightarrow \mathcal{O}_{Y_d}$. Let $F(x) \in \mathcal{O}_{X_d}[x] \subset \mathcal{O}_{Y_d}[x]$ be the degree-d polynomial given by

$$x^d + \sum_{i=1}^{d} (-1)^i f_i x^{d-i} = \prod_{i=1}^{d} (x - \alpha_i).$$

Now let $\mathcal{E}_d \to X_d$ be the affine scheme given by $\mathrm{Spec}(\mathcal{O}_{X_d}[x, F(x)^{-1}])$, and let $\tilde{\mathcal{E}}_d \to X_d$ be the affine scheme given by $\mathrm{Spec}(\mathcal{O}_{X_d}[x, y]/(y^2 - F(x))[F(x)^{-1}])$. Then, as a complex manifold, $\mathcal{E}_d \to X_d$ is the family whose fiber over each $\mathbb{C}$-point T of X_d can be identified with $\mathbb{C} \setminus T$. Meanwhile, $\tilde{\mathcal{E}}_d$ is a degree-2 cover of $\mathcal{E}_d$ whose fiber over each T is the curve given by $y^2 = \prod_{z \in T}(x - z)$ minus the branch points $\{(z, 0)\}_{z \in T}$.

We now define a scheme $C_d \to X_d$ with smooth, projective fibers similarly to how we defined C in §1.1.1. Let $\mathcal{C}'_d$ be the affine scheme given by $\mathrm{Spec}(\mathcal{O}_{X_d}[x, y]/(y^2 - F(x)))$. Let $\mathcal{C}''_d$ be the affine scheme over X_d defined by the equation

$$y'^2 = x'(1 + \sum_{i=1}^{d} (-1)^i f_i x'^i) = x' \prod_{i=1}^{d} (1 - \alpha_i x') \tag{2.6}$$

if d is odd, and by the equation

$$y'^2 = (1 + \sum_{i=1}^{d} (-1)^i f_i x'^i) = \prod_{i=1}^{d} (1 - \alpha_i x') \tag{2.7}$$

if d is even. We glue the open subset of $\mathcal{C}'_d$ defined by $x \neq 0$ to the open subset of $\mathcal{C}''_d$ defined by $x' \neq 0$ via the mapping

$$x' \mapsto \frac{1}{x},\ y' \mapsto \frac{y}{x^{\lfloor (d+1)/2 \rfloor}},$$

and denote the resulting scheme by $\mathcal{C}_d \to X_d$. The fiber of $\mathcal{C}_d$ of each $\mathbb{C}$-point T of X_d is a smooth, projective model of the hyperelliptic curve defined by $y^2 = \prod_{z \in T}(x - z)$ of genus $g := \lfloor (d-1)/2 \rfloor$. If d is odd, $\mathcal{C}_d$ has one "section at infinity" given by $(x', y') = (0, 0) \in \mathcal{C}_d''$; if d is even, $\mathcal{C}_d$ has two "sections at infinity" given by $(x', y') = (0, \pm 1) \in \mathcal{C}_d''$. There is an obvious inclusion $\tilde{\mathcal{E}}_d \hookrightarrow \mathcal{C}_d$; if d is odd (resp. if d is even), $\tilde{\mathcal{E}}_d$ is just $\mathcal{C}_d$ with $d+1$ (resp. $d+2$) sections removed.

By slight abuse of notation, we also denote the pullback of $\mathcal{E}_d \to X_d$ induced by $Y_d \to X_d$ by $\mathcal{E}_d \to Y_d$, and denote the pullbacks of $\tilde{\mathcal{E}}_d$ and $\mathcal{C}_d$ similarly. Note that $\mathcal{E}_d \to Y_d$ may be identified with the map $Y_{d+1} \to Y_d$ defined by projecting onto the first d coordinates of each $\mathbb{C}$-point in Y_{d+1}.

2.2.2 The induced monodromy representation

From now on, wherever possible, we will simplify notation by suppressing the subscript d from X_d, Y_d, $\mathcal{E}_d$, $\tilde{\mathcal{E}}_d$, and $\mathcal{C}_d$.

Proposition 2.2.1. *The families $\mathcal{E}$, $\tilde{\mathcal{E}}$, and $\mathcal{C}$ are fiber bundles over Y, and hence over X.*

Proof. As noted above, we may view the family $\mathcal{E} \to Y$ as the family $Y_{d+1} \to Y_d$, which is a fiber bundle according to Theorem 3 of [7]. The fact that $\tilde{\mathcal{E}}$ and $\mathcal{C}$ are also fiber bundles follows from viewing $\tilde{\mathcal{E}}$ as a cover of $\mathcal{E}$ and $\mathcal{C}$ as $\tilde{\mathcal{E}}$ with d sections added.

□

We define a section s of $\mathcal{E} \to X$ by

$$s : T \mapsto \max_{z \in T}(|z|) + 1 \in \mathbb{C} \setminus T = X_T.$$

This may be lifted to a section of $\tilde{\mathcal{E}} \to X$ and hence also of $\mathcal{C} \to X$; we fix a particular choice of lifting $\tilde{s} : X \to \tilde{\mathcal{E}} \hookrightarrow \mathcal{C}$. If d is odd, let $\underline{\infty} : X_d \to \mathcal{C}$ be the section taking each T to the point $(x', y') = (0, 0) \in \mathcal{C}_T''$; then it is clear that $\tilde{s}$ can be continuously deformed to $\underline{\infty}$. If d is even, let $\underline{\infty} : X_d \to \mathcal{C}$ be the section taking each T to the point $(x', y') = (0, 1) \in \mathcal{C}_T''$; then we assume without loss of generality that $\tilde{s}$ can be continuously deformed to $\underline{\infty}$.

As in §2.1, we fix $T_0 := (0, 1, ..., d-1)$ as a basepoint of Y; denote its image in X also by T_0. Let $P_0 = s(T_0) = d \in \mathcal{E}_{T_0}$ and $\infty_{T_0} = \underline{\infty}(T_0) \in \mathcal{C}(T_0)$.

It is shown in [7] that Y (and thus also X) has trivial ith homotopy groups for $i \geq 2$. Therefore, since $\mathcal{E} \to Y$ is a fibration by Proposition 2.2.1, the induced long exact sequence of homotopy can be truncated to the short exact sequence

$$1 \to \pi_1(\mathbb{C} \setminus T_0, P_0) \to \pi_1(\mathcal{E}, P_0) \to \pi_1(X, T_0) \to 1. \tag{2.8}$$

The section $s : X \to \mathcal{E}$ induces a homomorphism $s_* : \pi_1(X, T_0) \to \pi_1(\mathcal{E}, P_0)$ which splits the above sequence. This splitting induces a monodromy action of $\pi_1(X, T_0)$ on $\pi_1(\mathbb{C}\setminus T_0, P_0)$ given by $\sigma \in \pi_1(X, T_0)$ acting as conjugation by $s_*(\sigma)$ on $\pi_1(\mathbb{C}\setminus T_0, P_0) \lhd \pi_1(\mathcal{E}, P_0)$. This lifts to an action of $\pi_1(X, T_0) = B_d$ on $\pi_1(\mathcal{C}_{T_0}, \infty_{T_0})$, which is in fact the monodromy action induced by the splitting of the short exact sequence

$$1 \to \pi_1(\mathcal{C}_{T_0}, \infty_{T_0}) \to \pi_1(\mathcal{C}, \infty_{T_0}) \to \pi_1(X, T_0) \to 1 \tag{2.9}$$

by $\underline{\infty}_* : \pi_1(X, T_0) \to \pi_1(\mathcal{C}, \infty_{T_0})$. In turn, this induces an action of B_d on the abelianization $\pi_1(\mathcal{C}_{T_0}, \infty_{T_0})^{\mathrm{ab}}$, which is the homology group $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$. We denote this action by

$$R : B_d \cong \pi_1(X, T_0) \to \mathrm{Aut}(H_1(\mathcal{C}_{T_0}, \mathbb{Z})). \tag{2.10}$$

This action respects the intersection pairing of $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$, so the image of R is actually contained in the corresponding subgroup of symplectic automorphisms $\mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$. This is the monodromy representation that we will be investigating for the rest of §2.2.

2.2.3 Relationship to the mapping class group

For this subsection, we will only be considering the representation R restricted to $P_d \lhd B_d$; we denote this restriction also by $R : P_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$. We now want to show that the representation R always factors through a particular mapping class group (Proposition 2.2.3). To this end, we first give a useful fact regarding hyperelliptic curves of genus g as 2-sheeted covers of the projective line, and then define some auxiliary representations which we will need to state Proposition 2.2.3.

Proposition 2.2.2. *Let C and C' be hyperelliptic curves of genus g; let $x : C \to \mathbb{P}^1_{\mathbb{C}}$, $x' : C' \to \mathbb{P}^1_{\mathbb{C}}$ be degree-2 ramified covering maps to the projective line; and let $B, B' \subset \mathbb{C}$ be the respective sets of $2g+2$ branch points of these*

coverings. Then every self-homeomorphism $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ which sends B to B' lifts to a homeomorphism $\tilde{f} : C \to C'$. In particular, if f fixes the subset B, then f lifts to a self-homeomorphism $\tilde{f} : C \to C$ which is unique up to deck transformation of $C \to \mathbb{P}^1_{\mathbb{C}}$.

Proof. Choose a basepoint $P_0 \in \mathbb{P}^1_{\mathbb{C}} \setminus B$, and choose $Q_0 \in C$ and $Q'_0 \in C'$ such that $x(Q_0) = P_0$ and $x'(Q'_0) = f(P_0)$. It follows from the lifting theorem (Theorem 4.1 of [5]) that the composition of maps $C \setminus x^{-1}(B) \xrightarrow{x} \mathbb{P}^1_{\mathbb{C}} \setminus B \xrightarrow{f} \mathbb{P}^1_{\mathbb{C}} \setminus B'$ lifts uniquely to a map $C \setminus x^{-1}(B) \to C' \setminus x'^{-1}(B')$ which sends Q_0 to Q'_0. Clearly this can be extended to a map $\tilde{f} : C \to C'$. By applying the same argument to f^{-1}, we see that $\tilde{f}$ is a homeomorphism. In the case that $C = C'$, note that there are two choices of basepoint Q'_0 of $C \setminus B$ such that the unique liftings obtained by choosing each one differ by a deck transformation. □

We define an action of the mapping class group $\pi_0\mathcal{Y}_d$ on $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$, which we will denote by $\varphi : \pi_0\mathcal{Y}_d \to \mathrm{Aut}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$, as follows. Choose an element of $\pi_0\mathcal{Y}_d$ and let f be a self-homeomorphism of $\mathbb{C}$ which represents it; we can extend f to a self-homeomorphism of the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$ which fixes ∞. Then by Proposition 2.2.2, $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ lifts to a unique self-homeomorphism $\tilde{f} : \mathcal{C}_{T_0} \to \mathcal{C}_{T_0}$ which fixes each of the 2 points of $\mathcal{C}_{T_0}$ which map to the basepoint $P_0 = d \in \mathbb{C} \setminus T_0 \subset S$ under the ramified covering map $\mathcal{C}_{T_0} \to \mathbb{P}^1_{\mathbb{C}}$. Define $\varphi([f])$ to be the automorphism $\tilde{f}_* \in \mathrm{Aut}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ induced by $\tilde{f}$.

If $d = 2g+1$, fix a self-homeomorphism of $\mathbb{P}^1_{\mathbb{C}}$ that fixes $0, 1, ..., d-1 \in \mathbb{P}^1_{\mathbb{C}}$ and sends ∞ to d. By Proposition 2.2.2, this lifts to a homeomorphism mapping $\mathcal{C}_{T_0}$ onto a hyperelliptic curve C' ramified over the points $(0, 1, ..., d)$, which is the fiber of $\mathcal{C}_{d+1}$ over the basepoint $T_0 = (0, 1, ..., d) \in \mathcal{Y}_{d+1}$. This homeomorphism yeilds an isomorphism $H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \xrightarrow{\sim} H_1(C', \mathbb{Z})$. Via this isomorphism, the action of P_{d+1} on $H_1(C', \mathbb{Z})$ defined in §2.2.2 yeilds an action of P_{d+1} on $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$ which we denote by $R' : P_{d+1} \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$.

Proposition 2.2.3. *Assume all of the above notation.*

a) If $d = 2g + 2$, then the representation $R : P_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ factors through $\pi_0\mathcal{Y}_d$ as the composition $\varphi \circ \partial$.

b) If $d = 2g + 1$, then the representation $R : P_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ factors through $R' : P_{d+1} \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ via the obvious inclusion $P_d \hookrightarrow P_{d+1}$; thus, by the statement of (a), R factors through $\partial : P_{d+1} \to \pi_0\mathcal{Y}_{d+1}$.

Proof. The main statement of part (b) is obvious from the construction of R' above, and so it will suffice to prove part (a).

Assume that $d = 2g+2$. Define $\mathcal{E}' \to X$ to be the quasiprojective scheme containing $\mathcal{E} \to X$ such that the fiber over each $\mathbb{C}$-point of X is $\mathbb{P}^1_{\mathbb{C}} \setminus T$; again, we also denote its pullback via $Y \to X$ by $\mathcal{E}' \to Y$. Let $\underline{\infty}$ denote the section of $\mathcal{E}' \to Y$ which takes each point in Y to ∞ in the fiber. Note that there is an obvious inclusion $\mathcal{E} \hookrightarrow \mathcal{E}'$ and a continuous deformation of $s : Y \to \mathcal{E}$ to $\underline{\infty} : Y \to \mathcal{E}'$. In fact, $R : P_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ is induced by the monodromy representation arising from the splitting of the analogous short exact sequence associated to $\mathcal{E}' \to Y$ via the section $\underline{\infty}$.

Note that the action of $\mathbb{C} \times \mathbb{C}^\times$ on $\mathbb{C}$ by $(a, b) \cdot z = a + bz$ induces an action of $\mathbb{C} \times \mathbb{C}^\times$ on Y (i.e. action by translation and homothety). Let $\bar{Y}$ be the quotient of Y by this action, and denote the quotient map by $\psi : Y \to \bar{Y}$. Then each element of $\bar{Y}$ can be uniquely represented by an ordered d-element subset of $\mathbb{C}$ whose first element is 0 and whose second element is 1, so we consider each element of $\bar{Y}$ to be an ordered subset of the form $(0, 1, z_3, ..., z_d)$. We also define the family $\bar{\mathcal{E}}' \to \bar{Y}$ to be the quotient of $\mathcal{E}'$ by this action. The section $\underline{\infty}$ of $\mathcal{E}' \to Y$ modulo this action is clearly a section of the family $\bar{\mathcal{E}}' \to \bar{Y}$ which we also denote by $\underline{\infty}$. In fact, $\underline{\infty} : \bar{Y} \to \bar{\mathcal{E}}'$ similarly sends each point in $\bar{Y}$ to ∞ in the fiber. It is clear that $\mathcal{E}' \to Y$ is the pullback of $\bar{\mathcal{E}}' \to \bar{Y}$ via the quotient map $\psi : Y \to \bar{Y}$. It then follows from the functoriality of the fundamental group that the induced monodromy action of P_d on $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus T_0, \infty)$ factors through the induced homomorphism of fundamental groups $\psi_* : P_d \to \bar{P}_d := \pi_1(\bar{Y}, T_0)$.

We observe that each element of $\bar{P}_d$ is the image of a braid in P_d which fixes the points 0 and 1; thus, the homomorphism ψ_* is surjective. We now furnish an isomorphism $\bar{\partial} : \bar{P}_d \xrightarrow{\sim} \pi_0\mathcal{Y}$ such that $\partial = \bar{\partial} \circ \psi_*$. Let $\bar{\mathcal{Y}}_0$ denote the group of self-homeomorphisms of $\mathbb{C}$ which fix 0 and 1, and let $\tilde{\psi} : \mathcal{Y}_0 \to \bar{\mathcal{Y}}_0$ be the homomorphism which sends an element $f \in \mathcal{Y}_0$ to the composition of f with the unique element in $\mathbb{C} \times \mathbb{C}^\times$ which sends $f(0)$ to 0 and $f(1)$ to 1. We have an evaluation map $\bar{\epsilon} : \bar{\mathcal{Y}}_0 \to \bar{Y}$ defined analogously to $\epsilon : \mathcal{Y}_0 \to Y$ in §2.1.2. Since $\bar{\mathcal{Y}}_0 \to \bar{Y}$ is actually a subfamily of $\mathcal{Y}_0 \to Y$, it is also a fibration. It is easy to check that the diagram below commutes.

$$\begin{array}{ccc} \mathcal{Y}_0 & \xrightarrow[\epsilon]{} & Y \\ \downarrow{\scriptstyle \tilde{\psi}} & & \downarrow{\scriptstyle \psi} \\ \bar{\mathcal{Y}}_0 & \xrightarrow[\bar{\epsilon}]{} & \bar{Y} \end{array} \tag{2.11}$$

Now we define a map $\bar{\partial} : \bar{P}_d \to \pi_0\mathcal{Y}$ by a construction analogous to that of $\partial : P_d \to \pi_0\mathcal{Y}$ in §2.1.2, as follows. Let γ be a loop in $\bar{Y}$ representing an

element of $\bar{P}_d$. Then we may lift it to a loop $\tilde{\gamma} : [0,1] \to \bar{\mathcal{Y}}_0$ with $\tilde{\gamma}(0) = \mathrm{id}$ and $\tilde{\gamma}(1) \in \mathcal{Y}$. Let $\bar{\partial}([\gamma])$ be the element of $\pi_0\mathcal{Y}$ represented by $\tilde{\gamma}(1)$. It follows from the commutativity of the diagram in (2.11) that $\partial = \bar{\partial} \circ \psi_*$. Thus, the kernel of ψ_* is contained in the kernel of ∂, which by Proposition 2.1.5 is generated by the element $(\beta_1\beta_2...\beta_{d-1})^d \in P_d$. This braid may be represented by the loop $\gamma : [0,1] \to Y$ defined by $\gamma(t) = (0, e^{2\pi\sqrt{-1}t}, ..., (d-1)e^{2\pi\sqrt{-1}t}) \in Y$ for $t \in [0,1]$, which can be lifted to $\tilde{\gamma} : [0,1] \to \mathcal{Y}_0$ defined by $\tilde{\gamma}(t) : z \mapsto e^{2\pi\sqrt{-1}t}z$ for $t \in [0,1]$. But clearly $\tilde{\psi} \circ \tilde{\gamma}$ is the trivial loop taking all $t \in [0,1]$ to the identity map $\mathrm{id} \in \bar{\mathcal{Y}}_0$, so $\bar{\epsilon} \circ \tilde{\psi} \circ \tilde{\gamma}$ is the trivial loop on $\bar{Y}$. Therefore, $(\beta_1\beta_2...\beta_{d-1})^d \in P_d$ is also in the kernel of ψ_*. Thus, $\bar{\partial}$ is an isomorphism, and R factors through $\partial : P_d \to \pi_0\mathcal{Y}_d$.

Next one can check by direct observation that the generators $A_{i,j} \in P_d$ each act on any loop on $\mathbb{C} \setminus T_0$ in the same way that the Dehn twist D_{γ_I} acts on it, letting $I = \{i-1, j-1\}$ and using the notation of §2.1.3. By Proposition 2.1.7, $\partial(A_{i,j}) = D_{\gamma_I}$. It then follows from the construction of $\varphi : \pi_0\mathcal{Y} \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ above that $R = \varphi \circ \partial$, and part (a) is proved.

□

2.2.4 Image of the monodromy representation

We now state and prove a key result which gives the image of P_d under R. This has been proved by A'Campo in [1] using root spaces and by J.-K. Yu in [33] by an elementary calculation. A similar statement was proved by Mumford in [18] for a representation whose image lies in $\mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))/\{\pm 1\}$; we give a variant of this proof for our representation R, since the main set-up for it has already been developed.

Theorem 2.2.4. *The image of $R : P_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ coincides with the level-2 principal congruence subgroup $\Gamma(2) \lhd \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$.*

Proof. For any element $a \in H_1(\mathcal{C}_{T_0}, \mathbb{Z})$, let $T_a \in \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ denote the transvection defined by $b \mapsto b + \omega(b,a)a$ for all $b \in H_1(\mathcal{C}_{T_0}, \mathbb{Z})$, where ω is the intersection pairing.

First observe that if $I \subseteq \{0, 1, ..., d-1\}$ has even cardinality, then the loop γ_I on $\mathbb{C} \setminus T_0$ lifts to two disjoint loops γ_1 and γ_2 on $\tilde{\mathcal{E}}_{T_0}$ and hence on $\mathcal{C}_{T_0}$, and that $[\gamma_1] = -[\gamma_2]$ in $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$. Moreover, the Dehn twist D_{γ_I} on $\mathbb{C} \setminus T_0$ lifts to the composition of Dehn twists $D_{[\gamma_1]} \circ D_{[\gamma_2]} = D_{[\gamma_2]} \circ D_{[\gamma_1]} = D^2_{[\gamma_1]}$ on $\mathcal{C}_{T_0}$, which fixes the points in the inverse image of the basepoint of $\mathbb{C} \setminus T_0$.

To show that $R(P_d) \subseteq \Gamma(2)$, note that it then follows from Propositions 2.1.7 and 2.1.8 and from the constrution of φ that for $1 \leq i < j \leq d$, $\varphi(A_{i,j})$ is the square of a transvection on $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$ and therefore lies in $\Gamma(2)$. Since $\{A_{i,j}\}_{1 \leq i < j \leq d}$ generates P_d, we obtain the desired inclusion.

To show the reverse inclusion, we make the following observations. For $1 \leq i \leq g := \lfloor (d-1)/2 \rfloor$, let $a_i \in H_1(\mathcal{C}_{T_0}, \mathbb{Z})$ (resp. $b_i \in H_1(\mathcal{C}_{T_0}, \mathbb{Z})$) be the class of oriented loops which map to the counterclockwise-oriented loop γ_I for $I = \{2i-1, 2i\}$ (resp. $I = \{2i, ..., 2g+1\}$). Then $\{a_i, b_i\}_{i=1}^g$ is a symplectic basis for $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$. Moreover, γ_I for $I = \{2i-1, ..., 2j\}$ (resp. $I = \{2i, ..., 2j-1\}$, resp. $I = \{2i-1, 2i, 2j, ..., 2g+1\}$, resp. $I = \{2i, ..., 2j-2, 2j+1, ..., 2g+1\}$, resp. $I = \{2i-1, 2i+1, ..., 2g+1\}$) lifts to two disjoint loops on $\mathcal{C}_{T_0}$, one of whose classes in $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$ is $a_i + a_j$ (resp. $b_i - b_j$, resp. $a_i + b_j$, resp. $b_i - a_j$, resp. $b_i - a_i$) for $1 \leq i < j \leq g$. So by applying Proposition 2.1.7 and 2.1.8, it follows that there are elements in $P_{2g+1} \subset P_{2g+2}$ which are mapped by $\partial : P_{2g+2} \to \pi_0 \mathcal{Y}_{2g+2}$ to Dehn twists, which in turn are mapped by φ to the squares of transvections $T_{a_i}^2, T_{b_i}^2, T_{a_i+a_j}^2, T_{b_i-b_j}^2, T_{a_i+b_j}^2, T_{b_i-a_j}^2, T_{b_i-a_i}^2 \in \Gamma(2)$ for $1 \leq i < j \leq g$. But it is a consequence of Propositions A.1 and A.3(b) of [17] that these squares of transvections generate all of $\Gamma(2)$. Therefore, for $d = 2g+2$, the inclusion $\Gamma(2) \subseteq R(P_d)$ follows from part (a) of Proposition 2.2.3; then for $d = 2g+1$, $\Gamma(2) \subseteq R(P_d)$ follows from part (b) of Proposition 2.2.3. Thus, $R(P_d) = \Gamma(2)$. □

2.3 Generic image of Galois

Let $\alpha_1, \alpha_2, ..., \alpha_d$ be transcendental and independent over $\mathbb{C}$, and let L be the subfield of $\mathbb{C}(\{\alpha_i\}_{1 \leq i \leq d})$ generated over $\mathbb{C}$ by the symmetric functions of the α_i's. Let C be a smooth projective model of the hyperelliptic curve over L given by

$$y^2 = \prod_{i=1}^{d} (x - \alpha_i), \tag{2.12}$$

and let J be its Jacobian. Note that C is defined over L and has genus $g := \lfloor (d-1)/2 \rfloor$, while J is an abelian variety over L of dimension g. For each $n \geq 0$, let $L_n = L(J[2^n])$ denote the extension of L over which the 2^n-torsion of J is defined; note that $L_1 = \mathbb{C}(\{\alpha_i\}_{1 \leq i \leq d})$ for all $d \neq 4$.

Fix an algebraic closure $\bar{L}$ of L, and write G_L for the absolute Galois group

$\mathrm{Gal}(\bar{L}/L)$. As in Chapter 1, we denote the ℓ-adic Tate module of J by $T_\ell(J)$, and denote the natural Galois action on $T_\ell(J)$ by $\rho_\ell : G_L \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J))$. Since L contains all 2-power roots of unity, the Weil pairing on $T_\ell(J)$ is Galois invariant, and so the image of G_L under ρ_ℓ is contained in $\mathrm{Sp}(T_\ell(J))$, the group of symplectic automorphisms with respect to the Weil pairing. For each prime ℓ and integer $n \geq 0$, write $\Gamma(\ell^n)$ for the principal level-ℓ^n congruence subgroup of $\mathrm{Sp}(T_\ell(J))$.

The main theorem is the following.

Theorem 2.3.1. *With the above notation, the image under ρ_2 of the Galois subgroup fixing L_1 coincides with $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. For $\ell \neq 2$, the image under ρ_ℓ of the Galois subgroup fixing L_1 coincides with $\mathrm{Sp}(T_\ell(J))$.*

2.3.1 Proof of the main theorem

This subsection is devoted to proving Theorem 2.3.1 by converting the topological result in Theorem 2.2.4 into an arithmetic statement. Lemma 2.3.2 below is the key result that allows us to do this.

Let $\widehat{B}_d$ denote the profinite completion of $B_d \cong \pi_1(X, T_0)$. Since X may be viewed as a scheme over the complex numbers, Riemann's Existence Theorem yields an isomorphism between its étale fundamental group $\pi_1^{\acute{e}t}(X, T_0)$ and $\widehat{B}_d$ ([10], Exposé XII, Corollaire 5.2). Meanwhile, the function field of X is L, so $\pi_1^{\acute{e}t}(X, T_0)$ is isomorphic to the Galois group $\mathrm{Gal}(L^{\mathrm{unr}}/L)$, where L^{unr} is the maximal extension of L unramified at all points of X. The representation $R : B_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ induces a homomorphism of profinite groups

$$R : \mathrm{Gal}(L^{\mathrm{unr}}/L) = \widehat{B}_d \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell) \tag{2.13}$$

for any prime ℓ. Composing this map with the restriction homomorphism $G_L := \mathrm{Gal}(\bar{L}/L) \twoheadrightarrow \mathrm{Gal}(L^{\mathrm{unr}}/L)$ yields a map which we denote $R_\ell : G_L \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell)$.

Lemma 2.3.2. *Assume the above notation, and let ℓ be any prime. Then there is an isomorphism of $\mathbb{Z}_\ell$-modules $T_\ell(J) \xrightarrow{\sim} H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$ making the representations ρ_ℓ and R_ℓ isomorphic.*

Proof. We proceed in four steps.

Step 1: We switch from (topological) fundamental groups to étale fundamental groups. Since X and $\mathcal{C}$, as well as $\mathcal{C}_T$ for each fiber T of X, can be

viewed as a scheme over the complex numbers, Riemann's Existence Theorem implies that the étale fundamental groups of X, $\mathcal{C}$, and each $\mathcal{C}_T$ (defined using a choice of geometric base point $\bar{T}_0$ 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

$$1 \to \pi_1^{\acute{e}t}(\mathcal{C}_{\bar{T}_0}, \infty_{\bar{T}_0}) \to \pi_1^{\acute{e}t}(\mathcal{C}, \infty_{\bar{T}_0}) \to \pi_1^{\acute{e}t}(X, \bar{T}_0) \to 1, \tag{2.14}$$

which is a short exact sequence by [10], Corollaire X.2.2. Moreover, the section $\underline{\infty} : X \to \mathcal{C}$ similarly gives rise to an action of $\pi_1^{\acute{e}t}(X, \bar{T}_0)$ on $\pi_1^{\acute{e}t}(\mathcal{C}_{T_0}, \infty_{\bar{T}_0})^{\mathrm{ab}}$.

Step 2: We switch from C to its Jacobian. Define $\mathcal{J} \to X$ to be the abelian scheme representing the Picard functor of the scheme $\mathcal{C} \to X$ (see [14], Theorem 8.1). Note that $\mathcal{J}_T$ is the Jacobian of $\mathcal{C}_T$ for each $\mathbb{C}$-point T of X, and the generic fiber of $\mathcal{J}$ is J/L, the Jacobian of C/L. Let $\infty \in C(L)$ be the image of the generic point of X under the map $\underline{\infty}_* : \pi_1^{\acute{e}t}(X, \bar{T}_0) \to \pi_1^{\acute{e}t}(\mathcal{C}, \infty_{\bar{T}_0})$. Let $f_\infty : C \to J$ be the morphism (defined over L) given by sending each point $P \in C(L)$ to the divisor class $[(P) - (\infty)]$ in $\mathrm{Pic}^0_L(C)$, which is identified with $J(L)$. By [14], Proposition 9.1, the induced homomorphism of étale fundamental groups $(f_\infty)_* : \pi_1^{\acute{e}t}(C, \infty) \to \pi_1^{\acute{e}t}(J, 0)$ factors through an isomorphism $\pi_1^{\acute{e}t}(C, \infty)^{\mathrm{ab}} \xrightarrow{\sim} \pi_1^{\acute{e}t}(J, 0)$. This induces an isomorphism $\pi_1^{\acute{e}t}(\bar{\mathcal{C}}_T, \infty_T)^{\mathrm{ab}} \xrightarrow{\sim} \pi_1^{\acute{e}t}(\mathcal{J}_T, 0_T)$ for each $T \in X$. Note that the composition of the section $\bar{s} : X \to \bar{\mathcal{C}}$ with f_∞ is the "zero section" $\underline{0} : X \to \mathcal{J}$ mapping each T to the identity element $0_T \in \mathcal{J}_T$. Thus, the action of $\pi_1^{\acute{e}t}(X, \bar{T}_0)$ on $\pi_1^{\acute{e}t}(\mathcal{C}_{T_0}, \infty_{\bar{T}_0})^{\mathrm{ab}}$ coming from the splitting of (2.14) is the same as the action of $\pi_1^{\acute{e}t}(X, \bar{T}_0)$ on $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ coming from the splitting of

$$1 \to \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0}) \to \pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{T}_0}) \to \pi_1^{\acute{e}t}(X, \bar{T}_0) \to 1 \tag{2.15}$$

induced by the section $\underline{0}_* : \pi_1^{\acute{e}t}(X, \bar{T}_0) \to \pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{T}_0})$.

Step 3: We now show that this action on $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ is isomorphic to a particular Galois action on $\pi_1^{\acute{e}t}(J_{\bar{L}}, 0)$ (and therefore on its ℓ-adic quotient $T_\ell(J)$). Let $\underline{\eta} : \mathrm{Spec}(L) \to X$ denote the generic point of X. Note that we may identify $\pi_1^{\acute{e}t}(L, \bar{L})$ with G_L, and that $\underline{\eta}_* : G_L \twoheadrightarrow \pi_1^{\acute{e}t}(X, \bar{\eta})$ 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 $\underline{0} : \mathrm{Spec}(L) \to J_L$ which induces $\underline{0}_* : G_L = \pi_1^{\acute{e}t}(L, \bar{L}) \to \pi_1^{\acute{e}t}(J_L, 0)$. Let $\bar{T}_0$ and $\bar{\eta}$ be geometric points over T_0 and η respectively. Then we have ([10], Corollaire X.1.4) an exact

sequence of étale fundamental groups

$$\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}}) \to \pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{\eta}}) \to \pi_1^{\acute{e}t}(X, \bar{\eta}) \to 1. \tag{2.16}$$

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

$$\begin{array}{ccccccccc}
 & & & & \overset{\underline{0}_*}{\curvearrowleft} & & & & \\
1 & \longrightarrow & \pi_1^{\acute{e}t}(J_{\bar{L}}, 0) & \longrightarrow & \pi_1^{\acute{e}t}(J_L, 0) & \longrightarrow & \pi_1^{\acute{e}t}(L, \bar{L}) & \longrightarrow & 1 \\
 & & \| & & \downarrow & \overset{\underline{0}_*}{\curvearrowleft} & \downarrow \underline{\eta}_* & & \\
 & & \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}}) & \longrightarrow & \pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{\eta}}) & \longrightarrow & \pi_1^{\acute{e}t}(X, \bar{\eta}) & \longrightarrow & 1 \\
 & & \downarrow \mathrm{sp} & & \downarrow \wr & \overset{\underline{0}_*}{\curvearrowleft} & \downarrow \wr\, \varphi & & \\
1 & \longrightarrow & \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0}) & \longrightarrow & \pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{T}_0}) & \longrightarrow & \pi_1^{\acute{e}t}(X, \bar{T}_0) & \longrightarrow & 1
\end{array}$$

Here the vertical arrow from $\pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{\eta}})$ to $\pi_1^{\acute{e}t}(\mathcal{J}, 0_{\bar{T}_0})$ is a change-of-basepoint isomorphism chosen to make the lower right square commute, and sp : $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}}) \to \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ is the surjective homomorphism induced by a diagram chase on the bottom two horizontal rows. Grothendieck's Specialization Theorem ([10], Corollaire X.3.9) states that sp is an isomorphism, which implies that the second row is also a short exact sequence. Thus, the action of $\pi_1^{\acute{e}t}(X, \bar{T}_0)$ on $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ arising from the splitting of the lower row by $\underline{0}_*$ is isomorphic to the action of $\pi_1^{\acute{e}t}(X, \bar{\eta})$ on $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}})$ arising from the splitting of the middle row by $\underline{0}_*$, via the isomorphism sp : $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}}) \to \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$. In turn, a simple diagram chase confirms that this action, after pre-composing with $\underline{\eta}_* : \pi_1^{\acute{e}t}(L, \bar{L}) \twoheadrightarrow \pi_1^{\acute{e}t}(X, \bar{\eta})$, can be identified with the action of $\pi_1^{\acute{e}t}(L, \bar{L})$ on $\pi_1^{\acute{e}t}(J_{\bar{L}}, 0)$ arising from the splitting of the top row by $\underline{0}_*$. We denote this action by $\tilde{R} : G_L = \pi_1^{\acute{e}t}(L, \bar{L}) \to \mathrm{Aut}(\pi_1^{\acute{e}t}(J_{\bar{L}}, 0))$. Since the Tate module $T_\ell(J)$ may be identified with the maximal pro-ℓ quotient of $\pi_1^{\acute{e}t}(J_{\bar{L}}, 0)$, $\tilde{R}$ induces an action of G_L on $T_\ell(J)$, which we denote by $\tilde{R}_\ell : G_L \to \mathrm{Aut}(T_\ell(J))$. One can identify the symplectic pairing on $\pi_1(\mathcal{J}_{T_0}, 0_{T_0})$ with the Weil pairing on $T_\ell(J)$ via the results in [16], Chapter IV, §24. Therefore, the image of $\tilde{R}_\ell$ is a subgroup of $\mathrm{Sp}(T_\ell(J))$.

By the above construction, we may identify the maximal pro-ℓ quotient of $\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ with $H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$. Note that the isomorphism sp :

$\pi_1^{\acute{e}t}(\mathcal{J}_{\bar{\eta}}, 0_{\bar{\eta}}) \xrightarrow{\sim} \pi_1^{\acute{e}t}(\mathcal{J}_{\bar{T}_0}, 0_{\bar{T}_0})$ induces an isomorphism of their maximal pro-ℓ quotients $\mathrm{sp}_\ell : T_\ell(J) \xrightarrow{\sim} H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$. By construction, the representation $\tilde{R}_\ell$ is isomorphic to the representation R_ℓ via sp_ℓ.

Step 4: It now suffices to show that $\tilde{R}_\ell = \rho_\ell$. To determine $\tilde{R}_\ell$, we are interested in the action of G_L on the group $\mathrm{Aut}_{J_{\bar{L}}}(Z)$ for each ℓ-power-degree covering $Z \to J_{\bar{L}}$. But each such covering is a subcovering of $[\ell^n] : J_{\bar{L}} \to J_{\bar{L}}$, 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 $\underline{0}_* : G_L \to \pi_1^{\acute{e}t}(J_L, 0)$ is induced by the inclusion of the L-point $0 \in J_L$. Thus, for any $\sigma \in G_L$, $\underline{0}_*(\sigma)$ acts on any connected étale cover of J_L via σ acting on the coordinates of the points. Since $\tilde{R}(\sigma)$ is conjugation by $\underline{0}_*(\sigma)$ on $\pi_1^{\acute{e}t}(J_{\bar{L}}, 0) \lhd \pi_1^{\acute{e}t}(J_L, 0)$, one sees that for each n, $\underline{0}_*(\sigma)$ acts on $\{t_P | P \in J[\ell^n]\}$ by sending each t_P to $\sigma^{-1} t_P \sigma = t_{P^\sigma}$. Thus, G_L acts on the Galois group of the covering $[\ell^n] : J_{\bar{L}} \to J_{\bar{L}}$ 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.

□

It is now easy to prove Theorem 2.3.1.

Proof (of Theorem 2.3.1) . Recall that P_d is the normal subgroup of $B_d \cong \pi_1(X, T_0)$ corresponding to the cover $Y \to X$, and that if $d \neq 4$, the function field of Y is L_1. It follows that if $d \neq 4$, the image of $\mathrm{Gal}(\bar{L}/L_1)$ under $\underline{\eta}_*$ is $\widehat{P}_d \lhd \widehat{B}_d \cong \pi_1^{\acute{e}t}(X, \bar{T}_0)$ (where $\widehat{P}_d$ denotes the profinite completion of P_d).

Suppose that $\ell = 2$. Then the statement of Theorem 2.2.4 implies that if $d \neq 4$ (resp. if $d = 4$), the image of $\mathrm{Gal}(\bar{L}/L_1)$ under R_2 coincides with (resp. contains) $\Gamma(2) \lhd \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_2)$. It then follows from Lemma 2.3.2 that if $d \neq 4$ (resp. if $d = 4$), the image of $\mathrm{Gal}(\bar{L}/L_1)$ under ρ_2 coincides with (resp. contains) $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. The containment is an equality in the $d = 4$ case as well since clearly $\rho_2(\mathrm{Gal}(\bar{L}/L_1)) \subseteq \Gamma(2) \lhd \mathrm{Sp}(T_2(J))$.

Now suppose that $\ell \neq 2$. By a suitable form of the strong approximation theorem applied to the algebraic group $\mathrm{Sp}_{2g}(\mathbb{Q})$ (see Theorem 7.12 of [21]), given any element $\alpha_\ell \in \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ and any integer $n \geq 1$, there is an element $\alpha \in \mathrm{Sp}_{2g}(\mathbb{Z})$ which is congruent to 1 modulo 2 and is also congruent to α_ℓ modulo ℓ^n. It follows that $\Gamma(2) \lhd \mathrm{Sp}_{2g}(\mathbb{Z}) \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is dense. Choosing a symplectic basis of the rank-$2g$ $\mathbb{Z}$-module $H_1(\mathcal{C}_{T_0}, \mathbb{Z})$ determines an isomorphism $\mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell) \xrightarrow{\sim} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, and we get that $\Gamma(2) \lhd \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z})) \subset \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell)$ is dense. Thus, since the image of R_ℓ similarly must contain $\Gamma(2) \lhd \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$ and also must be closed in

the ℓ-adic topology by the construction of R_ℓ from R, the restriction of R_ℓ to $\mathrm{Gal}(\bar{L}/L_1)$ is surjective. Then by Lemma 2.3.2, $\rho_2 : \mathrm{Gal}(\bar{L}/L_1) \to \mathrm{Sp}(T_\ell(J))$ is surjective as well.

□

2.3.2 Corollaries and applications

We first give some easy immediate corollaries to Theorem 2.3.1.

Corollary 2.3.3. *Let G_ℓ denote the image under ρ_ℓ of all of G_L. Then we have the following:*

a) We have $G_2 \supset \Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. Moreover, if $d \neq 4$, $G_2/\Gamma(2) \cong S_d$, and if $d = 4$, $G_2/\Gamma(2) \cong S_3$.

b) For each $n \geq 1$, the homomorphism ρ_2 induces an isomorphism

$$\bar{\rho}_2^{(n)} : \mathrm{Gal}(L_n/L_1) \xrightarrow{\sim} \Gamma(2)/\Gamma(2^n)$$

via the restriction map $\mathrm{Gal}(\bar{L}/L_1) \twoheadrightarrow \mathrm{Gal}(L_n/L_1)$.

Proof. If $d \neq 4$ (resp. if $d = 4$), then $\mathrm{Gal}(L_1/L) \cong S_d$ (resp. $\mathrm{Gal}(L_1/L) \cong S_3$), and so part (a) immediately follows from the theorem.

To prove part (b), note that for any $n \geq 0$, the image under ρ_2 of the Galois subgroup fixing the 2^n-torsion points is clearly $G_2 \cap \Gamma(2^n)$. But $G_2 \supset \Gamma(2)$, so for any $n \geq 1$, the image under ρ_2 of $\mathrm{Gal}(\bar{L}/L_n)$ is $\Gamma(2^n)$. Then part (b) immediately follows by the definition of $\bar{\rho}_2^{(n)}$.

□

We also present a proposition which results from constructions used to prove Theorem 2.3.1, and which will be the main tool we use in §2.4 and §2.5 to derive generators for the fields of definition of 4-torsion and 8-torsion respectively.

Proposition 2.3.4. *For $n \geq 1$, the extension L_n/L is the Galois subextension of L^{unr}/L corresponding to the quotient of $\widehat{B}_d \cong \mathrm{Gal}(L^{\mathrm{unr}}/L)$ induced by the subgroup $R^{-1}(\Gamma(2^n)) \lhd B_d$.*

Proof. For $n \geq 1$, let $\mathcal{B}_n$ denote the set of bases of the free $\mathbb{Z}/2^n\mathbb{Z}$-module $J[2^n]$. Then it was shown in the proof of Theorem 2.3.1 that G_L acts on $\mathcal{B}_n$ through a representation isomorphic to $R_2 : \pi_1^{\text{ét}}(X, \bar{T}_0) \to \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_2)$ via an isomorphism $\mathrm{Sp}(T_2(J)) \cong \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_2)$, and the subgroup

fixing all elements of $\mathcal{B}_n$ corresponds to $R_2^{-1}(\Gamma(2^n)) \lhd \pi_1^{\text{ét}}(X, \bar{T}_0)$. Hence, by covering space theory, there is a connected cover $X_{(n)} \to X$ corresponding to an orbit of $\mathcal{B}_n$ 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 $L \hookrightarrow L_n$ of function fields, and the statement follows.

□

Remark 2.3.5. a) The fact that $\rho_\ell : G_L \to \mathrm{Sp}(T_\ell(J))$ must factor through $\mathrm{Gal}(L^{\mathrm{unr}}/L)$ can also be shown using the criterion of Néron-Ogg-Shafarevich ([26], Theorem 1).

b) It follows directly from Proposition 2.3.4 that for each $n \geq 1$, L_n/L_1 is the subextension of L^{unr}/L_1 corresponding to the quotient induced by $R^{-1}(\Gamma(2^n)) \lhd R^{-1}(\Gamma(2))$. Note that if $d \neq 4$, $L_1 = \mathbb{C}(\{\alpha_i\}_{i=1}^d)$, and $R^{-1}(\Gamma(2)) = P_d \lhd B_d$. In the case that $d = 4$, L_1 is the subfield of $L(\{\alpha_i\}_{i=1}^4)$ given in Proposition 1.2.1(c), which in fact is generated over $\mathbb{C}$ by 3 independent transcendental elements. Therefore, if $d = 4$, $R^{-1}(\Gamma(2))$ is a subgroup of B_4 which is isomorphic to P_3 and which contains $P_4 \lhd B_4$.

2.4 Fields of 4-torsion of hyperelliptic Jacobians

We retain all notation used in §2.3. In addition, for this section, we denote by $-1 \in \mathrm{Gal}(L_2/L_1)$ the Galois automorphism mapping to the scalar matrix $-1 \in \Gamma(2)/\Gamma(4)$ via the isomorphism $\bar{\rho}_2^{(2)}$ given by Corollary 2.3.3(b).

In this section, we apply the construction which we developed in §2.3 to give generators of the extension L_2/L obtained by adjoining the 4-torsion points of J/L.

Theorem 2.4.1. *(a) If $d = 2g + 1$, then*

$$L_2 = L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i < j \leq d}), \tag{2.17}$$

and the Galois element $-1 \in \mathrm{Gal}(L_2/L_1)$ acts by changing the sign of each of the generators given above.

(b) If $d = 2g + 2$, then

$$L_2 = L_1(\{\sqrt{\alpha_i - \alpha_j} \prod_{\substack{1 \le l \le d-1 \\ l \ne i,j}} \sqrt{\alpha_l - \alpha_d}\}_{1 \le i < j \le d}), \tag{2.18}$$

and the Galois element $-1 \in \mathrm{Gal}(L_2/L_1)$ acts by changing the sign of each of the generators given above.

We prove the statement for odd d first, in §2.4.1, and then prove the statement for even d in §2.4.2, using some of the lemmas in §2.4.1.

2.4.1 The case of odd degree

We first need some results concerning the structures of the pure braid group P_d and quotients of congruence subgroups of $\mathrm{Sp}(T_2(J))$.

Lemma 2.4.2. *For all integers $d \ge 2$, the abelianization of P_d is isomorphic to $\mathbb{Z}^{d(d-1)/2}$. More explicitly, it is freely generated by the images of the generators $A_{i,j}$ of P_d.*

Proof. This follows by checking that the relations between the $A_{i,j}$'s given in Lemma 1.8.2 of [4] lie in the kernel of the abelianization map.

□

Lemma 2.4.3. *The quotient $\Gamma(2)/\Gamma(4)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$.*

Proof. For $\Gamma(2), \Gamma(4) \lhd \mathrm{Sp}_{2g}(\mathbb{Z})$, this is shown in the proof of Corollary 2.2 of [22]. The statement for $\Gamma(2), \Gamma(4) \lhd \mathrm{Sp}(T_2(J)) \cong \mathrm{Sp}_{2g}(\mathbb{Z}_2)$ follows immediately from this.

□

To simplify notation, we let $\tilde{L} = L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{1 \le i < j \le d})$. The proof of the following lemma is a variation on J.-K. Yu's argument in the proof of Corollary 7.4 in [33].

Lemma 2.4.4. *For $d = 3$ and all $d \ge 5$, $L_2 \subseteq \tilde{L}$. This inclusion is an equality if and only if $d = 2g + 1$.*

Proof. It follows from Lemma 2.4.2 that the maximal abelian quotient of exponent 2 of $\widehat{P}_d$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{d(d-1)/2}$. Thus, $\widehat{P}_d$ has a unique normal subgroup inducing a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{d(d-1)/2}$, and so there is a unique Galois cover of $X_{(1)}$ corresponding to this quotient. The field extension $\tilde{L} \supset L(\{\alpha_i\}_{1\leq i\leq d})$ is unramified away from the hyperplanes defined by $(\alpha_i - \alpha_j)$ with $i \neq j$ and is obtained from L_1 by adjoining $2g^2+g$ independent square roots of elements in $L_1^\times \backslash (L_1^\times)^2$. Furthermore, note that since $d \neq 4$, $L_1 = L(\{\alpha_i\}_{1\leq i\leq d})$. Therefore, $\tilde{L}$ is the function field of the unique maximal Galois cover of $X_{(1)}$ with an abelian Galois group of exponent 2. Now by Proposition 2.3.4, since $d \neq 4$, L_2/L_1 is the subextension of L^{unr}/L_1 corresponding to the quotient induced by $R^{-1}(\Gamma(4)) \lhd R^{-1}(\Gamma(2)) \cong P_d$. Lemma 2.4.3 shows that $\Gamma(2)/\Gamma(4) \cong R^{-1}(\Gamma(2))/R^{-1}(\Gamma(4)) \cong \mathrm{Gal}(L_2/L_1)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$, which is abelian of exponent 2; therefore, $L_2 \subseteq \tilde{L}$. Moreover, $d(d-1)/2 = 2g^2 + g$ if and only if $d = 2g+1$, in which case L_2 itself is the unique maximal Galois extension of L of exponent 2 and so $L_2 = \tilde{L}$.

□

We assume the following notation for the rest of this section. Let $r : \widehat{P}_d \to \Gamma(2) \lhd \mathrm{Sp}(T_2(J))$ be the homomorphism induced from the restriction of the natural Galois representation ρ_2 on $\mathrm{Gal}(\bar{L}/L_1)$, by factoring through $\mathrm{Gal}(L^{\mathrm{unr}}/L(\{\alpha_i\}_{1\leq i\leq d})) \cong \widehat{P}_d$. Let

$$\Sigma = (A_{1,2})(A_{1,3}A_{2,3})...(A_{1,d}A_{2,d}...A_{d-1,d}) \in \widehat{P}_d.$$

Lemma 2.4.5. *With the above notation, if $d = 2g+1$, then $r(\Sigma) = -1 \in \Gamma(2)$.*

Proof. Let $\bar{r}^{(2)} : \widehat{P}_d \to \Gamma(2)/\Gamma(4)$ denote the composition of r with reduction modulo 4. Then since $\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$ by Lemma 2.4.3, $\bar{r}^{(2)}$ factors through the maximal abelian quotient of $\widehat{P}_d$ of exponent 2. As noted above in the proof of Lemma 2.4.4, since $d = 2g+1$, the maximal abelian quotient of $\widehat{P}_d$ of exponent 2 is isomorphic to $\Gamma(2)/\Gamma(4)$, so $\bar{r}^{(2)}$ factors through this isomorphism. It then follows from Lemma 2.4.2 that the element Σ is mapped by $\bar{r}^{(2)}$ to a nontrivial element of $\Gamma(2)/\Gamma(4)$. Thus, $r(\Sigma)$ is a nontrivial element of $\Gamma(2)$. Proposition 2.1.1 says that Σ is in the center of $\widehat{P}_d$, and since r is surjective by Theorem 2.3.1, $r(\Sigma)$ must lie in the center of $\Gamma(2)$. Since the center of any symplectic group consists of scalar matrices and $\Gamma(2)$ is an open

subgroup of a symplectic group, the only nontrivial element in the center of $\Gamma(2)$ is the scalar matrix -1. Thus, $r(\Sigma) = -1$.

□

Lemma 2.4.6. *Assume $d \neq 4$. For $1 \leq i < j \leq d$, the restriction of the Galois element $A_{i,j} \in \widehat{P}_d \cong \mathrm{Gal}(L^{\mathrm{unr}}/L_1)$ to $\tilde{L}$ acts by sending $\sqrt{\alpha_i - \alpha_j}$ to $-\sqrt{\alpha_i - \alpha_j}$ and fixing all other generators.*

Proof. Fix (i, j) such that $1 \leq i < j \leq d$, and let $\tilde{L}_{i,j}$ be the subfield of $\tilde{L}$ fixed by the subgroup of $\mathrm{Gal}(\tilde{L}/L_1)$ generated by the images of all $A_{i',j'}$ for $(i', j') \neq (i, j)$. Clearly $\tilde{L}_{i,j}$ is a quadratic extension of $L_1 = L(\{\alpha_i\}_{i=1}^d)$. By considering the action of $A_{i,j}$ on Y_d locally around the hyperplane given by $\alpha_i = \alpha_j$ and localizing L_1 at the prime $(\alpha_i - \alpha_j)$, it is clear that $\tilde{L}_{i,j}/L_1$ is ramified at the prime $(\alpha_i - \alpha_j)$. Therefore $\tilde{L}_{i,j} = L(\{\alpha_i\}_{i=1}^d, \sqrt{\alpha_i - \alpha_j})$, and the restriction of $A_{i,j}$ to $\tilde{L}_{i,j}$ acts by $\sqrt{\alpha_i - \alpha_j} \mapsto -\sqrt{\alpha_i - \alpha_j}$. The claim easily follows by considering $\tilde{L}$ as the compositum of all $\tilde{L}_{i,j}$ for $1 \leq i < j \leq d$.

□

The following proposition, along with the second statement in Lemma 2.4.4, gives the statement of Theorem 2.4.1(a).

Proposition 2.4.7. *If $d = 2g+1$, the Galois element $-1 \in \mathrm{Gal}(L_2/L_1)$ acts by sending $\sqrt{\alpha_i - \alpha_j}$ to $-\sqrt{\alpha_i - \alpha_j}$ for $1 \leq i < j \leq d$.*

Proof. Since Σ is a product of the all of the generators $A_{i,j}$, the claim follows from Lemmas 2.4.5 and 2.4.6.

□

2.4.2 The case of even degree

We retain the notation of §2.4.1, including our definition of $r : \widehat{P}_d \to \Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. We first need the following key lemma, which is analogous to Lemma 2.4.5.

Lemma 2.4.8. *As above, let*

$$\Sigma = (A_{1,2})(A_{1,3}A_{2,3})...(A_{1,d}A_{2,d}...A_{d-1,d}) \in \widehat{P}_d.$$

For $1 \leq k \leq 2g + 2$, let Σ_k be defined as the same product as above, except that all $A_{i,j}$ with $k \in \{i, j\}$ are omitted. Then if $d = 2g + 2$, we have

a) $r(\Sigma) = 1$, and

b) $r(\Sigma_k) = -1$ for $1 \leq k \leq d$.

Proof. It follows from Lemma 2.3.2 that $r : \widehat{P}_d \to \Gamma(2) \lhd \mathrm{Sp}(T_2(J))$ is isomorphic to the 2-adic representation induced from $R : P_d \to \Gamma(2) \lhd \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$. Therefore, it will suffice to show that (a) $R(\Sigma) = 1$, and (b) $R(\Sigma_k) = -1$ for $1 \leq k \leq d$. By Proposition 2.2.3(a), R factors through the map $\partial : P_d \to \pi_0 \mathcal{Y}_d$. By Corollary 2.1.5, Σ lies in the kernel of ∂ and thus also lies in the kernel of R. This implies part (a).

Proposition 2.2.3(b) and Proposition 2.4.5 show that R maps

$$\Sigma_d = (A_{1,2})(A_{1,3}A_{2,3})...(A_{1,d-1}A_{2,d-1}...A_{d-2,d-1})$$

to $-1 \in \Gamma(2) \lhd H_1(\mathcal{C}_{T_0}, \mathbb{Z})$. Now repeated applications of Proposition 2.1.6 show that $\Sigma_k = (\beta_{d-1}\beta_{d-2}...\beta_{k+1})\Sigma_d(\beta_{d-1}\beta_{d-2}...\beta_{k+1})^{-1}$ for each k. Thus, the Σ_k's all lie in the same conjugacy class of B_d, so their images all lie in the same conjugacy class of $R(\Sigma_d) = -1 \in \mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$. But -1 lies in the center of $\mathrm{Sp}(H_1(\mathcal{C}_{T_0}, \mathbb{Z}))$, so $R(\Sigma_k) = -1$ for $1 \leq k \leq d$. Part (b) follows. □

We now assume that $d = 2g + 2$ with $g \geq 2$. Then Lemma 2.4.4 says that L_2 is a proper subfield of $\tilde{L}$; we want to determine which subfield it is. Since $\mathrm{Gal}(L_2/L_1)$ is a free $\mathbb{Z}/2\mathbb{Z}$-module of finite rank, we may consider it as a finite-dimensional vector space over $\mathbb{F}_2$. By Kummer theory, it may be identified with the dual of a finite subgroup $H < L_1^\times/(L_1^\times)^2$, which we also view as a finite-dimensional vector space over $\mathbb{F}_2$. More precisely, there is a canonical isomorphism

$$H \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(L_2/L_1), \mathbb{F}_2)$$

defined explicitly as follows: for any element in H, a representative $a \in L_1^\times$ gets mapped to the homomorphism $\mathrm{Gal}(L_2/L_1) \to \mathbb{F}_2$ given by $\sigma \mapsto a^\sigma/a \in \{\pm 1\} \cong \mathbb{F}_2$. It is clear from this construction that L_2 is generated over L_1 by square roots of representatives in $L_1^\times$ of all elements of $H < L_1^\times/(L_1^\times)^2$.

Now assume that $g \neq 1$, so that $L_1 = L(\{\alpha_i\}_{1 \leq i \leq d})$. Let H' be the subgroup of $L_1^\times/(L_1^\times)^2$ generated by the elements $(\alpha_i - \alpha_j)$ modulo $(L_1^\times)^2$ for $1 \leq i < j \leq 2g + 2$. Since the $(\alpha_i - \alpha_j)$'s are independent, we may view H' as a vector space over $\mathbb{F}_2$ of dimension $(2g + 2)(2g + 1)/2$ with a basis given by the set of classes of the $(\alpha_i - \alpha_j)$'s. Let S be the set of pairs of integers (i, j) with $1 \leq i < j \leq d$. Then we may identify each $(i, j) \in S$ with the class of $(\alpha_i - \alpha_j)$, and consider H' as the vector space $\bigoplus_{s \in S} \mathbb{F}_2 s$. There is an obvious bijection between the elements of H' and subsets of S.

Note that Lemma 2.4.4 implies that $H < H'$, so we may consider H as a subspace of the vector space H'.

Lemma 2.4.9. *Any element of H, viewed as a subset $T \subset S$, has the following properties:*

i) T has even cardinality; and

ii) for every $k \in \{1, ..., 2g+2\}$, the number of elements $(i,j) \in T$ such that $k \in \{i,j\}$ is odd; or, for every $k \in \{1, ..., 2g+2\}$, the number of elements $(i,j) \in T$ such that $k \in \{i,j\}$ is even.

Proof. Define Σ and Σ_i as in Lemma 2.4.8. Then Σ is a product of all of the standard generators $A_{i,j}$ and therefore, by Lemma 2.4.6, Σ changes the sign of $\sqrt{\alpha_i - \alpha_j} \in \tilde{L}$, for all $1 \leq i < j \leq 2g+2$. But part (a) of Lemma 2.4.8 implies that Σ fixes all square roots of representatives in $L_1^\times$ of elements of H, so elements of H must each be represented by a product of an even number of terms of the form $(\alpha_i - \alpha_j)$; in other words, each element of H corresponds to an even-cardinality subset $T \subset S$, which is property (i).

Meanwhile, for each $k \in \{1, ..., 2g+2\}$, let

$$\Sigma'_k = A_{1,k}...A_{k-1,k}A_{k,k+1}...A_{k,2g+2}.$$

Since $\Gamma(2)/\Gamma(4)$ is abelian, it is easy to see that the images of $\Sigma_k\Sigma'_k$ and Σ are equal in $\Gamma(2)/\Gamma(4)$. Then it follows from both (a) and (b) of Lemma 2.4.8 that Σ'_k maps to $-1 \in \Gamma(2)/\Gamma(4)$. Now Σ'_k is a product of all generators $A_{i,j}$ such that $k \in \{i,j\}$, and therefore, by Lemma 2.4.6, Σ'_k changes the sign of $\sqrt{\alpha_k - \alpha_i} \in \tilde{L}$ for all $1 \leq i \leq 2g+2$, $i \neq k$ while fixing all $\sqrt{\alpha_i - \alpha_j}$ with $k \notin \{i,j\}$. Thus, if an element of H is fixed by -1 (resp. not fixed by -1), then the corresponding subset $T \subset S$ must contain an even (resp. odd) number of elements (i,j) with $k \in \{i,j\}$ for each k. So the corresponding subset T satisfies property (ii).

□

Lemma 2.4.10. *The set H_0 of all subsets $T \subset S$ satisfying properties (i) and (ii) of Lemma 2.4.9 is a subspace of $H' = \bigoplus_{s \in S} \mathbb{F}_2 s$ of dimension $2g^2 + g$.*

Proof. First of all, let $T, T' \subset S$ be any subsets satisfying properties (i) and (ii). Then their sum corresponds to the subset $(T \cup T') \setminus (T \cap T')$, and it is easy to show that this subset must also satisfy properties (i) and (ii). It follows that H_0 is a subspace of H'.

Let $S_1 = \{(1, 2g+2), (2, 2g+2), ..., (2g+1, 2g+2)\} \subset S$, and let H_1 be the subspace of H' spanned by the elements of S_1. We claim that $H' = H_0 \oplus H_1$. For each $1 \leq i < j \leq 2g+1$, let

$$h_{i,j} = \sum_{k=1}^{2g+1} (k, 2g+2) - (i, 2g+2) - (j, 2g+2) + (i, j) \in H_0.$$

For any element of H', one may obtain an element of H_1 by adding elements $h_{i,j}$ for appropriate choices of i and j. Thus, every element of H' is the sum of an element of H_0 and an element of H_1. Moreover, choose any nonzero element of H_1, which corresponds to a nonempty subset $T \subset S_1 \subset S$. If $T = S_1$, then T consists of $2g+1$ elements and violates property (i), and therefore $T \notin H_0$. If $T \subsetneq S_1$, then since T is also nonempty, there is some $k \in \{1, ..., 2g+1\}$ such that $(k, 2g+2) \in T$, but there is some other $k' \in \{1, ..., 2g+1\}$ such that $(k', 2g+2) \notin T$. Then by definition of S_1, there is exactly 1 element of $(i, j) \in T$ with $k \in \{i, j\}$, but there are 0 elements $(i, j) \in T$ with $k' \in \{i, j\}$. This violates property (ii), so again $T \notin H_0$. Therefore, $H_0 \cap H_1 = \{0\}$, and the claim follows. In particular, $\dim(H') = \dim(H_0) + \dim(H_1)$.

Since there are $2g+1$ elements in S_1, the dimension of H_1 is $2g+1$. So

$$\dim(H_0) = \dim(H') - \dim(H_1) = (2g+2)(2g+1)/2 - (2g+1) = 2g^2 + g.$$

□

Proposition 2.4.11. *With all of the above notation, L_2 is the extension of L_1 obtained by adjoining square roots of elements of the form*

$$\prod_{(i,j)\in T} (\alpha_i - \alpha_j) \in K_1,$$

where T is a subset of S satisfying properties (i) and (ii) of Lemma 2.4.9. Moreover, the square root of such an element $\prod_{(i,j)\in T}(\alpha_i - \alpha_j)$ where $T \subset S$ satisfies (i) and (ii) is fixed by $-1 \in \mathrm{Gal}(L_2/L_1)$ if and only if T satisfies

iii) for every $k \in \{1, ..., 2g+2\}$, the number of elements $(i, j) \in T$ such that $k \in \{i, j\}$ is even.

Proof. First assume $g \neq 1$. Lemma 2.4.9 shows that $H \subseteq H_0$, and Lemma 2.4.10 shows that H_0 is a subspace of dimension $2g^2 + g$. Since H is finite-dimensional and dual to $\mathrm{Gal}(L_2/L_1)$, the dimension of H is equal to the

rank of $\mathrm{Gal}(L_2/L_1) \cong \Gamma(2)/\Gamma(4)$ as a free $\mathbb{Z}/2\mathbb{Z}$-module. By Lemma 2.4.3, $\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$. Therefore, the dimensions of H and H_0 are equal, so $H = H_0$, which implies the first statement of the proposition for $g \neq 1$.

Let L_2' be the subfield of L_2 fixed by $\{\pm 1\} \lhd \mathrm{Gal}(L_2/L_1)$. It was shown in the proof of Lemma 2.4.9 that if $T \subset S$ is the subset corresponding to L_2', the number of elements $(i,j) \in T$ such that $k \in \{i,j\}$ is even for all k. This proves the second statement of the proposition for $g \neq 1$.

Now assume $g = 1$. Then L_1 is the subfield of $L(\{\alpha_i\}_{i=1}^4)$ given in Proposition 1.2.1(c). One checks that if we let $A_1 = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$, $A_2 = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$, and $A_3 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$, we get $L_1 = L(A_1, A_2, A_3)$. Moreover, the A_i's are algebraically independent, and their product is a square root of the discriminant of the α_i's. Since L_2 is unramified over L at all points of X, then clearly L_2 is unramified over L_1 away from the ideals (A_i) for $i = 1, 2, 3$. But $\mathrm{Gal}(L_2/L_1) \cong \Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^3$, so by a similar argument as in the proof of Lemma 2.4.4, $L_2 = L_1(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3})$. It is easy to check that this is still the extension of L_1 described in the first statement of the theorem. Moreover, it follows from Lemma 2.4.6 that the element $\Sigma_4 = A_{1,2}A_{1,3}A_{2,3}$ acts on $L_2 = L_1(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3})$ by changing the sign of each $\sqrt{A_i}$. But Lemma 2.4.8 implies that Σ acts as the scalar matrix $-1 \in \Gamma(2)/\Gamma(4)$. Thus,

$$L_2' = L_1(\sqrt{A_2A_3}, \sqrt{A_3A_1}, \sqrt{A_1A_2}).$$

It is easy to check that this is still the extension of L_1 described in the second statement of the proposition. Thus, all claims still hold for $g = 1$.

□

It is easy to convert the above description of L_2 and of the action of $-1 \in \mathrm{Gal}(L_2/L_1)$ to the descriptions given in Theorem 2.4.1(b).

Proof (of Theorem 2.4.1(b)) . Recall the definition of $H = H_0 < H'$ used above, and of H_1 used in the proof of Lemma 2.4.10. It is shown in the proof of Lemma 2.4.10 that any element of H' is the sum of an element in H_1 and elements of the form

$$h_{i,j} := \sum_{k=1}^{2g+1} (k, 2g+2) - (i, 2g+2) - (j, 2g+2) + (i,j) \in H_0.$$

It is also shown that $H' = H \oplus H_1$, and therefore, the elements $h_{i,j}$ generate

H. Each $h_{i,j}$ corresponds to the element in $L^\times/(L^\times)^2$ represented by

$$\sqrt{\alpha_i - \alpha_j} \prod_{\substack{1 \leq l \leq 2g+1 \\ l \neq i,j}} \sqrt{\alpha_l - \alpha_{2g+2}},$$

so L_2 must be generated over L_1 by these elements for $1 \leq i < j \leq 2g+1$. Moreover, it follows directly from the second statement of Proposition 2.4.11 that $-1 \in \mathrm{Gal}(L_2/L_1)$ changes the sign of each of these generators.

□

2.5 Fields of 8-torsion of elliptic curves

In this section, we will give generators for the extension L_3/L in the case that J/L is an elliptic curve, or in other words, for degrees $d = 3$ and $d = 4$. Throughout the section, for any index $i \in \{1, 2, 3\}$, we will consider i as an element of $\mathbb{Z}/3\mathbb{Z}$. If $d = 3$, for each $i \in \mathbb{Z}/3\mathbb{Z}$, we fix an element $A_i \in L_2$ such that $A_i^2 = \alpha_{i+1} - \alpha_{i+2}$. If $d = 4$, for each $i \in \mathbb{Z}/3\mathbb{Z}$, fix an element $A_i \in L_2$ such that $A_i^2 = (\alpha_i - \alpha_4)(\alpha_{i+1} - \alpha_{i+2})$. One checks that in either case, we have the identity

$$A_1^2 + A_2^2 + A_3^2 = 0, \tag{2.19}$$

which we will exploit below. Now for each $i = 1, 2, 3$, fix an element $B_i \in \bar{L}$ such that $B_i^2 = A_i(A_{i+1} + \zeta_4 A_{i+2})$. The result is as follows.

Theorem 2.5.1. *Assume the above notation for $d = 3$ or $d = 4$. Then*

$$L_3 = L_2(B_1, B_2, B_3). \tag{2.20}$$

We now state state some elementary properties of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For each $n \geq 1$, $\Gamma(2^n)/\Gamma(2^{n+1}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ (see the proof of Corollary 2.2 of [22]), and therefore, $|\Gamma(2)/\Gamma(8)| = 64$. It is also straightforward to show that $\Gamma(2) \lhd \mathrm{SL}_2(\mathbb{Z})$ can be decomposed into the direct product $\Gamma(2)' \times \{\pm 1\}$, where

$$\Gamma(2)' = \{\sigma \in \Gamma(2) \mid \sigma_{1,1} \equiv \sigma_{2,2} \equiv 1 \pmod 4\}. \tag{2.21}$$

Lemma 2.5.2. *The group $\Gamma(2)'/\Gamma(8)$ can be presented as*

$$\langle \sigma, \tau \mid \sigma^4 = \tau^4 = [\sigma^2, \tau] = [\sigma, \tau^2] = [\sigma, \tau]^2 = [[\sigma, \tau], \sigma] = [[\sigma, \tau], \tau] = 1 \rangle. \tag{2.22}$$

Proof. Let σ (resp. τ) be the image of $\tilde{\sigma} := \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$ (resp. $\tilde{\tau} := \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$) in $\Gamma(2)'/\Gamma(8)$. It is well known that $\tilde{\sigma}$ and $\tilde{\tau}$ generate $\Gamma(2)'$ (see, for instance, Proposition A.1 of [17]), so σ and τ generate $\Gamma(2)'/\Gamma(8)$. It is then straightforward to check that the relations given in (2.22) hold. To show that these relations determine the $\Gamma(2)'/\Gamma(8)$, one checks that the only nontrivial element of the commutator subgroup of the group given by (2.22) is cyclic of order 2, and that the quotient by this commutator subgroup is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; therefore, the group has order 32. Since $\Gamma(2)'/\Gamma(8)$ also has order 32, it must be fully determined by the relations in (2.22).

□

Lemma 2.5.3. *The only normal subgroup of $R^{-1}(\Gamma(2))$ which induces a quotient isomorphic to $\Gamma(2)/\Gamma(8)$ is $R^{-1}(\Gamma(8)) \lhd R^{-1}(\Gamma(2)) \cong P_3$, where $R : B_d \to \mathrm{Sp}(T_2(J))$ is the representation defined in §2.2.2.*

Proof. Clearly $R^{-1}(\Gamma(2))/R^{-1}(\Gamma(8)) \cong \Gamma(2)/\Gamma(8)$. As in Remark 2.3.5(b), $R^{-1}(\Gamma(2)) \cong P_3$ if $d = 3$ or $d = 4$, so it suffices to show that P_3 has a unique quotient isomorphic to $\Gamma(2)/\Gamma(8)$.

Let $N \lhd P_3$ be a normal subgroup whose corresponding quotient is isomorphic to $\Gamma(2)/\Gamma(8)$. By Proposition 2.1.1, $A_{1,2}A_{1,3}A_{2,3}$ generates the center of P_3; therefore, its image modulo N must lie in the center of $P_3/N \cong \Gamma(2)/\Gamma(8)$. It can easily be deduced from Lemma 2.5.2 that the center of $\Gamma(2)/\Gamma(8)$ is an elementary abelian 2-group, so the image of $A_{1,2}A_{1,3}A_{2,3}$ in P_3/N must have order dividing 2. It cannot be trivial, since then P_3/N could be generated by the images of $A_{1,2}$ and $A_{1,3}$, and it again can be deduced from Lemma 2.5.2 that $\Gamma(2)/\Gamma(8)$ cannot be generated by only 2 elements. Therefore, the image of $A_{1,2}A_{1,3}A_{2,3}$ modulo N has order 2, and $(A_{1,2}A_{1,3}A_{2,3})^2 \in N$, so the quotient map factors through $P_3/\langle (A_{1,2}A_{1,3}A_{2,3})^2 \rangle$. But the discussion in §3.6.4 of [8] shows that $P_3/(A_{1,2}A_{1,3}A_{2,3})^2 \cong \Gamma(2) \lhd \mathrm{SL}_2(\mathbb{Z})$, so the quotient map factors through $\Gamma(2)$. Any surjective homomorphism $\Gamma(2) = \Gamma(2)' \times \{\pm 1\} \twoheadrightarrow \Gamma(2)/\Gamma(8)$ takes $-1 \in \Gamma(2)$ to a nontrivial element of $\Gamma(2)/\Gamma(8)$, since $\Gamma(2)'$ can be generated by only 2 elements, whereas $\Gamma(2)/\Gamma(8)$ cannot. Then one checks from the presentation given in the statement of Lemma 2.5.2 that the image of $\Gamma(2)'$ must be isomorphic to $\Gamma(2)'/\Gamma(8)$. Thus, it suffices to show that the only normal subgroup of $\Gamma(2)'$ which induces a quotient isomorphic to $\Gamma(2)'/\Gamma(8)$ is $\Gamma(8)$.

Let $N' \lhd \Gamma(2)'$ be a normal subgroup such that $\Gamma(2)'/N' \cong \Gamma(2)'/\Gamma(8)$. Let σ and τ be the matrices given in the proof of Lemma 2.5.2, and let

$\phi_N : \Gamma(2)' \twoheadrightarrow \Gamma(2)'/N'$ be the quotient homomorphism. One checks from the presentation given in the statement of Lemma 2.5.2 that each element of $\Gamma(2)'/N'$ has order dividing 4; that each square element is in the center; and that the each commutator has order dividing 2 and is in the center. It follows that $\phi_{N'}(\sigma^4) = \phi_{N'}(\tau^4) = \phi_{N'}([\sigma^2, \tau]) = \phi_{N'}([\sigma, \tau^2]) = \phi_{N'}([\sigma, \tau]^2) = \phi_{N'}([[\sigma, \tau], \sigma]) = \phi_{N'}([[\sigma, \tau], \tau]) = 1$. Thus, N' contains the subgroup normally generated by $\{\sigma^4, \tau^4, [\sigma^2, \tau], [\sigma, \tau^2], [\sigma, \tau]^2, [[\sigma, \tau], \sigma], [[\sigma, \tau], \tau]\}$. But the statement and proof of Lemma 2.5.2 show that $\Gamma(8)$ is normally generated by these elements, so $\Gamma(8) \trianglelefteq N'$. Since $|\Gamma(2)'/N'| = |\Gamma(2)'/\Gamma(8)|$, we have $\Gamma(8) = N'$, as desired.

□

We are now ready to prove Theorem 2.5.1.

Proof (of Theorem 2.5.1) . Let $L' = L_2(B_1, B_2, B_3)$. First we check that L' is generated over L_2 by square roots of three elements of independent classes in $L_2^\times/(L_2^\times)^2$, and thus, $[L' : L_2] = 8$. Therefore, $[L_2 : L_1] = 8$ implies $[L' : L_1] = 64$.

Using the relation (2.19), for each i, we compute

$$(A_i(A_{i+1} + \zeta_4 A_{i+2}))(A_i(A_{i+1} - \zeta_4 A_{i+2})) = -A_i^4. \tag{2.23}$$

In light of this, for $i = 1, 2, 3$, we define B_i' to be the element of L' such that $B_i'^2 = A_i(A_{i+1} - \zeta_4 A_{i+2})$ and $B_i B_i' = \zeta_4 A_i^2 \in L_1$. Define $\sigma \in \mathrm{Gal}(L'/L_1)$ to be automorphism which acts by

$$\sigma : (A_1, A_2, A_3, B_1, B_2, B_3) \mapsto (A_1, A_2, -A_3, B_1', B_2', \zeta_4 B_3'),$$

and let $\tau \in \mathrm{Gal}(L'/L_1)$ be the automorphism which acts by

$$\tau : (A_1, A_2, A_3, B_1, B_2, B_3) \mapsto (-A_1, A_2, A_3, \zeta_4 B_1, B_2', B_3').$$

Note that σ^2 and τ^2 both act trivially on L_2 while sending (B_1, B_2, B_3) to $(B_1, B_2, -B_3)$ and to $(-B_1, B_2, B_3)$ respectively; it is now easy to check that σ^2 (resp. τ^2) has order 2 and commutes with τ (resp. σ). One also checks that $[\sigma, \tau]$ acts trivially on L_2 and sends (B_1, B_2, B_3) to $(-B_1, -B_2, -B_3)$, and that this automorphism also commutes with both σ and τ. Thus, σ and τ satisfy the relations given in (2.22). Moreover, σ and τ have exact order 4, while $[\sigma, \tau]$ has exact order 2, and it is straightforward to verify that this implies that $\langle \sigma, \tau \rangle$ has order $32 = |\Gamma(2)'/\Gamma(8)|$ and therefore is isomorphic to

$\Gamma(2)'/\Gamma(8)$. Note also that $\langle\sigma,\tau\rangle$ fixes A_2, whose orbit under $\mathrm{Gal}(\bar{L}/L_1)$ has cardinality 2, so if ρ is any automorphism in $\mathrm{Gal}(L'/L_1)$ which does not fix A_2, then $\langle\sigma,\tau,\rho\rangle$ has order 64 and must be all of $\mathrm{Gal}(L'/L_1)$. We choose ρ to be the automorphism that acts by changing the sign of all A_i's and all B_i's. Then ρ commutes with σ and τ, and

$$\mathrm{Gal}(L'/L_1) = \langle\sigma,\tau\rangle \times \langle\rho\rangle \cong \Gamma(2)'/\Gamma(8) \times \{\pm 1\} \cong \Gamma(2)/\Gamma(8). \tag{2.24}$$

One can check that L'/L_1 is unramified away from the primes $\{(A_i^2)\}_{i=1}^3$, and thus, L' is a subextension of L^{unr}/L_1. As noted in Remark 2.3.5(b), $\mathrm{Gal}(L^{\mathrm{unr}}/L_1) \cong \widehat{P}_3$ if $d = 3$ or $d = 4$, and the subextension L' corresponds to some normal subgroup of $\widehat{P}_3$ inducing a quotient isomorphic to $\mathrm{Gal}(L'/L_1) \cong \Gamma(2)/\Gamma(8)$. Lemma 2.5.3 then implies that this normal subgroup of $\widehat{P}_3$ is the one corresponding to $R^{-1}(\Gamma(8)) \lhd P_3$. But Proposition 2.3.4 shows that the subextension corresponding to $R^{-1}(\Gamma(8))$ is L_3. Therefore, $L' = L_3$.

□

2.6 Generalization to other ground fields

The goal of this section is to strengthen the main results of this chapter (Theorems 2.3.1, 2.4.1, and 2.5.1) by generalizing from a ground field L which is transcendental over $\mathbb{C}$ to a ground field K which is transcendental over some field k of characteristic different from 2. (Although the statement of Theorem 2.3.1 will only be generalized for $\ell = 2$, it can be generalized for odd ℓ in an analogous way using a similar argument; we omit this in order to avoid cumbersome notation.)

As in Chapter 1, let k be any field of characteristic different from 2; let α_1, α_2, ... , α_d be transcendental and independent over k; and let K be the subfield of $k(\{\alpha_i\}_{1\le i\le d})$ generated over k by the symmetric functions of the α_i's. We will also fix the following notation. Let C_K be the hyperelliptic curve defined over K given by the equation (2.12), and let J_K be its Jacobian. For each $n \ge 0$, let $K_n = K(J_K[2^n])$ be the extension of K over which the 2^n-torsion points of J_K are defined, and let $K_\infty = \bigcup_{n=0}^\infty K_n$ and $L_\infty = \bigcup_{n=0}^\infty L_n$. Let $\rho_{2,K} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_2}(T_2(J_K))$ be the homomorphism arising from the natural Galois action on the Tate module of J_K; recall that the image of $\rho_{2,K}$ is contained in the group of symplectic similitudes $\mathrm{GSp}(T_2(J_K))$ and is further contained in $\mathrm{Sp}(T_2(J_K))$ if and only if K contains all 2-power roots

of unity. Whenever a statement concerning the "generic" Jacobian over L remains true when $\mathbb{C}$ is replaced by some field k in this way, then we shall say that that statement "holds over k". (In what follows, we canonically identify $T_2(J)$ with $T_2(J_K)$ and $\Gamma(2^n)$ with the level-2^n congruence subgroup of $\mathrm{Sp}(T_2(J_K))$ for each $n \geq 0$.)

Lemma 2.6.1. *Suppose that k is a subset of $\mathbb{C}$. Then the statements of Theorem 2.3.1 (with $\ell = 2$) and Corollary 2.3.3 hold over k.*

Proof. For any $n \geq 0$, let $\theta_n : \mathrm{Gal}(L_\infty/L_n) \to \mathrm{Gal}(K_\infty/K_n)$ be the composition of the natural inclusion $\mathrm{Gal}(L_\infty/L_n) \hookrightarrow \mathrm{Gal}(L_\infty/K_n)$ with the natural restriction map $\mathrm{Gal}(L_\infty/K_n) \twoheadrightarrow \mathrm{Gal}(K_\infty/K_n)$. Let $\bar{\rho}_2^{(\infty)}$ (resp. $\bar{\rho}_{2,K}^{(\infty)}$) be the representation of $\mathrm{Gal}(L_\infty/L)$ (resp. $\mathrm{Gal}(K_\infty/K)$) induced from ρ_2 (resp. $\rho_{2,K}$) by the restriction homomorphism of the Galois groups. It is easy to see that $\bar{\rho}_2^{(\infty)} = \bar{\rho}_{2,K}^{(\infty)} \circ \theta_0$. It will suffice to show that θ_0 is an isomorphism when $K = K(\mu_2)$.

First, observe that $L_\infty = K_\infty\mathbb{C}$ and $L_n = K_n\mathbb{C}$, and that therefore, $K_\infty L_n = K_\infty\mathbb{C} = L_\infty$. Choose any $\sigma \in \mathrm{Gal}(L_\infty/L_n)$ such that $\theta_n(\sigma)$ acts trivially on K_∞. Then σ acts trivially on K_∞ as well as on L_n, so it acts trivially on their compositum $K_\infty L_n = L_\infty$. Thus, θ_n is injective.

Now suppose that $n \geq 1$. Then, as in the proof of Corollary 2.3.3(b), the image under $\bar{\rho}_2^{(\infty)}$ of $\mathrm{Gal}(L_\infty/L_n)$ coincides with the congruence subgroup $\Gamma(2^n)$. Therefore, since θ_n is injective, the image under $\bar{\rho}_K$ of $\mathrm{Gal}(K_\infty/K_n)$ contains $\Gamma(2^n)$. If K contains all 2-power roots of unity, then the Weil pairing is Galois invariant, and so the image of $\mathrm{Gal}(K_\infty/K_n)$ must also be contained in $\Gamma(2^n)$. Therefore, θ_n is an isomorphism for $n \geq 1$ when $K = K(\mu_2)$.

Now if $d \neq 4$, using Corollary 2.3.3(a) and the fact that $\mathrm{Gal}(K(\{\alpha_i\}_{i=1}^d)/K) \cong S_d$ by Proposition 1.2.1(c), we get the commutative diagram below, whose top and bottom rows are short exact sequences.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L_\infty/L_1) & \longrightarrow & \mathrm{Gal}(L_\infty/L) & \longrightarrow & S_d & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta_0} & & \| & & \\ 1 & \longrightarrow & \mathrm{Gal}(K_\infty/K_1) & \longrightarrow & \mathrm{Gal}(K_\infty/K) & \longrightarrow & S_d & \longrightarrow & 1 \end{array} \tag{2.25}$$

By the Short Five Lemma, if θ_1 is an isomorphism, then so is θ_0. Thus, θ_0 is an isomorphism when $d \neq 4$ and $K = K(\mu_2)$. The fact that θ_0 is an isomorphism when $d = 4$ and $K = K(\mu_2)$ follows from a similar argument. □

Lemma 2.6.2. *Suppose that k is a subfield of $\mathbb{C}$. Then the statement of Theorem 2.4.1 (resp. Theorem 2.5.1) holds over $K(\zeta_4)$ (resp. over $K(\zeta_8)$).*

Proof. For any $n \geq 1$, define $\bar{\rho}_2^{(n)} : \mathrm{Gal}(L_n/L_1) \xrightarrow{\sim} \Gamma(2)/\Gamma(2^n) \lhd \mathrm{Sp}(J[2^n])$ as in the statement of Corollary 2.3.3(b), and define $\bar{\rho}_{2,K}^{(n)} : \mathrm{Gal}(K_n/K_1) \to \mathrm{GSp}(J_K[2^n])$ in the obvious way. Additionally, let $\bar{\theta}^{(n)} : \mathrm{Gal}(L_n/L) \to \mathrm{Gal}(K_n/K)$ be the composition of the natural inclusion $\mathrm{Gal}(L_n/L) \hookrightarrow \mathrm{Gal}(L_n/K)$ with the natural restriction map $\mathrm{Gal}(L_n/K) \twoheadrightarrow \mathrm{Gal}(K_n/K)$. It is easy to see that $\bar{\rho}_2^{(n)} = \bar{\rho}_{2,K}^{(n)} \circ \bar{\theta}^{(n)}$. It will suffice to show that $\bar{\theta}^{(2)}$ is an isomorphism when $K = K(\zeta_4)$ and that $\bar{\theta}^{(3)}$ is an isomorphism when $K = K(\zeta_8)$.

As in the proof of Lemma 2.6.1, observe that $L_n = K_n\mathbb{C}$, and that therefore, $K_nL_1 = K_n\mathbb{C} = L_n$. Choose any $\sigma \in \mathrm{Gal}(L_n/L_1)$ such that $\bar{\theta}^{(n)}(\sigma)$ acts trivially on K_n. Then σ acts trivially on K_n as well as on L_1, so it acts trivially on their compositum $K_nL_1 = L_n$. Thus, $\bar{\theta}^{(n)}$ is injective. It follows that the image under $\bar{\rho}_{2,K}^{(n)}$ contains $\Gamma(2)/\Gamma(2^n) \lhd \mathrm{GSp}(J_K[2^n])$. If $K = K(\zeta_4)$ (resp. if $K = K(\zeta_8)$), then the Weil pairing on $J[4]$ (resp. on $J[8]$) is Galois invariant, and so the image of $\mathrm{Gal}(K_2/K)$ (resp. of $\mathrm{Gal}(K_3/K)$) must also be contained in $\Gamma(2)/\Gamma(4) \lhd \mathrm{GSp}(J[4])$ (resp. $\Gamma(2)/\Gamma(8) \lhd \mathrm{GSp}(J[8])$). Therefore, $\bar{\theta}^{(2)}$ (resp. $\bar{\theta}^{(3)}$) is an isomorphism when $K = K(\zeta_4)$ (resp. when $K = K(\zeta_8)$), as desired.

□

Lemma 2.6.3. *Suppose that $k = \mathbb{F}_p$ for some prime $p \neq 2$. Then the statement of Theorem 2.4.1 (resp. Theorem 2.5.1) holds over $K(\zeta_4)$ (resp. over $K(\zeta_8)$).*

Proof. Fix an integer $n \geq 1$. Consider the affine scheme

$$S := \mathrm{Spec}(\mathbb{Z}[\tfrac{1}{2}, \zeta_{2^n}, \{\alpha_i\}_{i=1}^d, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq d}])$$

and the affine scheme $\mathcal{C}^{(S)} \to S$ given by

$$\mathcal{C}^{(S)} = \mathrm{Spec}(\mathcal{O}_S[x, y]/(y^2 - F(x))),$$

where $\mathcal{O}_S$ is the coordinate ring of S and $F(x) = \prod_{i=1}^d (x - \alpha_i)$. Define $\mathcal{J}^{(S)} \to S$ to be the abelian scheme representing the Picard functor of the scheme $\mathcal{C}^{(S)} \to S$ (see [14], Theorem 8.1). Let J_0 denote the Jacobian of the hyperelliptic curve defined over $K' := \mathbb{Q}(\zeta_{2^n}, \{\alpha_i\}_{i=1}^d)$ by the equation in (2.12). Note that the generic fiber of $\mathcal{J}^{(S)} \to S$ is J_0, while the fiber over the

prime (p) is the Jacobian J_K over K_1 when $k = \mathbb{F}_p(\zeta_{2^n})$. Proposition 20.7 of [13] implies that the kernel of the multiplication-by-2^n map on $\mathcal{J}^{(S)} \to S$, which we denote by $\mathcal{J}^{(S)}[2^n] \to S$, is a finite étale group scheme over S. Since the morphism $\mathcal{J}^{(S)}[2^n] \to S$ is finite, $\mathcal{J}^{(S)}[2^n]$ is an affine scheme whose coordinate ring we denote by $\mathcal{O}_{S,n}$; finiteness implies that $\mathcal{O}_{S,n}$ is an integral extension of $\mathcal{O}_S$. Then the corresponding extension of function fields is $K'(J_0[2^n])/K'$. If $n = 2$, then by Lemma 2.6.2, the extension of function fields of $K'(J_0[2^n])/K'$ is given by the generators in the statement of Theorem 2.4.1. It is easy to check that these elements are integral over $\mathcal{O}_S$ and thus may be used to generate a subextension of $\mathcal{O}_{S,2}$ over $\mathcal{O}_S$ whose fraction field coincides with the fraction field of $K'(J_0[2^n])$. It follows that the fraction field of the reduction modulo (p) of $\mathcal{O}_{S,2}$ is generated over the fraction field of the reduction modulo (p) of $\mathcal{O}_S$ by the images modulo (p) of the generators given in the statement of Theorem 2.4.1. But these fraction fields are clearly K_2 and K_1 respectively. This proves that Theorem 2.4.1 holds over $K(\zeta_4)$ when $k = \mathbb{F}_p$; the claim that Theorem 2.5.1 holds over $K(\zeta_8)$ when $k = \mathbb{F}_p$ follows from a similar argument.

□

Proposition 2.6.4. *Suppose that k is any field of characteristic different from 2. Then the statement of Theorem 2.4.1 (resp. Theorem 2.5.1) holds over $K(\zeta_4)$ (resp. over $K(\zeta_8)$).*

Proof. Let $\mathfrak{f}$ be the prime subfield of k, and let $\mathfrak{F}$ be the purely transcendental extension of $\mathfrak{f}$ obtained by adjoining the symmetric functions of the α_i's. Then since the coefficients of the equation (2.12) are elements of $\mathfrak{F}$, we may consider C (and hence also J) to be defined over the subfield $\mathfrak{F} \subseteq K$. If the characteristic of k is 0 (resp. $p > 0$), then $\mathfrak{f} = \mathbb{Q}$ (resp. $\mathfrak{f} = \mathbb{F}_p$), and Lemma 2.6.2 (resp. Lemma 2.6.3) gives the statement of the proposition when $K = \mathfrak{F}$. The statement for general K immediately follows since $K_2 = K\mathfrak{F}(J[4])$ and $K_3 = K\mathfrak{F}(J[8])$.

□

Chapter 3

Dyadic torsion of elliptic curves

Let k be any field of characteristic different from 2. Fix an integer $d \geq 3$; let $\alpha_1, \alpha_2, ..., \alpha_d$ be transcendental and independent over k; and let K be the subfield of $k(\{\alpha_i\}_{i=1}^d)$ generated over k by the symmetric functions of the α_i's. Let C be a smooth projective model of the hyperelliptic curve over K given by

$$y^2 = \prod_{i=1}^{d}(x - \alpha_i), \tag{3.1}$$

and let J be its Jacobian. The main goal of this chapter is to describe generators of the extension of K over which all 2-power torsion is defined when $d = 3$, in which case the genus is $g = 1$ and C (as well as J) is an elliptic curve. For our main result, we describe these generators using recursive formulas. To set up these formulas, we first require the notion of a "decoration" on a 3-regular tree, which is developed in the following section. The main result (Therem 3.2.1) will be stated and proved in §3.2. In §3.3, we will apply the constructions developed in §3.2 to obtain additional results (Proposition 3.3.1 and Theorem 3.3.2), and in §3.4, we will apply the results of this chapter to curves in the Legendre family.

3.1 Construction of decorations for genus 1

3.1.1 Equivalence classes of rank-2 $\mathbb{Z}_2$-lattices

In this subsection, the genus of C may be any integer $g \geq 1$. Let $T_2(J)$ denote the 2-adic Tate module of E, and let $V_2(J) = T_2(J) \otimes \mathbb{Q}_2$. Then $V_2(J)$ is

a $2g$-dimensional vector space over $\mathbb{Q}_2$ which contains the rank-$2g$ $\mathbb{Z}_2$-lattice $T_2(J)$. Clearly, $\mathbb{Q}_2^\times$ acts upon the set of all rank-$2g$ $\mathbb{Z}_2$-lattices in $V_2(J)$ as follows: for any such lattice Λ and any $a \in \mathbb{Q}_2^\times$, then let $a\Lambda = \{a\lambda \mid \lambda \in \Lambda\}$, which is also a rank-$2g$ $\mathbb{Z}_2$-lattice in $V_2(J)$. We define a graph $\mathcal{L}$ as follows. The vertices of $\mathcal{L}$ are the set of all rank-$2g$ $\mathbb{Z}_2$-lattices in $V_2(J)$ modulo the equivalence relation where Λ is equivalent to Λ' if $\Lambda = a\Lambda'$ for some $a \in \mathbb{Q}_2$. The equivalence class of a lattice Λ will be denoted $[\Lambda]$. Two vertices are connected by an edge if they can be written as $[\Lambda]$ and $[\Lambda']$, where $\Lambda \subset \Lambda'$ and $\Lambda'/\Lambda \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus g}$. It is easy to see that this relation is symmetric, so the edge set of this graph is well-defined. From now on, let $\Lambda_0 = T_2(J)$.

Proposition 3.1.1. *a) Each vertex of $\mathcal{L}$ is represented uniquely by a lattice which contains Λ_0 but does not contain $2^{-1}\Lambda_0$.*

b) There is a bijection between vertices of $\mathcal{L}$ and finite subgroups of $J[2^\infty]$ which do not contain all of $J[2]$.

Proof. Let Λ be any rank-$2g$ $\mathbb{Z}_2$-lattice in $V_2(J)$. Consider the sequence of $\mathbb{Z}_2$-lattices $\{2^{-n}\Lambda \cap \Lambda_0\}_{n=0}^\infty$. Each lattice $2^{-n}\Lambda \cap \Lambda_0$ is an open subgroup of Λ_0 (in the 2-adic topology); moreover, since $\cup_{n=0}^\infty 2^{-n}\Lambda = V_2(J)$, this sequence of lattices forms an open cover of Λ_0. But Λ_0 is compact, so this cover has a finite subcover. It follows that for some $n' \geq 0$, $2^{-n'}\Lambda \geq \Lambda_0$. Now there must be a maximal $m' \geq 0$ such that $2^{-n}\Lambda \geq 2^{-m'}\Lambda_0$, or else $2^{-n'}\Lambda \geq \cup_{n=0}^\infty 2^{-n}\Lambda_0 = V_2(J)$, which is impossible. Then $2^{m'-n'}\Lambda$ contains Λ but not $2^{-1}\Lambda$, and the first part of (a) follows from the fact that $[2^{m'-n'}\Lambda] = [\Lambda]$. To prove uniqueness, suppose that Λ' and Λ are two lattices in the same class which each contain Λ_0 but not $2^{-1}\Lambda_0$. Then $\Lambda' = a\Lambda$ for some $a \in \mathbb{Q}_2^\times$. Let $v_2(a)$ be the 2-adic valuation of a. If $v_2(a) > 0$, then $a\Lambda$ does not contain Λ_0, which is a contradiction, and if $v_2(a) < 0$, then $a\Lambda$ contains $2^{-1}\Lambda_0$, which is a contradiction. Thus, $v_2(a) = 0$ and $a \in \mathbb{Z}_2^\times$, so $\Lambda' = a\Lambda = \Lambda$, and part (a) is proved.

To prove (b), it suffices by (a) to construct a bijection between the set of lattices Λ which contain Λ_0 but not $2^{-1}\Lambda_0$ and the set of finite subgroups of $J[2^\infty]$ which do not contain all of $J[2]$. Let Λ be a lattice containing Λ_0 but not $2^{-1}\Lambda_0$. Then Λ/Λ_0 is clearly a finite $\mathbb{Z}_2$-module. Choose $n \geq 0$ such that 2^n kills Λ/Λ_0. Then $2^n\Lambda_0 \leq 2^n\Lambda \leq \Lambda_0$, so we may identify $\Lambda/\Lambda_0 \cong 2^n\Lambda/2^n\Lambda_0$ with a subgroup of $\Lambda_0/2^n\Lambda_0$. But $\Lambda_0 = T_2(J)$, and $T_2(J)/2^nT_2(J)$ is naturally identified with $J[2^n]$, so we may identify $N := \Lambda/\Lambda_0$ with a subgroup of $J[2^n] < J[2^\infty]$. The fact that Λ does not contain $2^{-1}\Lambda_0$ implies that N does not contain $J[2]$. Conversely, let N be a finite subgroup of $J[2^\infty]$ which

does not contain $J[2]$. Then N is a subgroup of $J[2^n]$ for some $n \geq 0$, and furthermore, it has an obvious $\mathbb{Z}_2$-module structure. By the inverse limit definition of $T_2(J)$, a subgroup of $J[2^n]$ lifts uniquely to a subgroup M of finite index of $T_2(J)$ which contains $2^n T_2(J)$, and such that there is a canonical isomorphism $M/2^n T_2(J) \cong N$ which respects the $\mathbb{Z}_2$-module structure. It is clear that M is a sublattice of $T_2(J)$. Let $\Lambda = 2^{-n}M$. Then there are natural isomorphisms of $\mathbb{Z}_2$-modules

$$\Lambda/T_2(J) \cong 2^n\Lambda/2^n T_2(J) \cong M/2^n T_2(J) \cong N. \tag{3.2}$$

By construction, this Λ is uniquely determined by N. Moreover, the fact that N does not contain $J[2]$ implies that Λ does not contain $2^{-1}\Lambda_0$. □

3.1.2 A 3-regular tree

For this subsection and for most of the rest of the chapter, we will assume that C has degree $d = 3$ and therefore genus $g = 1$ – in other words, C is an elliptic curve and can be identified with its Jacobian J. In this case, we will write E for the elliptic curve C (and J), but we will continue to denote the associated graph by $\mathcal{L}$.

Proposition 3.1.2. *With the above definitions, $\mathcal{L}$ is a 3-regular tree.*

Proof. This is proved in Chapter II, §1 of [25].

□

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 $|\mathcal{L}|_n$ (resp. $|\mathcal{L}|_{\leq n}$, resp. $|\mathcal{L}|_{\geq n}$) denote the subset of vertices of $\mathcal{L}$ which are of distance n (resp. $\leq n$, resp. $\geq n$) from $v_0 := [\Lambda_0]$.

Proposition 3.1.3. *Under the bijection given in Proposition 3.1.1(b), for $n \geq 0$, each vertex $v \in |\mathcal{L}|_n$ is identified with a cyclic order-2^n subgroup of $E[2^n]$.*

Proof. First, note that for each $n \geq 1$, $J[2^n]$ is a free $\mathbb{Z}/2^n\mathbb{Z}$-module of rank 2, so any subgroup of $J[2^n]$ not containing $J[2]$ must be cyclic. Now let $N < J[2^n]$ be a cyclic subgroup of order 2^n corresponding to a vertex $v \in |\mathcal{L}|$. Then one easily verifies that $\{N \cap J[2^i]\}_{i=0}^n$ is a sequence of cyclic subgroups

whose corresponding vertices form a path from v_0 to v with n edges. Now assume inductively that the claim of the proposition holds for any $m \leq n-1$. Then $v \notin |\mathcal{L}|_m$ for any $m \leq n-1$ since N is cyclic of order $2^n \neq 2^m$. Thus, $v \in |\Lambda|_n$, and the claim is proved.

□

3.1.3 Decorations on 3-regular trees

In order to define "decoration", we first set up some notation.

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 Λ representing v such that $\Lambda > \Lambda_0$ and $\Lambda/\Lambda_0 \cong \mathbb{Z}/2\mathbb{Z}$. There are three such lattices Λ which represent the three vertices in $|\mathcal{L}|_1$, all contained in $2^{-1}\Lambda_0$. Then each such Λ can be identified with an order-2 subgroup of $E[2]$ via the induced injection $\Lambda/\Lambda_0 \hookrightarrow 2^{-1}\Lambda_0/\Lambda_0$ composed with the obvious isomorphisms $2^{-1}\Lambda_0/\Lambda_0 \cong \Lambda_0/2\Lambda_0 = T_2(E)/2T_2(E) \cong E[2]$. 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 3.1.4. *A decoration on the tree $\mathcal{L}$ is a map $\Psi : |\mathcal{L}|_{\geq 1} \to \bar{K}$ with the following properties:*

a) For any vertex $v \in |\mathcal{L}|_{\geq 1}$, $\Psi(v) \neq \Psi(v')$.

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

$$x^2 + 2(2\Psi((\tilde{v})') + \Psi(\tilde{v}))x + \Psi((\tilde{v}))^2 \in \bar{K}[x], \tag{3.3}$$

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

$$x^2 + 2(\Psi((\tilde{v})') - 2\Psi(\tilde{v}))x + \Psi((\tilde{v})')^2 \in \bar{K}[x]. \tag{3.4}$$

Proposition 3.1.5. *A decoration on $\mathcal{L}$ exists.*

Proof. For each $N \geq 1$, define F_N to be the set of all functions $\Psi : |\mathcal{L}|_{\leq n} \backslash \{v_0\}$ that satisfy the conditions of Definition 3.1.4 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 (because the inverse limit of nonempty sets is also 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 Ψ_N. This amounts to showing that for each $v \in |\mathcal{L}|_n$ with $n \geq 2$, the polynomial $x^2 + 2(\Psi(v') - 2\Psi(v))x + \Psi(v')^2$ has two distinct roots in $\bar{K}$. It is clear from property (b) of the definition and a little computation that for $v \in |\mathcal{L}|_2$, the polynomial $x^2 + 2(\Psi(v') - 2\Psi(v))x + \Psi(v')^2$ 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 $x^2 + 2(\Psi(v') - 2\Psi(v))x + \Psi(v')^2$, then the constant coefficient $(\Psi(v'))^2$ would be 0. But $\Psi(v')$ is a root of the polynomial $x^2 + 2(\Psi(\tilde{v}') - 2\Psi(\tilde{v}))x + \Psi(\tilde{v}')^2$, which by the inductive assumption, has nonzero roots. Thus, the polynomial $x^2 + 2(\Psi(v') - 2\Psi(v))x + \Psi(v')^2$ has nonzero roots. Now suppose that its roots are equal. Then its discriminant $4(\Psi(v') - 2\Psi(v))^2 - 4\Psi(v')^2 = 16\Psi(v)(\Psi(v) - \Psi(v'))$ 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 $x^2 + 2(\Psi(\tilde{v}') - 2\Psi(\tilde{v}))x + \Psi(\tilde{v}')^2$, and by the inductive assumption, they are distinct and nonzero, so we have a contradiction.

□

3.2 Field of dyadic torsion for genus 1

Define K_n for $n \geq 0$ and K_∞ as in §2.6. Let G be the image of the natural homomorphism $\rho_2 : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(T_2(E)) := \mathrm{Aut}_{\mathbb{Z}_2}(T_2(E))$. As in §2.3.2, for any integer $n \geq 0$, we write $\bar{\rho}_2^{(n)} : \mathrm{Gal}(K_n/K) \to \mathrm{GL}(E[2^n])$ for the homomorphism induced by the natural Galois action on $E[2^n]$, and denote its image by $\bar{G}^{(n)}$. Let $G(n)$ denote the kernel of the natural surjection $G \twoheadrightarrow \bar{G}^{(n)}$; it is the image under ρ_2 of the normal subgroup $\mathrm{Gal}(\bar{K}/K_n) \lhd \mathrm{Gal}(\bar{K}/K)$. Note that $G(0) = G$. For any extension field K' of K, let $K'(\mu_2) = \bigcup_{n=1}^{\infty} K'(\zeta_{2^n})$.

We now state the main theorem, which we will prove in the remainder of this section.

Theorem 3.2.1. *Let an elliptic curve E/K be defined as above, with Weierstrass roots α_1, α_2, and α_3. Define the tree $\mathcal{L}$ associated with this elliptic*

curve as above, and let Ψ be a decoration on $\mathcal{L}$. Set

$$K'_\infty := K(\{\Psi(v)\}_{v\in|\mathcal{L}|_{\geq 1}}).$$

a) For any $i,j \in \{1,2,3\}$ with $i \neq j$, choose an element $a_{i,j} \in \bar{K}$ whose square is $\alpha_i - \alpha_j$. Then we have

$$K_\infty = K'_\infty(a_{i,j})(\mu_2).$$

b) Any Galois automorphism whose image under ρ_2 is -1 acts on K_∞ by fixing $K'_\infty(\mu_2)$ and sending $a_{i,j}$ to $-a_{i,j}$.

Remark 3.2.2. In the case that the degree $d = 4$ and C is a smooth projective model of the curve given by (3.1) with J its Jacobian, for any $i \in \{1,2,3,4\}$, we may determine the field extension $K(\hat{\alpha}_i, J[2^\infty])/K(\hat{\alpha}_i)$, where $\hat{\alpha}_i$ is a square root of $\prod_{1\leq j\leq 4, j\neq i}(\alpha_j - \alpha_i)$, as follows. There is a morphism from C to the (degree-3) elliptic curve E over $K(\hat{\alpha}_i)$ given by

$$E : y'^2 = \prod_{1\leq j\leq 4, j\neq i} (x' - 1/(\alpha_j - \alpha_i)),$$

which is defined by $x' = 1/x - \alpha_i$, $y' = y/\hat{\alpha}_i(x - \alpha_i)$. Then we may apply the above theorem to E to find the extension of $K(\hat{\alpha}_i)$ obtained by adjoining all 2-power torsion points of E. Since the morphism $C \to E$ is defined over $K(\hat{\alpha}_i)$, this is the field of dyadic torsion of the Jacobian J of C, considered as a curve over $K(\hat{\alpha}_i)$. It seems likely that the extension $K(J[2^\infty])/K$ may be described as in the statement of Therem 3.2.1, with a similar definition of "decoration", except where $\Psi(v(i)) = (\alpha_i - \alpha_4)(\alpha_{i+1} - \alpha_{i+2})$ for each $i \in \mathbb{Z}/3\mathbb{Z}$. This is analogous to the the situation in §2.5, and would result from a generalization of Lemma 2.5.3 stating that $R^{-1}(\Gamma(2^n))$ is the unique normal subgroup of $R^{-1}(\Gamma(2))$ which induces a quotient isomorphic to $\Gamma(2)/\Gamma(2^n)$.

3.2.1 Compositions of 2-isogenies of elliptic curves

In this subsection, we will assign to each $v \in |\mathcal{L}|_n$ an elliptic curve E_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 3.2.9(b)) is defined over $K(N_v)$. We will do this using a well-known isogeny of degree 2 which is defined over the field of definition of its kernel. (Note that it is well known, as in Exercise 3.13(e) of [28], that for any finite subgroup $N < E(\bar{K})$, 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 α_{i+1} or α_{i+2} as though $i \in \mathbb{Z}/3\mathbb{Z}$.

Proposition 3.2.3. *Define, for any distinct, nonzero $\beta, \gamma \in \bar{K}$, the elliptic curves $E_{\beta,\gamma}$ and $E'_{\beta,\gamma}$ over $\bar{K}$ given by the following Weierstrass equations:*

$$E_{\beta,\gamma} : y^2 = x(x-\beta)(x-\gamma), \tag{3.5}$$

$$E'_{\beta,\gamma} : y^2 = x^3 + 2(\beta+\gamma)x^2 + (\beta-\gamma)^2 x. \tag{3.6}$$

Let $\phi_{\beta,\gamma} : E_{\beta,\gamma} \to E'_{\beta,\gamma}$ be the morphism given by

$$\phi_{\beta,\gamma} : (x,y) \mapsto (\frac{y^2}{x^2}, y(\frac{\beta\gamma}{x^2} - 1)). \tag{3.7}$$

Then

a) $\phi_{\beta,\gamma}$ is an isogeny of degree 2 whose kernel is generated by $(0,0) \in E_{\beta,\gamma}[2]$, and

b) the points $(\beta,0), (\gamma,0) \in E_{\beta,\gamma}[2]$ are mapped by $\phi_{\beta,\gamma}$ to the point $(0,0) \in E'_{\beta,\gamma}[2]$.

Proof. This is given as an example of a 2-isogeny of elliptic curves in Example 4.5 of Chapter III in [28], with $a = -(\beta+\gamma)$, $b = \beta\gamma$, and $r = (\beta-\gamma)^2$. Direct computation shows that $\phi_{\beta,\gamma}((\beta,0)) = \phi_{\beta,\gamma}((\gamma,0)) = (0,0) \in E'_{\beta,\gamma}[2]$, proving part (b). This implies that the difference of the points $(\beta,0), (\gamma,0) \in E_{\beta,\gamma}[2]$, which is $(0,0) \in E_{\beta,\gamma}[2]$, lies in the kernel of $\phi_{\beta,\gamma}$, proving part (a). □

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

For any $z \in \bar{K}$, denote by E_z the elliptic curve with Weierstrass equation given by

$$y^2 = (x-\alpha_1-z)(x-\alpha_2-z)(x-\alpha_3-z). \tag{3.8}$$

Let t_z the isomorphism $E \to E_z$ sending $(x,y) \mapsto (x+z, y)$. Now define, for $i \in \mathbb{Z}/3\mathbb{Z}$,

$$\phi_{v(i)} : E \to E'_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i},\ \phi_i := \phi_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i} \circ t_{-\alpha_i}. \tag{3.9}$$

We assign $E_{v(i)} := E'_{\alpha_{i+1}-\alpha_i, \alpha_{i+2}-\alpha_i}$. It follows from Proposition 3.2.3 that for each i, $\phi_{v(i)} : E \to E_{v(i)}$ is an isogeny whose kernel is the order-2 cyclic subgroup $N_{v(i)} = \langle(\alpha_i, 0)\rangle$ of $E(K_1)$.

From now on, for each $i \in \mathbb{Z}/3\mathbb{Z}$, let $a_{v(i)} = \alpha_{i+1} - \alpha_{i+2}$. Then we may write the Weierstrass equation for $E_{v(i)}$ as

$$\begin{aligned} y^2 &= x^3 + 2((\alpha_{i+2} - \alpha_i) - (\alpha_i - \alpha_{i+1}))x^2 + (\alpha_{i+1} - \alpha_{i+2})^2 x \\ &= x^3 + 2(2(\alpha_{i+2} - \alpha_i) + (\alpha_{i+1} - \alpha_{i+2}))x^2 + (\alpha_{i+1} - \alpha_{i+2})^2 x \\ &= x^3 + 2(2a_{v(i)'} + a_{v(i)})x^2 + a_{v(i)}^2 x. \end{aligned} \tag{3.10}$$

Since 0 is a root of the cubic in the above equation, we know that $(0,0) \in E_{v(i)}[2]$, and Proposition 3.2.3(b) implies that $(0,0)$ is the image of both points in $E[2] \backslash N_{v(i)}$. It follows that the inverse image of $\langle (0,0) \rangle < E_{v(i)}[2]$ under $\phi_{v(i)}$ is $E[2]$. Then the inverse images of the other two order-2 subgroups of $E_{v_j}(\bar{K})$ under $\phi_{v(i)}$ 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 $|\mathcal{L}|_2$ whose parent vertex is $v(i)$. Let a_v (resp. $a_{v'}$) be the (nonzero) root of the cubic in the above equation such that $\phi_{v(i)}$ takes N_v (resp. $N_{v'}$) to the subgroup $\langle (a_v, 0) \rangle$ (resp. $\langle (a_{v'}, 0) \rangle$) of $E_{N_{v(i)}}(\bar{K})$. Now, using the notation of above, we have the elliptic curve $E'_{-a_v, a_{v'} - a_v}$ and the isogeny $\phi_{-a_v, a_{v'} - a_v} \circ t_{-a_v} : E_{v_j} \to E'_{-a_v, a_{v'} - a_v}$. Its kernel is $\langle a_v, 0 \rangle$. Therefore, if we assign $E_v := E'_{-a_v, a_{v'} - a_v}$ and

$$\phi_v := \phi_{-a_v, a_{v'} - a_v} \circ t_{-a_v} \circ \phi_{v(i)} : E \to E_v, \tag{3.11}$$

then ϕ_v has kernel N_v. Its Weierstrass equation can be written as

$$\begin{aligned} y^2 &= x^3 + 2((-a_v) + (a_{v'} - a_v))x^2 + ((-a_v) - (a_{v'} - a_v))^2 x \\ &= x^3 + 2(a_{v'} - 2a_v)x^2 + a_{v'}^2 x. \end{aligned} \tag{3.12}$$

Thus, we have defined the desired E_v and ϕ_v for all $v \in |\mathcal{L}|_2$.

Now we will define the desired ϕ_{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 $E_{N_{\tilde{v}}}$ and an isogeny $\phi_{N_{\tilde{v}}} : E \to E_{N_{\tilde{v}}}$ whose kernel is $N_{\tilde{v}}$. Suppose that $E_{N_{\tilde{v}}}$ has Weierstrass equation

$$y^2 = x(x - a_v)(x - a_{v'}), \tag{3.13}$$

that E_{N_v} has Weierstrass equation

$$y^2 = x^3 + 2(a_{v'} - 2a_v)x^2 + a_{v'}^2 x, \tag{3.14}$$

and that $\phi_{N_v} = \phi_{-a_v, a_{v'}-a_v} \circ t_{-a_v} \circ \phi_{N_{\tilde{v}}}$. 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 $E_{N_{\tilde{v}}}[2]$. The inverse image of $\langle (0,0) \rangle < E_{N_v}[2]$ under ϕ_{N_v} therefore contains $E[2]$ and is not a cyclic subgroup of $E(\bar{K})$. The inverse images under ϕ_{N_v} of the other two order-2 subgroups of $E_{N_v}(\bar{K})$ therefore correspond to the two order-2^{n+1} cyclic subgroups of $E(\bar{K})$ 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 $\tilde{u} = v$. Let a_u (resp. $a_{u'}$) be the (nonzero) root of the cubic in the above equation such that ϕ_{N_v} takes N_u (resp. $N_{u'}$) to the subgroup $\langle (a_u, 0) \rangle$ (resp. $\langle (a_{u'}, 0) \rangle$) of $E_{N_v}(\bar{K})$. Now, using the notation of above, we have the elliptic curve $E'_{-a_u, a_{u'}-a_u}$ and the isogeny $\phi_{-a_u, a_{u'}-a_u} \circ t_{-a_u} : E_{N_v} \to E'_{-a_u, a_{u'}-a_u}$. Its kernel is $\langle (a_u, 0) \rangle$. Therefore, if we assign $E_{N_u} := E'_{-a_u, a_{u'}-a_u}$ and

$$\phi_{N_u} := \phi_{-a_u, a_{u'}-a_u} \circ t_{-a_u} \circ \phi_{N_v} : E \to E_{N_u},$$

then ϕ_{N_u} has kernel N_u. Its Weierstrass equation can be written as

$$\begin{aligned} y^2 &= x^3 + 2((-a_v) + (a_{v'} - a_v))x^2 + ((-a_v) - (a_{v'} - a_v))^2 x \\ &= x^3 + 2(a_{u'} - 2a_u)x^2 + a_{u'}^2 x. \end{aligned} \tag{3.15}$$

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_v and ϕ_v for all $v \in |\mathcal{L}|_{n+1}$. In this way, E_v, ϕ_v, and $a_v \in \bar{K}$ are defined for all $v \in |\mathcal{L}|_{\geq 1}$. Furthermore, for all $v \in |\mathcal{L}|$, we define K_v to be the extension of K obtained by adjoining the coefficients of the Weierstrass equation of E_v given above.

Remark 3.2.4. With the above notation, for any $v \in |\mathcal{L}|_n$ with $n \geq 2$, let a_u and $a_{u'}$ be the two distinct nonzero roots of the cubic in (3.14). Then we have shown above that the isogeny

$$\phi_{a_u, a_{u'}} \circ \phi_{-a_v, a_{v'}-a_v} \circ t_{-a_v} : E_{N_{\tilde{v}}} \to E'_{a_u, a_{u'}} \tag{3.16}$$

has kernel $E_{N_{\tilde{v}}}[2]$. In fact, one can compute that it takes

$$E_{N_{\tilde{v}}} : y^2 = x(x - a_v)(x - a_{v'}) \tag{3.17}$$

to

$$E'_{a_u, a_{u'}} : y^2 = x(x - 4a_v)(x - 4a_{v'}). \tag{3.18}$$

These two elliptic curves are easily verified to be isomorphic over K; for instance, one can define an isomorphism $E_{N_{\tilde{v}}} \to E'_{a_u, a_{u'}}$ by $(x, y) \mapsto (4x, 8y)$.

Lemma 3.2.5. *Using the above notation, define* $\Psi : |\mathcal{L}|_{\geq 1} \to \bar{K}$ *by setting* $\Psi(v) = a_v$ *for* $v \in |\mathcal{L}|_{\geq 1}$. *Then* Ψ *is a decoration on* $\mathcal{L}$.

Proof. The assignments of $a_{v(i)}$ for $i \in \mathbb{Z}/3\mathbb{Z}$ satisfy the property (b) given in Definition 3.1.4. By construction, Ψ also satisfies property (c) also (see the cubics in (3.10) and (3.12)). Finally, as in the proof of Proposition 3.1.5, the roots of the above quadratics must be distinct, fulfilling property (a). □

Definition 3.2.6. *For any integer* $n \geq 0$, *define the extension* K'_n *of* K *to be the compositum of the fields* K_v *for all* $v \in |\mathcal{L}|_{\leq n}$. *Define the extension* K'_∞ *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

$$K = K'_0 \subset K'_1 \subset K'_2 \subset ... \subset K'_n \subset ..., \tag{3.19}$$

with $K'_\infty = \bigcup_{n \geq 0} K'_n$.

Lemma 3.2.7. *For each* $v \in |\mathcal{L}|_n$ *with* $n \geq 1$, *let* $\{v_0, v_1, ..., v_n = v\}$ *be the sequence of vertices in the path of length* n *from* v_0 *to* v. *Let* $\tilde{K}_v$ *denote the compositum of the fields* K_v *for all* $v \in \{v_0, v_1, ..., v_n\}$. *Then*

$$\tilde{K}_v = K(\alpha_1, \alpha_2, \alpha_3, \{a_v\}_{v \in \{v_2, ..., v_n\}}).$$

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_v is given by a Weierstrass equation of the form (3.10) or (3.12) and is therefore defined over $K(a_v, a_{v'})$. But $a_v a_{v'}$ is a coefficient of $E_{\tilde{v}}$, and so the only element that we need to adjoin to $\tilde{K}_{\tilde{v}} = K(\alpha_1, \alpha_2, \alpha_3, \{a_u\}_{u \in \{v_0, v_1, ..., v_{n-1} = \tilde{v}\}})$ to obtain $\tilde{K}_v$ is a_v. Moreover, a_v does lie in this extension, since $-(a_v + a_{v'})$ is a coefficient in the equation for E_v and $2(2a_{v'} + a_v)$ (resp. $2(a_{v'} - 2a_v)$) is a coefficient of $E_{\tilde{v}}$ if $n = 1$ (resp. $n \geq 2$). Thus, we have proved the claim for $n + 1$. □

Proposition 3.2.8. *a) For any* $n \geq 1$, $K'_n = K(\{\Psi(v)\}_{v \in |\mathcal{L}|_{\leq n} \setminus \{v_0\}})$ *for any decoration* Ψ *on* $\mathcal{L}$.

b) As in the statement of Theorem 3.2.1, $K'_\infty = K(\{\Psi(v)\}_{v\in|\mathcal{L}|_{\geq 1}})$ for any decoration Ψ on $\mathcal{L}$.

(In particular, the extensions $K(\{\Psi(v)\}_{v\in|\mathcal{L}|_{\leq n}\setminus\{v_0\}})$ and $K(\{\Psi(v)\}_{v\in|\mathcal{L}|_{\geq 1}})$ do not depend on the choice of decoration Ψ.)

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 3.2.7 that

$$K'_n = K(\{a_v\})_{v\in|\mathcal{L}|_{\leq n}\setminus\{v_0\}}), \tag{3.20}$$

from which it follows that

$$K'_\infty = K(\{a_v\}_{v\in|\mathcal{L}|_{\geq 1}}). \tag{3.21}$$

Therefore, it suffices to show that for any decoration Ψ, $K(\{\Psi(v)\}_{v\in|\mathcal{L}|_n}) = K(\{a_v\}_{v\in|\mathcal{L}|_n})$. Choose any decoration Ψ. By Definition 3.1.4(b), $\Psi(v) = a_v$ for any $v \in |\mathcal{L}|_1$, so the above claim is true for $n = 1$. Now assume inductively that for some $n \geq 1$, there is a permutation σ on $|\mathcal{L}|_{\leq n}$ which preserves distances between vertices (in particular, it acts on each $|\mathcal{L}|_i$ for $1 \leq i \leq n$), such that $\Psi(v) = a_{\sigma(v)}$ for all $v \in |\mathcal{L}|_{\leq n}$. For any $i \in \{1, ..., n\}$, two vertices in $|\mathcal{L}|_i$ are of distance 2 apart if and only if they are twins, so it is clear that $\sigma(v') = \sigma(v)'$ for all $v \in |\mathcal{L}|_{\leq n}$. Now choose any $v \in |\mathcal{L}|_{n+1}$. Since $\Psi(v)$ is a root of the quadratic polynomial $x^2 + 2(\Psi(\tilde{v}) + 2\Psi((\tilde{v})'))x + \Psi(\tilde{v})^2 = x^2 - 2(a_{\sigma(\tilde{v})} + 2a_{\sigma(\tilde{v})'})x + a^2_{\sigma(\tilde{v})}$ (resp. $x^2 + 2(\Psi((\tilde{v})') - 2\Psi(\tilde{v}))x + \Psi((\tilde{v})')^2 = x^2 - 2(a_{\sigma(\tilde{v})'} - 2a_{\sigma(\tilde{v})})x + a^2_{\sigma(\tilde{v})'}$) if $n = 1$ (resp. $n \geq 2$), there must exist $u \in |\mathcal{L}|_{n+1}$ with $\tilde{u} = \sigma(\tilde{v})$ such that $\Psi(v) = a_u$. Extend σ to a permutation on $|\mathcal{L}|_{\leq n+1}$ by assigning σ to take each $v \in |\mathcal{L}|_{n+1}$ to the vertex u obtained in this way. Then this extension σ is clearly a permutation on $|\mathcal{L}|_{\leq n+1}$, and one can easily check that σ preserves distances between vertices. Therefore, we have the equalities

$$K(\{\Psi(v)\}_{v\in|\mathcal{L}|_{n+1}}) = K(\{a_{\sigma(v)}\}_{v\in|\mathcal{L}|_{n+1}\setminus\{v_0\}}) = K(\{a_v\}_{v\in|\mathcal{L}|_{n+1}\setminus\{v_0\}}), \tag{3.22}$$

and we are done.

□

Proposition 3.2.9. *With the above notation,*

a) the isogeny ϕ_{N_v} is defined over $K(N_v)$, and $K_v \subseteq K(N_v)$,

b) for all $n \geq 0$, $K'_n \subseteq K_n$, and equality holds for $n = 0, 1$.

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

Now assume inductively that for some $n \geq 1$ and all $v \in |\mathcal{L}|_n$, ϕ_v is defined over $K(N_v)$ and $K_v \subseteq K(N_v)$. Choose any $v \in |\mathcal{L}|_{n+1}$. We may apply the inductive assumption to $\tilde{v}$, since $\tilde{v} \in |\mathcal{L}|_n$. Let P be a generator of the cyclic order-2^{n+1} subgroup N_v. Then P has coordinates in $K(N_v)$ and $\phi_{\tilde{v}}$ is defined over $K(N_{\tilde{v}}) \subseteq K(N_v)$, and it follows that $\phi_{\tilde{v}}(P) = (a_v, 0)$ has coordinates in $K(N_v)$. Thus, $a_v \in K(N_v)$. But $a_v a_{v'}$ is a coefficient of $E_{\tilde{v}}$ and $K_{\tilde{v}} \subseteq K(N_{\tilde{v}})$, 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 $\phi_v = \phi_{-a_v, a_{v'} - a_v} \circ t_{-a_v} \circ \phi_{\tilde{v}}$ is defined over $K(N_{\tilde{v}})(a_v, a_{v'}) \subseteq K(N_v)$. Moreover, the Weierstrass equation (3.12) of $E_v = E'_{-a_v, a_{v'} - a_v}$ has coefficients in $K(a_v, a_{v'}) \subseteq K(N_v)$, and so $K_v \subseteq K(N_v)$, thus proving part (a).

Now part (a) and the fact that K'_n is the compositum of the fields K_v for all $v \in |\mathcal{L}|_{\leq n} \backslash \{v_0\}$ imply that K'_n is contained in the compositum of the extensions $K(N_v)$ for all $v \in |\mathcal{L}|_{\leq n} \backslash \{v_0\}$. Since $\{N_v\}_{v \in |\mathcal{L}|_{\leq n}}$ is the set of all cyclic subgroups of $E[2^n]$ and therefore generates $E[2^n]$, this compositum is K_n. Thus, $K'_n \subseteq K_n$, which is the statement of (b).

□

Remark 3.2.10. Using Proposition 3.2.8(a) and Definition 3.1.4, one can directly compute that $a_{1,2}a_{1,3}$ (or any of its conjugates) lies in K'_2, as is already known from Theorem 2.4.1, Proposition 2.6.4, and Proposition 3.2.12 below, and that $a_{1,2}a_{1,3}$ has a square root in K'_3. Then Proposition 3.2.9 implies that K_3 itself contains a square root of $a_{1,2}a_{1,3}$. In fact, it is possible to confirm this using Theorem 1.2.3. With the notation of §2.5, one computes that the square of the element $(1 - \zeta_4)^{-1}(B_3 - B'_3)B_2/(A_1 - \zeta_4 A_3) \in K_3$ is

$$\begin{aligned} &-\zeta_4 2^{-1}(B_3 - B'_3)^2 B_2^2/(A_1 - \zeta_4 A_3)^2 \\ &= 2^{-1}(2A_3(A_1 - \zeta_4 A_3))(-A_2\zeta_4(A_3 + \zeta_4 A_1))/(A_1 - \zeta_4 A_3)^2 \\ &= A_3 A_2 (A_1 - \zeta_4 A_3)^2/(A_1 - \zeta_4 A_3)^2 = A_3 A_2 = a_{1,2}a_{1,3}. \end{aligned} \tag{3.23}$$

3.2.2 The subfield fixed by the scalar subgroup

We now characterize the compositum of the fields of definition of these isogenous elliptic curves as the fixed subextension of K_∞/K corresponding to the

scalar subgroup of G. In order to do so, we first want to determine how the absolute Galois group of K acts on the a_v's defined above. We will adopt the following notation. The automorphism group $\mathrm{GL}(T_2(E))$ acts on the set of rank-2 $\mathbb{Z}_2$-lattices in $V_2(E)$ by left multiplication, and this action stabilizes $|\mathcal{L}|$, since $\mathrm{GL}(T_2(E))$ fixes $T_2(E)$. (In fact, this action of $\mathrm{GL}(T_2(E))$ on $\mathcal{L}$ is the action of $\mathrm{Aut}_{\mathbb{Z}_2}(T_2(E)) \subset \mathrm{Aut}_{\mathbb{Q}_2}(V_2(E))$ on the tree described in [25], §1.2.) In particular, this action preserves adjacency of vertices, so each $|\mathcal{L}|_n$ is invariant under the action. We will denote the action of $G \subseteq \mathrm{GL}(T_2(E))$ on $|\mathcal{L}|$ by $(s, v) \mapsto s \cdot v$ for an automorphism s and a vertex v. Note that this action of G, when restricted to $|\mathcal{L}|_{\leq n}$, factors through $G \twoheadrightarrow \bar{G}^{(n)}$. We similarly denote the resulting action of $\bar{G}^{(n)}$ on the induced subtree whose set of vertices is $|\Lambda|_n$ by $(\bar{s}, v) \mapsto \bar{s} \cdot v$ for an automorphism $\bar{s}$ and a vertex v.

For any Galois element $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and vertex $v \in |\mathcal{L}|$, let $v^\sigma := \rho_2(\sigma) \cdot v$. If $v \in |\mathcal{L}|_{\leq n}$ for some $n \geq 1$, then let $v^{\sigma|K_n} = \bar{\rho}_2^{(n)}(\sigma) \cdot v$.

Lemma 3.2.11. *For any $\sigma \in \mathrm{Gal}(\bar{K}/K_1)$ and $v \in |\mathcal{L}|$, we have $a_v^\sigma = a_{v^\sigma}$. If $v \in |\mathcal{L}|_{\leq n}$, then $a_v^{\sigma|_{K_n}} = a_{v^{\sigma|K_n}}$.*

Proof. Choose any $\sigma \in \mathrm{Gal}(\bar{K}/K_1)$. We will prove that $a_v^\sigma = a_{v^\sigma}$ for all $v \in |\mathcal{L}|_n$ for each $n \geq 1$. The claim is trivially true for $n = 1$. Moreover, in the $n = 1$ case, E_{N_v} and ϕ_{N_v} are clearly defined over K_1 and are therefore fixed by σ. In particular, for any $v \in |\mathcal{L}|_1$, $a_v^\sigma = a_{v^\sigma}$, $E_v^\sigma = E_{v^\sigma}$, and $\phi_v^\sigma = \phi_{v^\sigma}$. Now choose $v \in |\mathcal{L}|_2$. Then a_v is a nonzero root of (3.10), which is the Weierstrass cubic for $E_{\tilde{v}}$. Let P be a generator of the cyclic order-4 subgroup N_v; then $\phi_{\tilde{v}}(P) = (a_v, 0) \in E_{\tilde{v}}[2]$, by the above construction of a_v. So we have

$$\phi_{\tilde{v}}(P^\sigma) = \phi_{\tilde{v}}^\sigma(P^\sigma) = (\phi_{\tilde{v}}(P))^\sigma = (a_v^\sigma, 0). \tag{3.24}$$

But P^σ generates $N_v^\sigma = N_{v^\sigma}$. Since $\tilde{v}^\sigma = \tilde{v}$, by the above construction, we have $\phi_{\tilde{v}^\sigma}(P^\sigma) = (a_{v^\sigma}, 0)$. Then (3.24) implies that $a_v^\sigma = a_{v^\sigma}$.

Now assume inductively that for some $n \geq 2$ and $\sigma \in |\mathcal{L}|_n$, $a_v^\sigma = a_{v^\sigma}$, $E_v^\sigma = E_{v^\sigma}$, and $\phi_v^\sigma = \phi_{v^\sigma}$. Choose any $v \in |\mathcal{L}|_{n+1}$. We may apply the induction assumption to $\tilde{v}$, since $\tilde{v} \in |\mathcal{L}|_n$. Then a_v is a nonzero root of the cubic polynomial (3.12), which is the Weierstrass cubic for $E_{\tilde{v}}$. Let P be a generator of the cyclic order-2^{n+1} subgroup N_v; then $\phi_{\tilde{v}}(P) = (a_v, 0) \in E_{\tilde{v}}[2]$, by the above construction of a_v. Then we have

$$\phi_{\tilde{v}^\sigma}(P^\sigma) = \phi_{\tilde{v}}^\sigma(P^\sigma) = (\phi_{\tilde{v}}(P))^\sigma = (\alpha_v^\sigma, 0). \tag{3.25}$$

But since P^σ generates $N_v^\sigma = N_{v^\sigma}$, again we have $\phi_{\tilde{v}^\sigma}(P^\sigma) = (a_{v^\sigma}, 0)$. Then (3.25) implies that $a_v^\sigma = a_{v^\sigma}$, and so the first statement is proved.

Now let $v \in |\mathcal{L}|_{\leq n}$. Then $a_v \in K_n$ by Proposition 3.2.9(b), and one easily checks from the definitions that $v^\sigma = v^{\sigma|_{K_n}}$ for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Thus, the second statement follows from the first.

□

Proposition 3.2.12. *For all $n \geq 1$, the image of $\mathrm{Gal}(K_n/K'_n)$ (resp. of $\mathrm{Gal}(K_\infty/K'_\infty)$) under $\bar{\rho}_2^{(n)}$ (resp. ρ_2) coincides with the subgroup of scalar automorphisms in G (resp. in $\bar{G}^{(n)}$).*

Proof. Fix $n \geq 1$. Since $K'_n \supseteq K_1$ for each $n \geq 1$, it suffices to consider the Galois subgroup $\mathrm{Gal}(K'_n/K_1) \subseteq \mathrm{Gal}(K_n/K_1)$. Proposition 3.2.7, with the help of Lemma 3.2.5, implies that K'_n is generated over K_1 by the elements a_v for all $v \in |\mathcal{L}|_{\leq n} \backslash \{v_0\}$. Therefore, the elements of $\mathrm{Gal}(K_\infty/K_1)$ which fix K'_n are exactly those which fix all of the elements a_v for $v \in |\mathcal{L}|_{\leq n} \backslash \{v_0\}$. By Lemma 3.2.11, these are the Galois elements which fix every vertex in $|\mathcal{L}|_{\leq n}$. It is easy to see that an element of $\mathrm{GL}(E[2^n])$ fixes every vertex in $|\mathcal{L}|_n$ if and only if it is a scalar automorphism. Thus, the image of $\mathrm{Gal}(K_n/K'_n)$ coincides with the subgroup of scalars, as desired. A similar argument proves the analogous statement for $\mathrm{Gal}(K_\infty/K'_\infty)$.

□

Remark 3.2.13. Since each $\sigma \in \mathrm{Gal}(\bar{K}/K)$ takes ζ_8 to $\zeta_8^{\det(\bar{\rho}_2^{(3)}(\sigma))}$, all scalar automorphisms in G must fix ζ_8. Thus, the above proposition implies that K'_∞ contains the 8th roots of unity.

3.2.3 A general lemma

In order to finish proving Theorem 3.2.1, we need a lemma that gives a generator for K_∞ over K'_∞. We will prove a more general statement for the Jacobian of the analogous hyperelliptic curve of any degree $d \geq 3$, as it will be used for the main result of the next chapter as well. To this end, in Lemma 3.2.14 below as well as its proof, K, J, $\rho_2 : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Sp}(T_2(J))$, K_1, and $\bar{\rho}_2^{(2)}$ are defined for any degree $d \geq 3$ analogously to how they are defined elsewhere in this chapter for $d = 3$. Again, let G be the image of Galois under ρ_2. We define K'_∞ to be the subextension of K_∞/K fixed by the scalar subgroup of G; when $d = 3$, Proposition 3.2.12 shows that this is consistent with the notation used in the rest of this section.

Note that, due to the Galois equivariance of the Weil pairing, the image of $\mathrm{Gal}(\bar{K}/K(\mu_2))$ under ρ_2 is $G \cap \mathrm{Sp}(T_2(J))$, and $K_\infty \supset K(\mu_2)$. The homomorphism ρ_2 induces an isomorphism $\mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} G$; if $-1 \in G$, we denote the element of $\mathrm{Gal}(K_\infty/K)$ mapping to -1 via this isomorphism also by $-1 \in \mathrm{Gal}(K_\infty/K)$.

The statement of the following lemma for $d = 3$, together with Lemma 3.2.8, gives the statement of Theorem 3.2.1.

Lemma 3.2.14. *Choose $i, j \in \{1, 2, ..., d\}$ with $i \neq j$. If d is odd, choose an element $a_{i,j} \in \bar{K}$ whose square is $\alpha_i - \alpha_j$. Then with all of the above notation, we have*

$$K_\infty = K'_\infty(a_{i,j})(\mu_2). \tag{3.26}$$

If $-1 \in G$, the Galois element $-1 \in \mathrm{Gal}(K_\infty/K)$ acts by fixing $K'_\infty(\mu_2)$ and sending $a_{i,j}$ to $-a_{i,j}$.

Proof. We first observe that by Galois equivariance, $K_\infty \supset K(\mu_2)$, and that by Theorem 1.2.2, $a_{i,j} \in K_2 \subset K_\infty$. If the scalar subgroup of G is trivial, then $K_\infty = K'_\infty$, and the claim is proved, so we assume that $-1 \in G$. Note that by Galois equivariance, -1 fixes everything in $K(\mu_2)$. So if we replace K with $K(\mu_2)$, it will suffice to assume that K contains all 2-power roots of unity and to prove that $K_\infty = K'_\infty(a_{i,j})$ and that $-1 \in \mathrm{Gal}(K_\infty/K)$ acts as claimed.

Since K contains all 2-power roots of unity, G is contained in $\mathrm{Sp}(T_2(J))$. But the only scalar automorphisms in $\mathrm{Sp}(T_2(J))$ are ± 1, so the image under ρ_2 of $\mathrm{Gal}(K_\infty/K'_\infty)$ coincides with $\{\pm 1\} \lhd G$. It immediately follows that K_∞ is generated over K'_∞ by any element of K_∞ which is not fixed by $-1 \in \mathrm{Gal}(K_\infty/K)$. Clearly, $\bar{\rho}_2^{(2)}(-1|_{K_2}) = -1 \in \Gamma(2)/\Gamma(4)$. But setting $n = 2$ in the statement of Proposition 3.2.12 implies that

$$\mathrm{Gal}(K_2/K'_2) \cong \{\pm 1\} < \Gamma(2)/\Gamma(4), \tag{3.27}$$

so any element in $K_2 \setminus K'_2$ will not be fixed by -1. Theorem 2.4.1 and Proposition 2.6.4 imply that $a_{i,j} \in K_2 \setminus K'_2$, so $K_\infty = K'_\infty(a_{i,j})$. Moreover, $a_{i,j}^2 \in K_1 \subset K'_\infty$, so -1 sends $a_{i,j}$ to $-a_{i,j}$.

□

3.3 Description of some subextensions

The constructions used in §3.2 to prove Theorem 3.2.1 may be used to obtain additional results describing various subextensions of K_∞/K. Throughout, we will assume that we have chosen $i, j \in \{1, 2, 3\}$ with $i \neq j$ and an element $a_{i,j} \in \bar{K}$ as in the statement of Theorem 3.2.1.

3.3.1 Extensions generated by x-coordinates

The following proposition characterizes certain subextensions of K_∞/K in terms of extensions of K generated by the x-coordinates of points in 2-power torsion subgroups of E.

Proposition 3.3.1. *With the above notation, assume that k is a subfield of $\mathbb{C}$. 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*

a) $K_n = K(x(E[2^n]))(a_{i,j})$ for all $n \geq 2$;
b) $K'_n(\zeta_{2^n}) \subseteq K(x(E[2^n]))$ for all $n \geq 1$; and
c) $K'_\infty(\mu_2) = K(x(E[2^\infty]))$.

Proof. The Galois equivariance of the Weil pairing implies that $K_n \supset K(\zeta_{2^n})$ for each $n \geq 0$ and that $K_\infty \supset K(\mu_2)$. For any $n \geq 1$, the subgroup of $\mathrm{Gal}(K_n/K)$ which fixes the x-coordinates of the points in $E[2^n]$ can be identified with the elements of $G \subset \mathrm{GL}(T_2(E))$ which send each point $P \in E[2^n]$ either to P or to $-P$. The only such automorphisms in $\mathrm{GL}(T_2(E))$ are the scalars ± 1. Thus, $K(x(E[2^n]))$ is the subextension of K_n corresponding to the subgroup $\bar{G}^{(n)} \cap \{\pm 1\} \lhd \bar{G}^{(n)} \cap \mathrm{SL}(E[2^n])$, and similarly, $K(x(E[2^\infty]))$ is the subextension of K_∞ corresponding to the subgroup $G \cap \{\pm 1\} \lhd G \cap \mathrm{SL}(T_2(E))$. Part (b) now follows from the fact that, by Galois invariance and Proposition 3.2.12, $K'_n(\zeta_{2^n})$ is the fixed field corresponding to the subgroup of scalars in $G \cap \mathrm{SL}(T_2(E))$, which contains $G \cap \{\pm 1\}$. Part (c) follows similarly. Note that $a_{i,j} \in K_2$ by Theorem 1.2.2. Therefore, we already have part (a) if $G \cap \{\pm 1\}$ is trivial, so we assume that $-1 \in G$. Then 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 follows from Theorem 2.4.1 and Proposition 2.6.4 that $a_{i,j} \in K_2 \subseteq K_n$ is not fixed by -1, hence the statement of part (a).

□

3.3.2 Bounding each field of 2^n-torsion

The description of K'_∞ given in the statement of Theorem 3.2.1 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 3.3.2. *Assume that k is a subfield of $\mathbb{C}$. For $1 \leq i < j \leq 3$ and each $n \geq 2$,*

$$K'_n(a_{i,j}, \zeta_{2^n}) \subseteq K_n \subsetneq K'_{n+1}(a_{i,j}, \zeta_{2^{n+1}}), \tag{3.28}$$

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

Proof. Fix $n \geq 2$. Proposition 3.2.9(b) and the inclusion $K_n \supset K(\zeta_{2^n})$ imply that $K'_n \subset K_n$, and by Theorem 1.2.2, $a_{i,j} \in K_2 \subseteq K_n$, thus implying the first inclusion. For $n = 2$, it has already been shown in the proof of Proposition 3.2.14 that the inclusion is an equality. Since $a_{i,j} \notin K'_\infty(\mu_2)$, it follows that $a_{i,j} \notin K(2^m)'(\zeta_{2^m})$ for any positive integer m. Note that Proposition 3.2.12, Corollary 2.3.3(b), and Lemma 2.6.1 imply that for $n \geq 3$, $\mathrm{Gal}(K_n/K'_n(\zeta_{2^n}))$ is identified with the subgroup $\{\pm 1, \pm(2^{n-1}+1)\} \lhd \mathrm{SL}(E[2^n])$, which has order 4. It follows that the degree of the first inclusion is 2 in this case. Equivalently, for all $n \geq 2$, $K_{n+1} \supset K'_{n+1}(a_{i,j}, \zeta_{2^{n+1}})$ is an extension of degree 2. We have (via $\bar{\rho}_2^{(n+1)}$) the following identifications:

$$\mathrm{Gal}(K_{n+1}/K) \cong G(2)/G(2^{n+1}), \tag{3.29}$$

$$\mathrm{Gal}(K_{n+1}/K'_{n+1}(\zeta_{2^{n+1}})) \cong \langle -1, 2^n + 1 \rangle \lhd G(2)/G(2^{n+1}). \tag{3.30}$$

These imply that $\mathrm{Gal}(K_{n+1}/K'_{n+1}(a_{i,j}, \zeta_{2^{n+1}}))$ is a subgroup of $\langle -1, 2^n+1 \rangle$ of order 2. Since $2^n + 1$ fixes all of K_2, which includes the element $a_{i,j}$, we have $\mathrm{Gal}(K_{n+1}/K'_{n+1}(a_{i,j}, \zeta_{2^{n+1}})) \cong \langle 2^n + 1 \rangle \lhd \Gamma(2)/\Gamma(2^{n+1})$. But this subgroup also leaves K_n fixed, whence the second inclusion $K_n \subset K'_{n+1}(a_{i,j}, \zeta_{2^{n+1}})$. The fact that $[K'_{n+1}(a_{i,j}) : K_n] = 4$ follows quickly from the fact that $\mathrm{Gal}(K_{n+1}/K_n) \cong (G(n) \cap \mathrm{SL}(T_2(E))/G(2^{n+1}) \cap \mathrm{SL}(T_2(E)) = \Gamma(2^n)/\Gamma(2^{n+1})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ (see the proof of Corollary 2.2 of [22]) and therefore has order 8.

□

3.4 Application to the Legendre family

In this section, we assume that k is a number field. Let E_λ be the elliptic curve defined over k by the Weierstrass equation in Legendre form

$$y^2 = x(x-1)(x-\lambda) \tag{3.31}$$

with $\lambda \in k$ (see Chapter III §1 of [28]). We now apply Theorem 3.2.1 and its proof to study the image of the natural 2-adic Galois action $\rho_2 : \mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}(T_2(E_\lambda))$ associated to E_λ.

For each finite prime $\mathfrak{p}$ of k not lying over 2, we denote the corresponding ring of integers by $R_\mathfrak{p} \subset k$, and denote the fraction field of a strict Henselization of $R_\mathfrak{p}$ by $k_\mathfrak{p}^{\mathrm{alg}}$. The field $k_\mathfrak{p}^{\mathrm{alg}}$ may be more explicitly described as consisting of the elements of the completion of k with respect to v which are algebraic over k. Let $v_\mathfrak{p} : (k_\mathfrak{p}^{\mathrm{alg}})^\times \to \mathbb{Z}$ be the (normalized) valuation corresponding to $\mathfrak{p}$, and let π be a uniformizer of $k_\mathfrak{p}^{\mathrm{alg}}$, so $v_\mathfrak{p}(\pi) = 1$. For each $z \in \bar{k}$, we write $v_\mathfrak{p}(z)$ for the image of z under the extension of $v_\mathfrak{p}$ to $k_\mathfrak{p}^{\mathrm{alg}}(z)$. It is clear that since $\mathfrak{p}$ does not lie over 2, for any $n \geq 1$, any algebraic extension of $k_\mathfrak{p}^{\mathrm{alg}}$ of degree 2^n is totally tamely ramified and is of the form $k_\mathfrak{p}^{\mathrm{alg}}(\pi^{1/2^n})$. Moreover, since $k_\mathfrak{p}^{\mathrm{alg}}$ is strictly Henselian, it contains all 2-power roots of each $u \in k_\mathfrak{p}^{\mathrm{alg}}$ such that $v_\mathfrak{p}(u) = 0$; in particular, $k_\mathfrak{p}^{\mathrm{alg}}$ contains all 2-power roots of unity.

Now we consider E_λ as an elliptic curve over $k_\mathfrak{p}^{\mathrm{alg}}$, determine the extension $k_\mathfrak{p}^{\mathrm{alg}}(E_\lambda[2^\infty])$, and describe the image under ρ_2 of $\mathrm{Gal}(\bar{k}/k_\mathfrak{p}^{\mathrm{alg}})$.

Proposition 3.4.1. *With the above notation, let $m = \max(v_\mathfrak{p}(\lambda), v_\mathfrak{p}(\lambda-1))$ and assume that $m > 0$. Then we have the following.*

a) For each $n \geq 1$, we have $k_\mathfrak{p}^{\mathrm{alg}}(E_\lambda[2^n]) = k_\mathfrak{p}(\pi^{m/2^{n-1}})$.

b) There is an element $a \in T_2(E_\lambda)$ whose image modulo 2 is $(1,0) \in E_\lambda[2]$ (resp. $(0,0) \in E_\lambda[2]$) if $v_\mathfrak{p}(\lambda) > 0$ (resp. if $v_\mathfrak{p}(\lambda-1) > 0$) such that the image under ρ_2 of $\mathrm{Gal}(\bar{k}/k_\mathfrak{p}^{\mathrm{alg}})$ is generated by $T_a^{2m} \in \mathrm{SL}(T_2(E_\lambda))$, where the transvection T_a acts by $b \mapsto b + e_2(b,a)a$ for all $b \in T_2(E_\lambda)$.

Proof. We assume that $m = v_\mathfrak{p}(\lambda) > 0$, so $v_\mathfrak{p}(\lambda-1) = 0$; the case that $m = v_\mathfrak{p}(\lambda-1) > 0$ and $v_\mathfrak{p}(\lambda) = 0$ is proved similarly. Let $(\alpha_1, \alpha_2, \alpha_3) = (1, 0, \lambda)$, so that E_λ is defined by the equation $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. We define the corresponding tree $\mathcal{L}$ as in §3.1.2. Let Ψ be a decoration on $\mathcal{L}$ as in §3.1.3. We claim that for each $n \geq 1$, there is a vertex $v \in |\mathcal{L}|_n$ such that $k_\mathfrak{p}^{\mathrm{alg}}(\Psi(v)) = k_\mathfrak{p}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$. We prove this claim by induction on

n. Indeed, for any vertex $v \in |\mathcal{L}|_1$, $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(v)) = k_{\mathfrak{p}}^{\mathrm{alg}}$, so the claim is true for $n = 1$. Moreover, for either vertex $v \in |\mathcal{L}|_2$ such that $\Psi(\tilde{v}) = \lambda - 1$, we have $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(v)) = k_{\mathfrak{p}}^{\mathrm{alg}}(\sqrt{\lambda}) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2})$, and so the claim is true for $n = 2$. Moreover, note that in this case, $v_{\mathfrak{p}}(\Psi(v)) = v_{\mathfrak{p}}(\Psi(v')) = v_{\mathfrak{p}}(-(1+\lambda)\pm 2\sqrt{\lambda}) = 0$, and $v_{\mathfrak{p}}(\Psi(v) - \Psi(v')) = v_{\mathfrak{p}}(\pm 4\sqrt{\lambda}) = m/2$. Now assume that for some $n \geq 2$, there is a vertex $v \in |\mathcal{L}|_n$ such that $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(v)) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$, $v_{\mathfrak{p}}(\Psi(v)) = v_{\mathfrak{p}}(\Psi(v')) = 0$, and $v_{\mathfrak{p}}(\Psi(v) - \Psi(v')) = m/2^{n-1}$. Let u be a vertex in $|\mathcal{L}|_{n+1}$ such that $v = \tilde{u}$. Since $\Psi(u)$ is a root of the quadratic polynomial in (3.4), using the inductive assumption, we have

$$\begin{aligned} v_{\mathfrak{p}}(\Psi(u) - \Psi(u')) &= v_{\mathfrak{p}}(\pm 4\sqrt{-\Psi(v)(\Psi(v') - \Psi(v))}) \\ &= (v_{\mathfrak{p}}(\Psi(v)) + v_{\mathfrak{p}}(\Psi(v) - \Psi(v')))/2 = m/2^n, \end{aligned} \tag{3.32}$$

and it follows that,

$$k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(u)) = k_{\mathfrak{p}}^{\mathrm{alg}}(\sqrt{-\Psi(v)(\Psi(v') - \Psi(v))}) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^n}). \tag{3.33}$$

Moreover, by the inductive assumption,

$$\begin{aligned} v_{\mathfrak{p}}(\Psi(u)) = v_{\mathfrak{p}}(\Psi(u')) &= v_{\mathfrak{p}}(\Psi(v) - (\Psi(v') - \Psi(v)) \pm 2\sqrt{-\Psi(v)(\Psi(v') - \Psi(v))}) \\ &= \min(v_{\mathfrak{p}}(\Psi(v)), v_{\mathfrak{p}}(\Psi(v) - \Psi(v')), v_{\mathfrak{p}}(\sqrt{-\Psi(v)(\Psi(v') - \Psi(v))}) = 0. \end{aligned} \tag{3.34}$$

This proves the claim for all $n \geq 1$.

We also claim that for each $n \geq 1$ and every vertex $v \in |\mathcal{L}|_n$, we have $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(v)) \subseteq k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$. Indeed, as above, this is true for $n = 1$, and the claim for all $n \geq 1$ follows from the fact that if $v \in |\mathcal{L}|_{\geq 2}$, then $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(v))$ is clearly an extension of degree at most 2 over $k_{\mathfrak{p}}^{\mathrm{alg}}(\Psi(\tilde{v}))$. Thus, $k_{\mathfrak{p}}^{\mathrm{alg}}(\{\Psi(v)\}_{v \in |\mathcal{L}|_{\leq n} \setminus \{v_0\}}) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$. Applying Proposition 3.3.2, we have

$$k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}}) \subseteq k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^n]) \subseteq k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^n}). \tag{3.35}$$

Moreover, for $n = 1$, as above we have $k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2]) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$. Suppose that $k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^n]) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^n})$ for some $n \geq 2$. Then there is some positive integer $m \leq n - 1$ such that $k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^{m+1}])/k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^m])$ is a cyclic extension of degree ≥ 4. This is impossible, since Corollary 2.3.3(b) implies that $\mathrm{Gal}(k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^{m+1}])/\mathrm{Gal}(k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^m])$ is isomorphic to a subgroup of $\Gamma(2^m)/\Gamma(2^{m+1}) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Therefore, $k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^n]) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{n-1}})$ for each $n \geq 1$, which is the statement of (a).

In order to prove (b), we first show that there exists a non-backtracking infinite path $\{v_0, v_1, v_2, ...\}$ such that $\Psi(v_i) \in k_{\mathfrak{p}}^{\mathrm{alg}}$ for $i = 1, 2, 3, ...$ Let v_1 be the vertex in $|\mathcal{L}|_1$ such that $\Psi(v_1) = -\lambda \in k_{\mathfrak{p}}^{\mathrm{alg}}$. Then clearly the values of $\Psi(u)$ for the two vertices $u \in |\mathcal{L}|_2$ such that $v_1 = \tilde{u}$ are $-\lambda + 2 \pm 2\sqrt{1-\lambda}$. Since $v_{\mathfrak{p}}(2\sqrt{1-\lambda}) = 0$, it is clear that for at least one such vertex u, $v_{\mathfrak{p}}(\Psi(u)) = 0$. Let v_2 be this vertex, and note that $\Psi(v_2) \in k_{\mathfrak{p}}^{\mathrm{alg}}$ and $v_{\mathfrak{p}}(\Psi(v_2)) = v_{\mathfrak{p}}(\Psi(v_2) - \Psi(v_2')) = 0$. Now assume inductively that for some $n \geq 0$, we have a non-backtracking path $\{v_0, v_1, v_2, ..., v_n\}$ such that $\Psi(v_i) \in k_{\mathfrak{p}}^{\mathrm{alg}}$ for $i = 1, 2, ..., n$ and $v_{\mathfrak{p}}(\Psi(v_i)) = v_{\mathfrak{p}}(\Psi(v_i) - \Psi(v_i')) = 0$. It is clear that the values of $\Psi(u)$ for the two vertices $u \in |\mathcal{L}|_{n+1}$ such that $v_n = \tilde{u}$ are $\Psi(v_n) - (\Psi(v_n') - \Psi(v_n)) \pm 2\sqrt{-\Psi(v_n)(\Psi(v_n') - \Psi(v_n))}$. Since the inductive assumption implies that $v_{\mathfrak{p}}(2\sqrt{-\Psi(v_n)(\Psi(v_n') - \Psi(v_n))}) = 0$, it is clear that for at least one such vertex u, $v_{\mathfrak{p}}(\Psi(u)) = 0$. Let v_{n+1} be this vertex; one checks again that $\Psi(v_{n+1}) \in k_{\mathfrak{p}}^{\mathrm{alg}}$ and $v_{\mathfrak{p}}(\Psi(v_{n+1})) = v_{\mathfrak{p}}(\Psi(v_{n+1}) - \Psi(v_{n+1}')) = 0$. In this way, we construct the desired infinte path $\{v_0, v_1, v_2, ...\}$.

Now there is a corresponding sequence of embedded subgroups $\{0\} < N_1 < N_2 < ...$ of $E_\lambda(\bar{k})$ such that each N_i is the cyclic subgroup of order 2^i corresponding to v_i. One checks using Theorem 2.4.1 (with Proposition 2.6.4) that the image of $\mathrm{Gal}(\bar{k}/k_{\mathfrak{p}}^{\mathrm{alg}})$ does not contain the scalar $-1 \in \mathrm{SL}(T_2(E_\lambda))$. It then follows from the above discussion and from Lemma 3.2.11 that $\mathrm{Gal}(\bar{k}/k_{\mathfrak{p}}^{\mathrm{alg}})$ fixes each of these subgroups elementwise. The subgroups N_i induce a cyclic $\mathbb{Z}_2$-submodule N of $T_2(E_\lambda)$. It is clear that the reduction modulo 2 of N is N_1, which is $\langle (0,1) \rangle < E_\lambda[2]$ since $\Psi(v_1) = -\lambda$. Let $a \in T_2(E_\lambda)$ be a generator of N; clearly, the image of a modulo 2 is $(0,1) \in E_\lambda[2]$. Since the image of $\mathrm{Gal}(\bar{k}/k_{\mathfrak{p}}^{\mathrm{alg}})$ in $\mathrm{SL}(T_2(E_\lambda))$ acts trivially on $\langle a \rangle \subset T_2(E_\lambda)$, it must be generated by some power of the transvection T_a. Let s be the greatest integer such that $2^s | m$. Since $k_{\mathfrak{p}}^{\mathrm{alg}}(E_\lambda[2^{s+2}]) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{m/2^{s+1}}) = k_{\mathfrak{p}}^{\mathrm{alg}}(\pi^{1/2})$ is quadratic over $k_{\mathfrak{p}}^{\mathrm{alg}}$, the Galois image modulo 2^{s+1} must be an order-2 subgroup of $\mathrm{SL}(E_\lambda[2^{s+2}])$. It follows that the Galois image is generated by $T_a^{2^{s+1}}$. Since $\langle T_a^{2^{s+1}} \rangle = \langle T_a^{2m} \rangle \subset T_2(E_\lambda)$, the statement of (b) is proved.

□

Remark 3.4.2. The j-invariant of E_λ is $2^8(\lambda^2 - \lambda + 1)^3/\lambda^2(\lambda - 1)^2$; thus, $v_{\mathfrak{p}}(j(E_\lambda)) < 0$. The hypotheses of Proposition 3.4.1 therefore imply that E_λ has multiplicative reduction at $\mathfrak{p}$. Then in this case, one may use the theory of Tate curves to show that the Galois image contains a power of a transvection as in the statement of Proposition 3.4.1 (this is Exercise 5.13(b) of [27] with $\ell = 2$; see also [24], A.1.5).

Proposition 3.4.3. *Let E_λ be the elliptic curve over k defined by the equation $y^2 = x(x-1)(x-\lambda)$ with $\lambda \in k$. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be primes of k which do not lie over 2, and let $v_\mathfrak{p}, v_{\mathfrak{p}'} : k^\times \to \mathbb{Z}$ be the respective (normalized) valuations. Suppose that $m := v_\mathfrak{p}(\lambda) > 0$ and $m' := v_{\mathfrak{p}'}(\lambda - 1) > 0$, and let s and s' be the greatest integers such that $2^s | m$ and $2^{s'} | m'$. Then the image under ρ_2 of $\mathrm{Gal}(\bar{k}/k)$ contains $\Gamma(2^{s+s'+2}) \lhd \mathrm{SL}(T_2(E_\lambda))$; in particular, $G \cap \mathrm{SL}(T_2(E_\lambda))$ is open with finite index in $\mathrm{SL}(T_2(E_\lambda))$.*

Proof. Define the algebraic extensions $k_\mathfrak{p}^{\mathrm{alg}}, k_{\mathfrak{p}'}^{\mathrm{alg}} \supset k$ as above. Then since $k \subset k_\mathfrak{p}^{\mathrm{alg}}, k_{\mathfrak{p}'}^{\mathrm{alg}}$, the image under ρ_2 of $\mathrm{Gal}(\bar{k}/k)$ contains the images of $\mathrm{Gal}(\bar{k}/k_\mathfrak{p}^{\mathrm{alg}})$ and of $\mathrm{Gal}(\bar{k}/k_{\mathfrak{p}'}^{\mathrm{alg}})$ in $\mathrm{SL}(T_2(E_\lambda))$. Proposition 3.4.1 says that there is some $a \in T_2(E_\lambda)$ whose image modulo 2 is $(1,0) \in E_\lambda[2]$, and some $a' \in T_2(E_\lambda)$ whose image modulo 2 is $(0,0) \in E_\lambda[2]$, such that the images of $\mathrm{Gal}(\bar{k}/k_\mathfrak{p}^{\mathrm{alg}})$ and of $\mathrm{Gal}(\bar{k}/k_{\mathfrak{p}'}^{\mathrm{alg}})$ are generated by $T_a^{2^{s+1}}$ and $T_{a'}^{2^{s'+1}}$ respectively. Clearly $a, a' \in T_2(E_\lambda)$ are independent, because their images modulo 2 are distinct elements of order 2 in $E_\lambda[2]$. Thus, with respect to the $\mathbb{Z}_2$-basis $\{a, a'\}$ of $T_2(E_\lambda)$, the cyclic subgroups of $\mathrm{SL}(T_2(E_\lambda))$ generated by $T_a^{2^{s+1}}$ and $T_{a'}^{2^{s'+1}}$ are generated by the matrices $\begin{bmatrix} 1 & 2^{s+1} \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 2^{s'+1} & 1 \end{bmatrix}$ respectively. The proposition then follows from the elementary lemma below.

□

Lemma 3.4.4. *Let $n, n' \geq 0$ be integers. The subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ generated by the matrices $A := \begin{bmatrix} 1 & 2^n \\ 0 & 1 \end{bmatrix}$ and $A' := \begin{bmatrix} 1 & 0 \\ 2^{n'} & 1 \end{bmatrix}$ contains $\Gamma(2^{n+n'}) \lhd \mathrm{SL}_2(\mathbb{Z}_2)$.*

Proof. It suffices to show that the images of A and A' modulo 2^r generate a subgroup of $\mathrm{SL}_2(\mathbb{Z}/2^r\mathbb{Z})$ containing $\Gamma(2^{n+n'})/\Gamma(2^r)$ for each $r \geq n + n'$. This is trivially true for $r = n + n'$. Assume inductively that this statement holds for some $r \geq n + n'$. Note that the surjectivity of each reduction-modulo-2^i map $\mathrm{SL}_2(\mathbb{Z}_2) \to \mathrm{SL}_2(\mathbb{Z}/2^i\mathbb{Z})$ (see Theorem 7.12 of [21]) implies that the obvious map $\mathrm{SL}_2(\mathbb{Z}/2^{r+1}) \to \mathrm{SL}_2(\mathbb{Z}/2^r)$ is surjective. Thus, to prove the statement for $r+1$, it will suffice to show that the subgroup of $\mathrm{SL}(\mathbb{Z}/2^{r+1}\mathbb{Z})$ generated by the images of A and A' contains $\Gamma(2^r)/\Gamma(2^{r+1})$. Straightforward calculations show that the images modulo 2^{r+1} of $A^{2^{r-n}}$, $(A')^{2^{r-n'}}$, and $(AA'A^{-1}A'^{-1})^{r-n-n'}$ generate $\Gamma(2^r)/\Gamma(2^{r+1})$, as desired.

□

Example 3.4.5. We compute the 2-adic image of $\mathrm{Gal}(\bar{k}/k(\mu_2))$ for the elliptic curve $E_7 : y^2 = x(x-1)(x-7)$ over $k = \mathbb{Q}$ as follows.

We apply Proposition 3.4.3, with $\lambda = 7$, $\mathfrak{p} = (7)$, and $\mathfrak{p}' = (3)$. Since 7 and 3 respectively divide $\lambda = 7$ and $\lambda - 1 = 6$ exactly once, we have $s = s' = 0$, and the proposition shows that $G \cap \mathrm{SL}(T_2(E_7))$ contains $\Gamma(4)$. We will therefore be able to fully describe $G \cap \mathrm{SL}(T_2(E_7))$ once we have determined its image modulo 4.

From the proof of Proposition 3.4.3, we see that $G \cap \mathrm{SL}(T_2(E_7))$ contains transvections T_a^2 and $T_{a'}^2$ for some $a, a' \in T_2(E_7)$ whose images modulo 2 are the points $(1,0), (0,0) \in E_7[2]$. The images modulo 4 of these transvections generate a subgroup of order 4 of $\Gamma(2)/\Gamma(4) \lhd \mathrm{SL}(E_7[4])$. Meanwhile, Theorem 1.2.2(a) shows that $\mathbb{Q}(E_7[4]) = \mathbb{Q}(\zeta_4, \sqrt{6}, \sqrt{7})$, which is Galois over $\mathbb{Q}(\zeta_4)$ with degree 4. Therefore, the image modulo 4 of $G \cap \mathrm{SL}(T_2(E_7))$ coincides with the subgroup of $\Gamma(2)/\Gamma(4)$ generated by the images of these two transvections. Thus, the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_2))$ is isomorphic to

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_2) \mid a \equiv d \equiv 1 \pmod 4,\ b \equiv c \equiv 0 \pmod 2 \right\},$$

via any $\mathbb{Z}_2$-basis of $T_2(E_7)$ whose image modulo 2 is the $\mathbb{Z}/2\mathbb{Z}$-basis $\{(1,0),(0,0)\}$ of $E_7[2]$.

Chapter 4

Dyadic torsion of 2-dimensional hyperelliptic Jacobians

Throughout this chapter, as in Chapter 3, k is any field of characteristic different from 2. Fix an integer $d \geq 3$; let $\alpha_1, \alpha_2, ..., \alpha_d$ be transcendental and independent over k; and let K be the subfield of $k(\{\alpha_i\}_{i=1}^d)$ generated over k by the symmetric functions of the α_i's. Again, let C be a smooth projective model of the hyperelliptic curve over K given by the equation in (3.1), and let J be its Jacobian. The main goal of this chapter is to describe generators of the extension of K over which all 2-power torsion is defined when $d = 5$ or $d = 6$ – that is, when the genus is $g = 2$.

In the following section, we will construct a 15-regular tree associated to J and develop the notion of a "decoration" on a 15-regular tree which will be needed to state the main result; this is somewhat analogous to the 3-regular tree and "decoration" developed in Chapter 3. The main result (Theorem 4.2.1) will be stated and proved in §4.2. In §4.3, we will apply the constructions developed in §4.2 to obtain Proposition 4.3.1.

4.1 Construction of decorations for genus 2

4.1.1 Preliminary results on the Weil pairing

Before constructing the desired 15-regular tree associated to J, we state and prove some technical lemmas involving the Weil pairing on Jacobian surfaces. In this subsection, we will drop the assumption that $d = 5$ or $d = 6$, so that

J is the Jacobian of a hyperelliptic curve of any (positive) genus g. Let $T_2(J)$ denote the 2-adic Tate module of J, and let $V_2(J) = T_2(J) \otimes \mathbb{Q}_2$. Then $V_2(J)$ is a $2g$-dimensional vector space over $\mathbb{Q}_2$ which contains the rank-$2g$ $\mathbb{Z}_2$-lattice $T_2(J)$. We denote the Weil pairing on $T_2(J)$ by $e_2 : T_2(J) \times T_2(J) \to T_2(\mu)$, and for each $n \geq 0$, we write $\bar{e}_2^{(n)} : J[2^n] \times J[2^n] \to \mu_{2^n}$ for the Weil pairing on $J[2^n]$. Below we will freely use a well-known identity of the Weil pairing ([13], Lemma 16.1): for $n \geq m$ and $P, Q \in J[2^n]$,

$$\bar{e}_2^{(n)}(P, Q) = \bar{e}_2^{(m)}(2^{n-m}P, 2^{n-m}Q). \tag{4.1}$$

For any $n \geq 0$, we say that a subgroup $N < J[2^n]$ is *Weil isotropic* if $\bar{e}_2^{(n)}(P, Q) = 1$ for all $P, Q \in N$, and that it is *maximal Weil isotropic* if it is not properly contained in any other Weil isotropic subgroup of $J[2^n]$. More generally, for any module over any ring which is equipped with an alternating bilinear pairing, we define "isotropic" and "maximal isotropic" similarly.

Lemma 4.1.1. *Let M be a free module of (finite) even rank $2m$ over a finite commutative ring Σ, equipped with a nondegenerate alternating bilinear pairing $e : M \times M \to \Sigma$. Then an isotropic submodule of M is maximal isotropic if and only if it has cardinality $|\Sigma|^m$.*

Proof. Let N be an isotropic submodule of M, and let

$$N^\perp = \{\mu \in M \mid e(\mu, \nu) = 0 \ \forall \nu \in N\}.$$

Since N is isotropic, $N \subseteq N^\perp$. Clearly, N is a maximal isotropic submodule if and only if $N = N^\perp$; thus, it suffices to show that $|N^\perp| = |M|/|N| = |\Sigma|^{2m}/|N|$.

Define a map from M to its dual space M^* given by $\mu \mapsto e(\mu, \cdot)$. Since e is nondegenerate, this is an isomorphism. Moreover, it maps $N^\perp$ to the submodule $\{\alpha \in M^* \mid \alpha(N) = 0\} \cong (M/N)^*$, which has cardinality $|M/N|$. Thus, $N^\perp$ has cardinality equal to $|M|/|N|$, as desired.

□

Lemma 4.1.2. *Let M be a vector space of dimension 4 over $\mathbb{F}_2$, equipped with a nondegenerate alternating bilinear pairing $e : M \times M \to \mathbb{F}_2$. Then M has exactly 15 maximal isotropic subspaces.*

Proof. This is well known and can be proved using elementary methods, for instance, choosing a symplectic basis of M and checking all subspaces of

dimension 2. Alternately, one can prove the lemma in the case of $M = J[2]$ by noting that, as in the proof of Proposition 4.1.11(a), there are exactly 15 permutation equivalence class representatives $R \in \mathcal{R}$ with $|R| = B$, which are in one-to-one correspondence with the maximal Weil isotropic subgroups of $J[2]$ as a result of Proposition 4.1.4.

□

Lemma 4.1.3. *Let J be the Jacobian of a curve, whose principal polarization determines a Weil pairing $e_2 : T_2(J) \times T_2(J) \to T_2(\mu)$. Let J' be another abelian variety, and let $\phi : J \to J'$ be an isogeny whose kernel is a maximal Weil isotropic subgroup of $J[2]$. Then J' has a principal polarization which determines a Weil pairing $e_2' : T_2(J') \times T_2(J') \to T_2(\mu)$ such that $e_2'(\phi(P), \phi(Q)) = e_2(P, Q)^2$ for all $P, Q \in T_2(J)$.*

Proof. Let $\lambda : J \xrightarrow{\sim} J^\vee$ be the canonical principal polarization on J, and let $\phi^\vee : (J')^\vee \to J^\vee$ be the dual isogeny corresponding to ϕ. Then Proposition 16.8 of [13], applied to the polarization 2λ, shows that J' has a polarization $\lambda' : J' \to (J')^\vee$ such that $\phi^\vee \circ \lambda' \circ \phi = 2\lambda$. By comparing degrees with the help of Lemma 4.1.1, we see that λ' is a principal polarization. Then by Lemma 16.2(c) of [13],

$$e_2'(\phi(P), \phi(Q)) = e_2(P, \lambda^{-1}(\phi^\vee \circ \lambda' \circ \phi(Q))) = e_2(P, 2Q) = e_2(P, Q)^2. \quad (4.2)$$

□

Lemma 4.1.4. *Let J be the Jacobian of the hyperelliptic curve C defined over K by (3.1), where the degree is any integer $d \geq 3$. With notation as in Proposition 1.2.1, let $P, P' \in J[2]$ be represented by divisors e_U and $e_{U'}$ respectively, where U and U' are even-cardinality subsets of the set of branch points B of C. Then $\bar{e}_2^{(1)}(P, P') = (-1)^{|U \cap U'|} \in \mu_2$.*

Proof. First assume that U and U' are disjoint; we will show that $\bar{e}_2^{(1)}(P, P') = 1$. If one of these sets is empty, say U, then $P = 0 \in J[2]$ and $\bar{e}_2^{(1)}(P, P') = 1$ and we are done, so assume that U and U' are both nonempty. If $U \cup U' = B$, then $P = P'$ by Proposition 1.2.1(a), and $\bar{e}_2^{(1)}(P, P') = 1$ and we are done. Now assume that $U \cup U' \subsetneq B$, and let $\beta \in \mathbb{P}^1_{\bar{K}} \setminus \{\infty\}$ be a branch point in $B \setminus (U \cup U')$. Then if d is odd (resp. if d is even), $|U'|(\infty) - |U'|(\beta, 0) \in \mathrm{Div}^0(C)$ (resp. $\frac{|U'|}{2}(\infty_1) + \frac{|U'|}{2}(\infty_2) - |U'|(\beta, 0) \in \mathrm{Div}^0(C)$) is the principal divisor of the function $(x - \beta)^{-|U'|/2} \in \bar{K}(C)$; adding this principal divisor to $e_{U'}$, we

see that P' is represented by the divisor $D_{P'} := \sum_{\alpha' \in U'}(\alpha, 0) - |U'|(\beta, 0) \in \mathrm{Div}^0(C)$. Now it is clear that $D_P := e_U$ and $D_{P'}$ are divisors representing P and P' respectively which have disjoint support. It is then shown in [11] (VI, §4, Theorem 12) that $\bar{e}_2^{(1)}(P, P')$ may be determined as follows. Let f_P and $f_{P'}$ be functions in $\bar{K}(C)$ whose principal divisors are $2D_P$ and $2D_{P'}$ respectively; then

$$\bar{e}_2^{(1)}(P, P') = \frac{f_P(D_{P'})}{f_{P'}(D_P)}, \tag{4.3}$$

where the evaluation of a function in $\bar{K}(C)$ at a divisor in $\mathrm{Div}^0(C)$ is defined multiplicatively. One checks that we may take $f_P = \prod_{\alpha \in U}(x - \alpha)$ and $f_{P'} = (x - \beta)^{-|U'|/2} \prod_{\alpha' \in U'}(x - \alpha')$. Then we compute

$$\bar{e}_2^{(1)}(P, P') = \frac{\prod_{\alpha \in U, \alpha' \in U'}(\alpha' - \alpha) \prod_{\alpha \in U}(\beta - \alpha)^{-|U'|/2}}{\prod_{\alpha' \in U', \alpha \in U}(\alpha - \alpha') \prod_{\alpha \in U}(\alpha - \beta)^{-|U'|/2}} = 1 = (-1)^{|U \cap U'|}. \tag{4.4}$$

Now suppose that U and U' are nonempty subsets whose intersection has even cardinality. Let $U'' = U \cap U'$, and let $P'' \in J[2]$ be the point represented by the divisor $e_{U''} \in \mathrm{Div}^0(C)$. Clearly $P - P''$ and $P' - P''$ are represented by $e_{U \setminus U'}$ and $e_{U' \setminus U''}$ respectively; note that the sets $U \setminus U''$, $U' \setminus U''$, and U'' are mutually disjoint. Using what we have shown above, we see that $\bar{e}_2^{(1)}(P - P'', P' - P'') = \bar{e}_2^{(1)}(P - P'', P'') = \bar{e}_2^{(1)}(P'', P' - P'') = \bar{e}_2^{(1)}(P'', P'') = 1$. Then by bilinearity of $\bar{e}_2^{(1)}$,

$$\bar{e}_2^{(1)}(P, P') = \bar{e}_2^{(1)}((P - P'') + P'', (P' - P'') + P'') = 1 = (-1)^{|U \cap U'|}. \tag{4.5}$$

Finally, suppose that U and U' are nonempty subsets whose intersection has odd cardinality. Assume further that $\bar{e}_2^{(1)}(P, P') = 1$. One checks that for any other subset $U'' \subset B$ such that $|U \cap U''|$ is odd, $|U \cap (U' \circ U'')|$ is even, where $U' \circ U''$ denotes the symmetric difference of U' and U''. Note that if $P'' \in J[2]$ is the point represented by $e_{U''}$, then $P' + P'' \in J[2]$ is represented by $e_{U' \circ U''}$. Then, by bilinearity, and the fact that $\bar{e}_2^{(1)}(P, P' + P'') = 1$ since $|U \cap (U' \circ U'')|$ is even, we have $\bar{e}_2^{(1)}(P, P'') = 1$. Since U'' was chosen to be an arbitrary subset whose intersection with U has odd cardinality, it follows that $\bar{e}_2^{(1)}(P, Q) = 1$ for any $Q \in J[2]$, which contradicts the nondegeneracy of the Weil pairing. Thus, $\bar{e}_2^{(1)}(P, P') = -1 = (-1)^{|U \cap U'|}$, and the statement is proved for all cases.

□

4.1.2 Equivalence classes of isotropic rank-4 $\mathbb{Z}_2$-lattices

We return to the assumption that the degree of the hyperelliptic curve C is $d = 5$ or $d = 6$, so that C has genus $g = 2$ and its Jacobian J is an abelian surface. We define the graph $\mathcal{L}$ as in §3.1.1. Again, the equivalence class in $\mathcal{L}$ of a lattice Λ will be denoted $[\Lambda]$, and we let $\Lambda_0 = T_2(J)$. Proposition 3.1.1 furnishes a bijection between the vertices of $\mathcal{L}$ and the finite subgroups of $J[2^\infty]$ which do not contain all of $J[2]$. Now we define S to be the induced subgraph of $\mathcal{L}$ whose set of vertices $|S| \subset |\mathcal{L}|$ consists of all vertices mapping under this bijection to subgroups of $J[2^\infty]$ which are maximal Weil isotropic in $J[2^n]$ for some $n \geq 0$.

In order to prove our result on the structure of S (Proposition 4.1.6), we first need a lemma.

Lemma 4.1.5. *Let v be a vertex of S; let N_v be the subgroup of $J[2^\infty]$ corresponding to it as in Proposition 3.1.1; and let $m(v)$ be the (unique) integer such that $N_v < J[2^{m(v)}]$ is maximal Weil isotropic. Let v' be a vertex adjacent to v, and let $N_{v'}$ and $m(v')$ be defined similarly. Then,*

a) N_v has rank 2 or 3; and

b) either $m(v') = m(v) + 1$ and $N_{v'} > N_v$, or $m(v') = m(v) - 1$ and $N_{v'} < N_v$. In either case, the induced quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proof. Since $J[2^{m(v)}]$ is a free $\mathbb{Z}/2^{m(v)}\mathbb{Z}$-module of rank 4, N_v may be viewed as a $\mathbb{Z}/2^{m(v)}\mathbb{Z}$-module of rank at most 4. By Lemma 4.1.1, the order of N_v is 2^{2n}, which forces the rank to be at least 2. If the rank of N_v were equal to 4, N_v would contain $J[2]$, so the rank is 2 or 3, which is the statement of (a).

Let Λ' and Λ be lattices representing v' and v respectively such that one lattice is contained in the other with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then, after possibly replacing Λ' with $2^{-1}\Lambda'$ and then possibly multiplying both lattices by a suitable scalar, one can assume that Λ contains Λ_0 but not $2^{-1}\Lambda_0$ and that $\Lambda' > \Lambda$ with $\Lambda'/\Lambda \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The latter condition implies that Λ' does not contain $2^{-1}\Lambda$. Clearly $2^{m(v)+1}$ kills both Λ/Λ_0 and Λ'/Λ_0, and as in the proof of Proposition 3.1.1(b), each may be identified with a subgroup of $J[2^{m(v)+1}]$. As in the proof of Proposition 3.1.1(b), $\Lambda/\Lambda_0 \cong N_v < J[2^{m(v)}]$; meanwhile, we denote the subgroup of $J[2^{m(v)+1}]$ identified with Λ'/Λ_0 by N'. Then $N' < J[2^{m(v)+1}]$ is a subgroup containing $N_v < J[2^{m(v)}]$ with $N'/N_v \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

If N' does not contain $J[2]$, then clearly $N' = N_{v'}$ and $m(w) = m(\tilde{w}) + 1$. To prove (b), it suffices to prove that if N' does contain $J[2]$, then $m(w) =$

$m(\tilde{w}) - 1$, and $N_{v'} < N_v$ with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Indeed, $2N' < N_v$ since N'/N_v has exponent 2. Then $2N'$ cannot contain $J[2]$ since N_v does not, so $2\Lambda'$ does not contain $2^{-1}\Lambda_0$. Thus, $2\Lambda'$ is the unique lattice representing v' which contains Λ_0 but not $2^{-1}\Lambda_0$. Then by the definition of S, $2N'$ must be maximal Weil isotropic in $J[2^m]$ for some $m \geq 0$; i.e. $2N' = N_{v'}$. Since $|2N'| = |N'|/|J[2]| = 2^{2(m(v)-1)}$, it follows from Lemma 4.1.1 that $N_{v'} = 2N'$ is maximal Weil isotropic in $J[2^{m(v)-1}]$, so $m(v') = m(v) - 1$. Moreover, the fact that $N'/N_v \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $N'/N_{v'} = N'/2N' \cong J[2]$ implies that $N_v/N_{v'} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, as desired.

□

Proposition 4.1.6. *With the above definition, S is a connected,* 15*-regular graph.*

Proof. We first show that S is connected by proving that for any vertex $v \in |S|$, there is a path from v to the root v_0. This is trivially true for $v = v_0$. For any vertex $v \in |S|$, let N_v be the subgroup corresponding to it in the definition of S, and let $m(v)$ be the (unique) integer such that $N_v < J[2^{m(v)}]$ is a maximal Weil isotropic subgroup not containing $J[2]$. Choose a vertex $v \neq v_0$, and assume inductively that the claim holds for $n = m(v) - 1$. By Lemma 4.1.5, N_v has rank 2 or 3. If the N_v has rank 2, then N_v is generated by two elements P_1 and P_2 each of order $2^{m(v)}$, and we define the subgroup $N' < N_v$ to be $\langle 2P_1, 2P_2 \rangle$. If N_v has rank 3, then some element of N_v has order $2^{m(v)}$; otherwise $\bar{e}_2^{(m(v))}(P, Q) = 1$ for all $P \in N_v$ and all $Q \in J[2]$, and by maximality, N_v would contain $J[2]$. We assume without loss of generality that N_v is generated by elements P_1, P_2, and P_3, where P_1 has order $2^{m(v)}$; in this case we define the subgroup $N' < N_v$ to be $\langle 2P_1, 2P_2, P_3 \rangle$. In either case, we have $N' < J[2^{m(v)-1}]$. It is easy to show that N' is Weil isotropic in $J[2^{m(v)-1}]$ using the identity in (4.1). Moreover, in either case, N' has order $2^{2(m(v)-1)}$, so Lemma 4.1.1 implies that N' is a maximal Weil isotropic subgroup of $J[2^{m(v)-1}]$ and represents a vertex $v' \in |S|$. Since in either case, $N' < N_v$ and $N_v/N' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, v' is connected to v by an edge. Then by the inductive assumption, there is a path from v' to v_0, and so there is also a path from v to v_0. Thus, S is connected.

We now prove that S is 15-regular. First of all, Lemma 4.1.2 implies that there are exactly 15 maximal Weil isotropic subgroups of $J[2]$, which implies that there are exactly 15 vertices adjacent to v_0. Now let v be any vertex different from v_0, and let N_v be the corresponding maximal Weil isotropic subgroup of $J[2^{m(v)}]$ not containing $J[2]$. Lemmas 4.1.1 and 4.1.3 imply

that a subgroup $N' < J[2^{m(v)+1}]$ containing N_v is maximal Weil isotropic if and only if N'/N_v is a maximal Weil isotropic subgroup of $(J/N_v)[2]$. Since Lemma 4.1.2 implies that there are exactly 15 maximal Weil isotropic subgroups of $(J/N_v)[2]$, it follows that there are exactly 15 maximal Weil isotropic subgroups of $J[2^{m(v)+1}]$ which contain N_v.

It will now suffice to produce a bijection between the vertices adjacent to v and the 15 maximal Weil isotropic subgroups of $J[2^{m(v)+1}]$ containing N_v. Suppose that v' is a vertex adjacent to v, and let $N_{v'}$ and N_v be the subgroups of $J[2^\infty]$ corresponding to v' and v respectively via Theorem 3.1.1(b). Let $m(v)$ be the (unique) integer such that $N_v < J[2^{m(v)}]$ is maximal Weil isotropic. Then Lemma 4.1.5 implies that $N_{v'}$ is a maximal Weil isotropic subgroup either of $J[2^{m(v)+1}]$ or of $J[2^{m(v)-1}]$. In the former case, let $N' = N_{v'}$, and in the latter case, let $N' = 2^{-1}N_{v'}$, as in the proof of Lemma 4.1.5(b)). In either case, we claim that $N' < J[2^{m(v)+1}]$ is Weil isotropic. Indeed, this is true by construction if $N' = N_{v'}$, and if $N' = 2^{-1}N_{v'}$, then for any $P, Q \in N'$, one easily shows using the identity (4.1) that $\bar{e}_2^{(m(v)+1)}(P,Q) = \bar{e}_2^{(m(v)-1)}(2P,2Q) = 1$. By checking the order of N' and applying Lemma 4.1.1, we verify that N' is a maximal Weil isotropic subgroup of $J[2^{m(v)+1}]$. As in the proof of Lemma 4.1.5(b), $N' > N_v$.

Now assume conversely that N' is a maximal Weil isotropic subgroup of $J[2^{m(v)+1}]$ which contains N_v. Again, Lemmas 4.1.1 and 4.1.3 imply that N'/N_v is a maximal Weil isotropic subgroup of $(J/N_v)[2]$. Any nontrivial subgroup of $(J/N_v)[2]$ has exponent 2, so $N'/N_v \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By an argument similar to the one used in the proof of Lemma 4.1.5, if $N' > J[2]$, then $2N' < N_v$ and $N_v/2N' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now if N' does not contain $J[2]$ (resp. if N' contains $J[2]$), by the construction used in the proof of Proposition 4.1.1(b), N' and N_v (resp. $2N'$ and N_v) correspond to lattices Λ' and Λ each containing Λ_0 but not $2^{-1}\Lambda_0$, and $\Lambda' > \Lambda$ (resp. $\Lambda > \Lambda'$) with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then by the definition of S, the vertex $v' \in |S|$ represented by Λ' is adjacent to v, and we are done.

□

Remark 4.1.7. a) The graph S is not simply connected; in particular, there exist vertices in $|S|_2$ with two distinct simple paths to the root. Assume $\{P_1, P_2, Q_1, Q_2\}$ is a symplectic basis of the free $\mathbb{Z}/4\mathbb{Z}$-module $J[4]$, and consider, for example, the vertex corresponding to the maximal Weil isotropic subgroup $N := \langle 2P_1, P_2, 2Q_1 \rangle < J[4]$. Then $\langle 2P_1, 2P_2 \rangle$ and $\langle 2P_2, 2Q_1 \rangle$ are distinct maximal Weil isotropic subgroups of $J[2]$ which are both contained

in N with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

b) A graph can be constructed for a Jacobian of any dimension g in an analogous manner to S. In general, the graph is still connected and regular, but is only simply connected if $g = 1$ (in which case it is the tree $\mathcal{L}$ from Chapter 3).

4.1.3 A 15-regular tree

We want to define a "decoration" on a tree, as we did in Chapter 3. Unfortunately, as is observed in Remark 4.1.7(a), S is not a tree. However, since S is connected and 15-regular with basepoint v_0, it has a universal covering graph which is a 15-regular tree, which we denote by T. Each vertex $w \in |T|$ corresponds to a non-backtracking path in S beginning at v_0, which we write as a sequence of vertices $\{v_0, v_1, ..., v_n\}$ with each $v_i \in |S|$ and v_{i-1} and v_i adjacent for $1 \leq i \leq n$. We designate $w_0 := \{v_0\}$ as the root of the tree T. Since T is a tree, one may define the "distance" between two vertices in $|T|$ to be the number of edges in a simple path connecting them. For any integer $n \geq 0$, let $|T|_n$ (respectively $|T|_{\leq n}$, $T_{\geq n}$) denote the subset of vertices of T which are of distance n (respectively $\leq n$, $\geq n$) from the root v_0. The fact that T is a tree also implies that each vertex $v \in |T|_n$ for $n \geq 1$ has exactly one "parent", that is, a unique vertex $\tilde{v} \in |T|_{n-1}$ of distance 1 from v.

Proposition 4.1.8. *For any $v \in |S|$, let N_v be the maximal Weil isotropic subgroup of $J[2^m]$ for some m not containing $J[2]$ which uniquely corresponds to v as in the definition of S. For any $w = \{v_0, ..., v_n\} \in |T|$, let $m(w)$ be the unique integer such that $N_{v_n} < J[2^{m(w)}]$ is a maximal Weil isotropic subgroup. Then,*

a) $m(w) \leq n$ and $n - m(w)$ is even.

Let $N_w = 2^{(m(w)-n)/2} N_{v_n}$. Then the assignment $w \mapsto N_w$ has the following properties.

b) If $w \in |T|_n$, then N_w is a maximal Weil isotropic subgroup of $J[2^n]$; and

c) If $w \in |T|_n$ for $n \geq 1$, and $\tilde{w} \in |T|_{n-1}$ is its parent vertex, then $N_w > N_{\tilde{w}}$ and $N_w/N_{\tilde{w}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proof. If $w \in |T|_1$, then $w = \{v_0, v_1\}$ and N_{v_1} is a maximal Weil isotropic subgroup of $J[2]$, so $m(w) = 1$ and parts (a) is clear. Thus, the claim of (a) is proved for $n = 1$ (note that (a) is trivially true for $n = 0$). Choose $n \geq 2$, and assume inductively that all the claims are true for $n - 1$. Choose

$w = \{v_0, v_1, ..., v_n\} \in |T|_n$; then we may apply the inductive assumptions to $\tilde{w} = \{v_0, v_1, ..., v_{n-1}\} \in |T|_{n-1}$. Lemma 4.1.5(b) implies that either $m(w) = m(\tilde{w})+1$ or $m(w) = m(\tilde{w})-1$. In the former case, we have $n-m(w) = (n-1)-m(\tilde{w})$, and in the latter case, we have $n-m(w) = (n-1)-m(\tilde{w})+2$. So in either case, the inductive assumption implies that $m(v) \leq n$ and $n-m(w)$ is even, thus proving part (a).

Let $P, Q \in N_w$. Then $2^{(n-m(w))/2}P, 2^{(n-m(w))/2}Q \in N_{v_n}$ and, using the identity in (4.1), we have $\bar{e}_2^{(n)}(P,Q) = 1$. Thus, N_w is a Weil isotropic subgroup of $J[2^n]$. Since $N_{v_n} < J[2^{m(w)}]$ is maximal Weil isotropic, by Lemma 4.1.1, $|N_{v_n}| = 2^{2m(w)}$. Then

$$|N_w| = |N_{v_n}| \cdot |J[2^{(n-m(w))/2}]| = 2^{2m(w)} \cdot 2^{2(n-m(w))} = 2^{2n}. \tag{4.6}$$

Now Lemma 4.1.1 implies that N_w is maximal Weil isotropic in $J[2^n]$, thus proving part (b).

Lemma 4.1.5(b) implies that if $m(w) = m(\tilde{w}) + 1$, then $N_{v_n} > N_{v_{n-1}}$ with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But $N_w = 2^{(m(w)-n)/2}N_{v_n}$ and $N_{\tilde{w}} = 2^{(m(w)-n)/2}N_{v_{n-1}}$, and it follows immediately that $N_w > N_{\tilde{w}}$ with $N_w/N_{\tilde{w}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Lemma 4.1.5(b) also implies that if $m(w) = m(\tilde{w}) - 1$, then $N_{v_{n-1}} < N_{v_n}$ with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But $N_w = 2^{(m(w)-n)/2}N_{v_n}$ and $N_{\tilde{w}} = 2^{(m(w)-n)/2} \cdot 2N_{v_{n-1}}$, and it follows immediately again that $N_w > N_{\tilde{w}}$ with $N_w/N_{\tilde{w}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus, part (c) is proved.

□

Remark 4.1.9. Note that for general $w, w' \in |T|$, N_w may contain $J[2]$, and that $N_w = N_{w'}$ does not imply that $w = w'$.

4.1.4 Decorations on 15-regular trees

Consider the set $\mathcal{R}$ consisting of all ordered triples (R_1, R_2, R_3), where the R_i's are pairwise disjoint (unordered) 2-element subsets of $\mathbb{P}^1_{\bar{K}} = \bar{K} \cup \{\infty\}$. We say that two such triples $(R_1, R_2, R_3), (R_1', R_2', R_3') \in \mathcal{R}$ are *permutation equivalent* if there is a permutation σ on $\{1, 2, 3\}$ such that $R_i' = R_{\sigma(i)}$ for $i = 1, 2, 3$. Let $\bar{\mathcal{R}}$ be the set of permutation equivalence classes of such triples; we will write $[(R_1, R_2, R_3)] \in \bar{\mathcal{R}}$ for the equivalence class of a triple (R_1, R_2, R_3). If $R = [(R_1, R_2, R_3)] \in \bar{\mathcal{R}}$, let $|R| := R_1 \cup R_2 \cup R_3 \subset \mathbb{P}^1_{\bar{K}}$; clearly this set has cardinality 6 and is well-defined regardless of the choice of representative for R.

Define $M : \mathcal{R} \to M_3(\bar{K})$ to be the map which sends (R_1, R_2, R_3) $= (\{r_{1,1}, r_{1,2}\}, \{r_{2,1}, r_{2,2}\}, \{r_{3,1}, r_{3,2}\}) \in \mathcal{R}$ to the 3-by-3 matrix $M(R)$ with entries in $\bar{K}$ defined as follows. If $\infty \notin R_i$, then the ith row of $M(R)$ is $(r_{i,1}r_{i,2}, -(r_{i,1} + r_{i,2}), 1)$. If $\infty \in R_i$ and we assume without loss of generality that $r_{i,2} = \infty$, then the ith row of $M(R)$ is $(-r_{i,1}, 1, 0)$.

Let $U \subset M_3(\bar{K})$ be the subset of matrices $A = (A_{i,j})$ such that $A_{i,3}x^2 + A_{i,2}x + A_{i,1} \in \bar{K}[x]$ is a squarefree polynomial of degree 1 or 2 for each i, and such that $A_{i,3} = 0$ for at most one $i \in \{1, 2, 3\}$. Note that $M(\mathcal{R}) \subset U$. Now define $N : U \to \mathcal{R}$ as follows. Let $A = (A_{i,j})$ be a matrix in U. Then if $A_{i,3} \neq 0$, let R_i be the set of roots of the (squarefree) quadratic polynomial $A_{i,3}x^2 + A_{i,2}x + A_{i,1} \in \bar{K}[x]$, and if $A_{i,3} = 0$, let $R_i = \{-A_{i,1}/A_{i,2}, \infty\}$. It is easy to check that $N \circ M$ is the identity function on $\mathcal{R}$.

For any matrix $A \in M_3(\bar{K})$, let

$$A^\vee = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{bmatrix} \mathrm{adj}(A),$$

where $\mathrm{adj}(A) := \det(A)A^{-1}$ denotes the adjugate of A.

If $(R_1, R_2, R_3) \in \mathcal{R}$ such that $M((R_1, R_2, R_3))^\vee \in M(\mathcal{R})$, then we assign $\mathrm{Ri}((R_1, R_2, R_3)) = N(M((R_1, R_2, R_3))^\vee)$. It turns out (see Proposition 4.1.11(b) below) that $\mathrm{Ri}((R_1, R_2, R_3))$ is defined for any $(R_1, R_2, R_3) \in \mathcal{R}$. Moreover, this map Ri clearly respects permutation equivalence, so it descends to a map $\mathrm{Ri} : \bar{\mathcal{R}} \to \bar{\mathcal{R}}$, which we call the *Richelot operator* on $\bar{\mathcal{R}}$.

Definition 4.1.10. *A decoration on the 15-regular tree T is a map $\Psi : |T|_{\geq 1} \to \bar{\mathcal{R}}$ with the following properties:*

a) For any two distinct vertices $w, w' \in |T|_{\geq 1}$ with the same parent vertex, $\Psi(w) \neq \Psi(w')$.

b) For any vertex $w \in |T|_1$, $|\Psi(w)| = \{\alpha_i\}_{i=1}^5 \cup \{\infty\}$ if $d = 5$, and $|\Psi(w)| = \{\alpha_i\}_{i=1}^6$ if $d = 6$.

c) For any vertex $w \in |T|_{\geq 2}$, $|\Psi(w)| = |\mathrm{Ri}(\Psi(\tilde{w}))|$ but $\Psi(w) \neq \mathrm{Ri}(\Psi(\tilde{w}))$.

The following proposition shows that there exists a decoration on T.

Proposition 4.1.11. *Let Ψ be a decoration on T. Then we have the following:*

a) There are exactly 15 permutation equivalence classes $R \in \bar{\mathcal{R}}$ with the property that $|R| = \{\alpha_i\}_{i=1}^5 \cup \{\infty\}$.

b) The Richelot operator Ri *is defined for all permutation classes in* $\bar{\mathcal{R}}$ *(in particular,* $\mathrm{Ri}(\Psi(w))$ *is defined for any* $w \in |T|_{\geq 1}$*).*

c) For any $w \in |T|_{\geq 1}$*, up to permutation equivalence, there are exactly* 14 *permutation equivalence classes* $R \in \bar{\mathcal{R}}$ *such that* $|R| = |\mathrm{Ri}(\Psi(w))|$ *but* $R \neq \mathrm{Ri}(\Psi(w))$*.*

Remark 4.1.12. Proposition 4.1.11 implies that a decoration exists via the following argument. For each $N \geq 1$, define F_N to be the set of all functions $\Psi : |T|_{\leq N} \setminus \{v_0\} \to \bar{K}$ which satisfy Definition 4.1.10 for $v \in |T|_{\leq N} \setminus \{v_0\}$. Clearly, each F_N is finite, and for each $N < N'$, there is a map $F_{N'} \to F_N$ by restriction, so it will suffice to show that each F_N is nonempty (because the inverse limit of nonempty sets is also nonempty). Part (a) implies that F_1 is nonempty, and parts (b) and (c) show that if F_N is nonempty, then so is F_{N+1}; thus, F_N is nonempty for all N as desired.

Proof. Note that there are exactly $\frac{1}{3!}\binom{6}{2}\binom{4}{2}\binom{2}{2} = 15$ partitions of 6 objects into 3 pairs. It immediately follows that if S is any element of $\bar{\mathcal{R}}$, there are 15 partitions of the 6 elements of $|S|$ into 3 pairs, and thus, there are 15 permutation equivalence classes R such that $|R| = |S|$. Part (a) follows from the fact that $\{\alpha_i\}_{i=1}^5 \cup \{\infty\}$ is a set of 6 objects. Let (R_1, R_2, R_3) be a representative of a permutation equivalence class in $R \in \bar{\mathcal{R}}$, and let $A = M((R_1, R_2, R_3))$. Then the polynomial $\prod_{i=1}^3 (A_{i,3}x^2 + A_{i,2}x + A_{i,1}) \in \bar{K}[x]$ is squarefree and has degree 5 or 6. By Lemma 8.4.2 of [29], $\prod_{i=1}^3 ((A^\vee)_{i,3}x^2 + (A^\vee)_{i,2}x + (A^\vee)_{i,1}) \in \bar{K}[x]$ is also squarefree of degee 5 or 6. Then $A^\vee \in U$, so $\mathrm{Ri}(R) = N(A^\vee)$ is defined, thus proving part (b). In particular, for any $w \in |T|_{\geq 1}$, $\mathrm{Ri}(\Psi(w))$ is defined and $|\mathrm{Ri}(\Psi(w))| \subset \mathbb{P}^1_{\bar{K}}$ has cardinality 6. Part (c) then follows from the same combinatorial argument as was used to prove (a).

□

4.2 Field of dyadic torsion for genus 2

Define K_n for $n \geq 0$ and K_∞ as in §2.6. Let G be the image of the natural homomorphism $\rho_2 : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(T_2(J)) := \mathrm{Aut}_{\mathbb{Z}_2}(T_2(J))$. As in §2.3.2, for any integer $n \geq 0$, we write $\bar{\rho}_2^{(n)} : \mathrm{Gal}(K_n/K) \to \mathrm{GL}(J[2^n])$ for the homomorphism induced by the natural Galois action on $J[2^n]$, and denote its image by $\bar{G}^{(n)}$. Let $G(n)$ denote the kernel of the natural surjection $G \twoheadrightarrow \bar{G}^{(n)}$; it is the image under ρ_2 of the normal subgroup $\mathrm{Gal}(\bar{K}/K_n) \lhd$

$\mathrm{Gal}(\bar{K}/K)$. Note that $G(0) = G$. For any extension field K' of K, let $K'(\mu_2) = \bigcup_{n=1}^{\infty} K'(\zeta_{2^n})$.

We now state the main theorem, which we will prove in the remainder of this section.

Theorem 4.2.1. *Assume the above notation, and let Ψ be a decoration on T. Set*

$$K'_\infty := K(\{\Psi(v)\}_{v \in |T| \setminus \{v_0\}}).$$

a) Choose $i, j \in \{1, 2, ..., 5\}$ with $i \neq j$, and choose an element $a_{i,j} \in \bar{K}$ whose square is $\alpha_i - \alpha_j$ (resp. $(\alpha_i - \alpha_j) \prod_{\substack{1 \leq l \leq 5 \\ l \neq i,j}} (\alpha_l - \alpha_6)\}_{1 \leq i < j \leq 6}$ if $d = 5$ (resp. if $d = 6$). Then we have

$$K_\infty = K'_\infty(a_{i,j})(\mu_2).$$

b) Any Galois automorphism whose image under ρ_2 is the scalar matrix $-1 \in \Gamma(2)$ acts on K_∞ by fixing $K'_\infty(\mu_2)$ and sending $a_{i,j}$ to $-a_{i,j}$ for $1 \leq i, j \leq 5$, $i \neq j$.

4.2.1 The Richelot isogeny

We define the Richelot isogeny following [29] (see also [9]). The statements of all results in this section assume that the ground field is K, although all results remain true for any algebraic extension of K. If $f \in K[x]$ is a square-free polynomial of degree 5 or 6 and $f = g_1 g_2 g_3$ with each $g_i \in K[x]$ a linear or quadratic polynomial, we will refer to the triple (g_1, g_2, g_3) as a *quadratic splitting* (of $f = g_1 g_2 g_3$). (Note that if (g_1, g_2, g_3) is a quadratic splitting, at most one of the g_i's is linear.) For any quadratic splitting (g_1, g_2, g_3), where each $g_i = g_{i3}x^2 + g_{i2}x + g_{i1}$ with each $g_{ij} \in K$, let g be the matrix in $M_3(\bar{K})$ whose (i, j)th entry is g_{ij}.

Now for any quadratic splitting (g_1, g_2, g_3), for $i = 1, 2, 3$, if g_i is quadratic, let R_{g_i} be the set of roots of g_i, and if g_i is linear, let $R_{g_i} = \{\alpha, \infty\}$ where α is the zero of g_i. Then $(R_{g_1}, R_{g_2}, R_{g_3})$ is clearly an element of $\mathcal{R}$.

For two polynomials $g_1, g_2 \in K[x]$, we denote $[g_1, g_2] = g_1 g_2' - g_2 g_1'$, where the ' symbol indicates the derivative. If (g_1, g_2, g_3) is a quadratic splitting, write $\mathrm{Ri}((g_1, g_2, g_3)) = (h_1, h_2, h_3)$, where $h_i = [h_{i+1}, h_{i+2}]$ for $i = 1, 2, 3$ (here we are treating i as an element of $\mathbb{Z}/3\mathbb{Z}$), and we say that $\mathrm{Ri}((g_1, g_2, g_3))$ is the *Richelot isogenous* quadratic splitting. The next proposition shows

that applying Ri to a quadratic splitting is compatible to applying Ri to the corresponding element of $\mathcal{R}$.

Proposition 4.2.2. *Let (g_1, g_2, g_3) be a quadratic splitting; let $(h_1, h_2, h_3) = \mathrm{Ri}(g_1, g_2, g_3)$; and assume the above notation. Then we have $(R_{h_1}, R_{h_2}, R_{h_3}) = \mathrm{Ri}((R_{g_1}, R_{g_2}, R_{g_3})) \in \mathcal{R}$. In particular, $(R_{h_1}, R_{h_2}, R_{h_3})$ is an element of $\mathcal{R}$, or equivalently, $h_1h_2h_3$ is squarefree of degree 5 or 6.*

Proof. The first statement is straightforward to check through computation, in particular, by proving the identity $h = g^\vee$ (where h is the matrix defined for (h_1, h_2, h_3) as g was for (g_1, g_2, g_3)). The fact that $h_1h_2h_3$ is squarefree of degree 5 or 6 follows from the first statement and Proposition 4.1.11(b) and is the statement of Lemma 8.4.2 in [29] in any case.

□

Recall that C is a hyperelliptic curve of degree $d = 5$ or $d = 6$. As in Chapter 1, let $B \subset \mathbb{P}^1_{\bar{K}}$ be the subset consisting of the x-coordinates of the branch points of C, where the x-coordinate of a point at infinity is $\infty \in \mathbb{P}^1_{\bar{K}}$, so $B = \{\alpha_i\}_{i=1}^5 \cup \{\infty\}$ if $d = 5$ and $B = \{\alpha_i\}_{i=1}^6$ if $d = 6$.

We define a bijection between the maximal Weil isotropic subgroups of $J[2]$ and the permutation equivalence classes $R \in \bar{\mathcal{R}}$ with $|R| = B$ as follows. By Proposition 1.2.1(a), each element of $J[2]$ is represented by a divisor of the form $e_U := \sum_{\alpha \in U}(\alpha, 0) - \#U \cdot (\infty)$, where $U \subseteq B$ has even cardinality, and conversely, any such divisor e_U represents an element of $J[2]$, and that two such subsets $U, U' \subseteq B$, e_U and $e_{U'}$ are equivalent in $\mathrm{Pic}^0(C)$ if and only if $U = U'$ or $U = B \setminus U'$. Thus, any element of $J[2]$ is represented uniquely by a divisor of the form e_U, where $U \subset B$ has cardinality 0 or 2. By slight abuse of notation, if $U \subset B$ has cardinality 0 or 2, we will consider e_U to be an element of $J[2]$. Note that with this notation, the trivial element of $J[2]$ is $e_\varnothing$. It follows from Lemma 4.1.4 that two elements $e_U, e_{U'} \in J[2]$ are Weil isotropic if and only if $U \cap U' = \varnothing$. Thus, if $N < J[2]$ is a maximal Weil isotropic subgroup, then $N = \langle e_U, e_{U'} \rangle$, for some $U, U' \subset B$ each of cardinality 2 and $U \cap U' = \varnothing$. Then $N = \{e_\varnothing, e_U, e_{U'}, e_{U''}\}$, where $U'' = B \setminus (U \cup U')$. Thus, $[(U, U', U'')] \in \bar{\mathcal{R}}$ with $|(U, U', U'')| = U \cup U' \cup U'' = B$, and the equivalence class $[(U, U', U'')]$ is uniquely determined by N. Conversely, any equivalence class $[(R_1, R_2, R_3)] \in \bar{\mathcal{R}}$ with $|[(R_1, R_2, R_3)]| = R_1 \cup R_2 \cup R_3 = B$ determines a maximal Weil isotropic subgroup of $J[2]$ given by $\{e_\varnothing, e_{R_1}, e_{R_2}, e_{R_3}\}$. This defines the bijection.

The following theorem, which states the existence of Richelot isogenies, is proved in [29], §8.4.

Theorem 4.2.3. *Assuming all of the above notations, let (g_1, g_2, g_3) be a quadratic splitting of the polynomial $f(x) \in K[x]$, so $R_g := [(R_{g_1}, R_{g_2}, R_{g_3})] \in \bar{\mathcal{R}}$ with $|R_g| = B$. Let N be the maximal Weil isotropic subgroup of $J[2]$ corresponding to R_g. Assume that $\det(g) \neq 0$. Let C be a smooth projective model of the affine hyperelliptic curve defined over K given by*

$$y^2 = Df(x), \tag{4.7}$$

where $D \in K$, and let J be its Jacobian. Let C' be a smooth projective model of the affine hyperelliptic curve, defined over $K(R_g)$, given by

$$y^2 = \det(g)^{-1} Dh_1h_2h_3, \tag{4.8}$$

where $(h_1, h_2, h_3) = \mathrm{Ri}(g_1, g_2, g_3)$, and let J' be its Jacobian. Then

a) there is an isogeny $\psi : J \to J'$ (defined over $K(R_g)$) whose kernel is N; and

b) the image of $J[2]$ under ψ is the maximal Weil isotropic subgroup of $J'[2]$ corresponding to $\mathrm{Ri}(R_g)$.

The isogeny $\psi : J \to J'$ in the above theorem is known as the *Richelot isogeny* corresponding to N, and C' (resp. J') is often referred to as the *Richelot isogenous* curve (resp. Jacobian). This Richelot isogeny ψ is given explicitly in §3 of [3] as follows. Any divisor class in $\mathrm{Pic}^0(C)$ can be represented by a divisor of the form $(x, y) - (\alpha, 0)$, with $\alpha \in R_{g_1}$. We set $\psi([(x, y) - (\alpha, 0)]) = [(z_1, t_1) - (z_2, -t_2)]$, where z_1 and z_2 are the roots of the polynomial in $g_2(x)h_2(z) + g_3(x)h_3(z) \in F[z]$, and

$$yt_i = \det(g)^{-1} g_2(x)h_2(z_i)(x - z_i) \tag{4.9}$$

for $i = 1, 2$.

Remark 4.2.4. If (g_1, g_2, g_3) is a quadratic splitting of $f(x)$ and if $\det(g) = 0$, then J is isogenous to the product of two elliptic curves (see, for instance, Chapter 14 of [9]). If $(h_1, h_2, h_3) = \mathrm{Ri}((g_1, g_2, g_3))$, then $\det(h) = 2\det(g)^2$, so in this case $\det(h) = 0$ also.

4.2.2 Compositions of $(2,2)$-isogenies of Jacobians

We now assign to each $w \in |T|_n$ a Jacobian surface J_w and an isogeny $\phi_w : J \to J_w$ whose kernel is N_{v_n}, which we will later show is defined over $K(N_{v_n})$.

Set $J_{w_0} = J$, and let $\phi_{w_0} : J \to J_{w_0}$ be the identity isogeny.

For any $w \in |T|_1$, let C_w (resp. J_w) be the Richelot isogenous curve (resp. Jacobian) corresponding to N_w as in Theorem 4.2.3, and let $\phi_w : J \to J_w$ be the corresponding Richelot isogeny. As in the above discussion, the maximal Weil isotropic subgroup $N_w < J[2]$ determines a permutation equivalence class $R_w \in \bar{\mathcal{R}}$, and that $|\mathrm{Ri}(R_w)|$ is the set B of x-coordinates of branch points of C_w. Moreover, the form of (4.9) shows that ϕ_w and J_w are defined over $K(R_w)$.

Now choose $w \in |T|_n$ for some $n \geq 1$, and assume inductively that a curve C_w whose Jacobian is J_w, as well as an isogeny $\phi_w : J \to J_w$ whose kernel is N_w, have been defined. Assume further that we have defined a curve $C_{\tilde{w}}$ whose Jacobian is $J_{\tilde{w}}$ and an isogeny $\phi_{\tilde{w}} : J \to J_{\tilde{w}}$ whose kernel is $N_{\tilde{w}}$. Moreover, assume that we have assigned an element $R_w \in \mathcal{R}$ such that $|R_w|$ is the set of x-coordinates of branch points of $C_{\tilde{w}}$. Let $u \in |T|$ with $w = \tilde{u}$. Then there is a corresponding maximal Weil isotropic subgroup $N_u < J[2^{n+1}]$ containing N_w. So $\phi_w(N_u)$ is a maximal Weil isotropic subgroup of $J_w[2]$, which again determines a permutation equivalence class $R_u \in \bar{\mathcal{R}}$ such that $|R_u|$ is the set of x-coordinates of branch points of C_w. Thus, $|R_u| = |\mathrm{Ri}(R_w)|$. Now let C_u (resp. J_u) be the Richelot isogenous curve (resp. Jacobian) and $\psi_u : J_w \to J_u$ be the Richelot isogeny associated to the maximal Weil isotropic subgroup $\phi_w(N_u) < J_w[2]$ as in Theorem 4.2.3. Then $\phi_u := \psi_u \circ \phi_w : J \to J_u$ is an isogeny whose kernel is N_u. Since the parent of every vertex in $|T|_{n+1}$ is a vertex in $|T|_n$, it follows that through the method described above, we have defined the desired C_w, J_w and ϕ_w for all $w \in |T|_{n+1}$.

In this way, C_w, J_w, ϕ_w, and $R_w \in \mathcal{R}$ are defined for all $w \in |T|_{\geq 1}$. Furthermore, for all $w \in |T|$, we define K_w to be the extension of K obtained by adjoining the coefficients of the Weierstrass equation of C_w given above.

Lemma 4.2.5. *Using the above notation, define $\Psi : |T|_{\geq 1} \to \bar{\mathcal{R}}$ by setting $\Psi(w) = R_w$ for $w \in |T|_{\geq 1}$. Then Ψ is a decoration on T.*

Proof. We have to show that the conditions in Definition 4.1.10 are fulfilled. First, let $w, w' \in |T|_n$ for some $n \geq 1$, and assume they have the same parent

vertex. So there are maximal Weil isotropic subgroups $N_w, N_{w'} < J[2^n]$, $N_{\tilde{w}} < J[2^{n-1}]$, such that $N_w, N_{w'} > N_{\tilde{w}}$. Then $\phi_{\tilde{w}}(N_w)$ and $\phi_{\tilde{w}}(N_{w'})$ are distinct maximal Weil isotropic subgroups of $J_{\tilde{w}}[2]$, and it follows that the associated elements $\Psi(w) = R_w, \Psi(w') = R_{w'} \in \bar{\mathcal{R}}$ must be distinct, thus satisfying part (a).

It is clear from the construction of R_w for $w \in |T|_1$ that part (b) is satisfied.

Finally, let $u = \{v_0, ..., v_{n-1}, v_n, v_{n+1}\} \in |T|_{n+1}$ and $w = \tilde{u} \in |T|_n$. Then by the above construction, $\phi_w = \psi_w \circ \phi_{\tilde{w}}$, where $\psi_w : J_{\tilde{w}} \to J_w$ is the Richelot isogeny associated to the maximal Weil isotropic subgroup $\phi_{\tilde{w}}(N_w) < J_w[2]$. Now suppose that $\Psi(u) = R_u$ coincides with $\mathrm{Ri}(\Psi(w)) = \mathrm{Ri}(R_w)$. Then Theorem 4.2.3(b) says that $\phi_w(N_u)$ is the image of $J_{\tilde{w}}[2]$ under ψ_w. It follows that $N_{\tilde{w}} = 2N_u$. Then by the definition of $w \mapsto N_w$ given in Proposition 4.1.8, $N_{v_{n-1}} = N_{v_{n+1}}$, so $v_{n+1} = v_{n-1}$, which contradicts the fact that the path $u = \{v_0, ..., v_{n-1}, v_n, v_{n+1}\} \in |T|$ is non-backtracking. Thus, $\Psi(u) \neq \mathrm{Ri}(\Psi(w))$, and part (c) is satisfied.

□

Definition 4.2.6. *For any integer $n \geq 0$, define the extension K'_n of K to be the compositum of the fields K_w for all $w \in |T|_{\geq 1}$. Define the extension K'_∞ 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

$$K = K'_0 \subset K'_1 \subset K'_2 \subset ... \subset K'_n \subset ..., \tag{4.10}$$

with $K'_\infty = \bigcup_{n \geq 0} K'_n$.

Lemma 4.2.7. *For any $w \in |T|_n$, let $\{w_0, w_1, ..., w_n\}$ be the sequence of vertices in the path of length n from w_0 to w. Let $\tilde{K}_w$ denote the compositum of the fields K_w for all $w \in \{w_0, w_1, ..., w_n\}$. Then*

$$\tilde{K}_w = K(\{R_w\}_{w \in \{w_1, w_2, ..., w_n\}}).$$

Proof. This is trivial for $n = 0$. Now assume inductively that the statement holds for some $n \geq 0$ and all $w \in |T|_n$. Choose any $w \in |T|_{n+1}$. We may apply the inductive assumption to $\tilde{w}$, since $\tilde{w} \in |T|_n$. One checks from the

form of (4.8) that the curve C_w, and hence also its Jacobian J_w, are defined over $\tilde{K}_{\tilde{w}}(R_w)$.

It will now suffice to show that any field over which J_w is defined must contain $\tilde{K}_{\tilde{w}}(R_w)$, and it will follow that $\tilde{K}_w = \tilde{K}_{\tilde{w}}(R_w)$. To do this, recall that $\phi_w : J \to J_w$ is the composition of $\phi_{\tilde{w}} : J \to J_{\tilde{w}}$ with a Richelot isogeny $\psi_w : J_{\tilde{w}} \to J_w$ whose kernel is the maximal Weil isotropic subgroup $N := \phi_{\tilde{w}}(N_w) < J_{\tilde{w}}[2]$. Let σ be an automorphism of the field $\tilde{K}_{\tilde{w}}(J_{\tilde{w}}[2])$ fixing $\tilde{K}_{\tilde{w}}$, and suppose that σ fixes ψ_w and J_w. Since $\psi_w^\sigma : J_{\tilde{w}} \to J_w^\sigma$ is an isogeny whose kernel is N^σ, it follows that σ stabilizes N as well. Therefore, any field over which ψ_w and J_w are defined must contain the subfield $K' \subset \tilde{K}_{\tilde{w}}(J_{\tilde{w}}[2])$ fixed by all such automorphisms σ which stabilize N. Recall that the 4 elements of N are represented by divisors of the form $e_\varnothing, e_{R_1}, e_{R_2}, e_{R_3} \in \mathrm{Div}^0(J_{\tilde{w}})$, where $R_w = [(R_1, R_2, R_3)]$. Thus, K' is the field fixed by all automorphisms σ which fix (R_1, R_2, R_3). It is easy to check from the construction of $M : \mathcal{R} \to M_3(\bar{K})$ that this field is generated by the entries of $M(R_w)$, and so $K' = \tilde{K}_{\tilde{w}}(R_w)$, as desired.

□

Proposition 4.2.8. *a) For any $n \geq 1$, $K'_n = K(\{\Psi(w)\}_{w \in |T|_{\leq n} \setminus \{w_0\}})$ for any decoration Ψ on T.*

b) As in the statement of Theorem 4.2.1, $K'_\infty = K(\{\Psi(w)\}_{w \in |T|_{\geq 1}})$ for any decoration Ψ on T.

(In particular, the extensions $K(\{\Psi(w)\}_{w \in |T|_{\leq n} \setminus \{w_0\}})$ and $K(\{\Psi(w)\}_{w \in |T|_{\geq 1}})$ do not depend on the choice of decoration Ψ.)

Proof. It follows directly from the definition of K'_n and the statement of Lemma 4.2.7 that

$$K'_n = K(\{R_w\})_{w \in |T|_{\leq n} \setminus \{w_0\}}), \tag{4.11}$$

from which it follows that

$$K'_\infty = K(\{R_w\}_{w \in |T| \setminus \{w_0\}}). \tag{4.12}$$

Therefore, it suffices to show that for any decoration Ψ, $K(\{\Psi(w)\}_{w \in |T|_n \setminus \{w_0\}}) = K(\{R_w\}_{w \in |T|_n \setminus \{w_0\}})$. Choose any decoration Ψ. By Definition 4.1.10 parts (a) and (b), the 15 elements $\Psi(v)$ for $v \in |T|_1$ are representatives of all 15 permutation equivalence classes of elements $R \in \mathcal{R}$ such that $|R| = \{\alpha_i\}_{i=1}^5 \cup \{\infty\}$. It follows that there is a permutation σ on $|T|_1$ such that for each $v \in |T|_1$, $\Psi(v) = R_{\sigma(v)}$. Now assume inductively that for some $n \geq 1$, there is a permutation σ on $|T|_{\leq n}$ which preserves distances between vertices (in particular,

it acts on each $|T|_i$ for $1 \leq i \leq n$), such that $\Psi(w) = R_{\sigma(w)}$ for all $w \in |T|_{\leq n}$. Now choose any $w \in |T|_n$. By Definition 4.1.10 parts (a) and (c), the 14 elements $\Psi(u)$ for any u such that $w = \tilde{u}$ coincide with the 14 elements $R \in \bar{\mathcal{R}}$ such that $|R| = |\mathrm{Ri}(R_w)|$. It follows from the inductive assumption that for each such u, there is a unique u' whose parent is $\sigma(w)$ such that $R_w = \Psi(u')$. Extend σ to be a permutation on $|T|_{n+1}$ by assigning $\sigma(u) = u'$. Since every vertex in $|T|_{n+1}$ has its parent in $|T|_n$, it is clear that σ is defined on $|T|_{n+1}$; moreover, one can easily check that σ is still a permutation which preserves distances between vertices. Thus, we have the equalities

$$\begin{aligned} K(\{\Psi(w)\}_{w \in |T|_{\leq n+1} \setminus \{w_0\}}) &= K(\{R_{\sigma(w)})\}_{w \in |T|_{\leq n+1} \setminus \{w_0\}}) \\ &= K(\{R_w\}_{w \in |T|_{\leq n+1} \setminus \{w_0\}}), \end{aligned} \tag{4.13}$$

and we are done.

□

Proposition 4.2.9. *With the above notation,*

a) the isogeny ϕ_w is defined over $K(N_w)$, and $K_w \subseteq K(N_w)$,

b) for all $n \geq 0$, $K'_n \subseteq K_n$, and equality holds for $n = 0, 1$.

Proof. First of all, we have shown in the proof of Lemma 4.2.7 that ϕ_w is defined over $K(N_w)$ for $w \in |T|_1$, and that in this case, $K_w = \tilde{K}_w$ is the subfield of K_1 fixed by all automorphisms $\sigma \in \mathrm{Gal}(K_1/K)$ which stabilize N_w. It follows that $K_w \subseteq K(N_w)$, and part (a) is proved in the case that $n = 1$. Now by Proposition 4.2.8(a), $K'_1 = K(\{R_w\}_{w \in |T|_1})$. The fact that this is contained in $K(\{\alpha_i\}_{i=1}^6) = K_1$ follows immediately from the fact that $|R_w| = \{\alpha_i\}_{i=1}^6$ for each $w \in |T|_1$. Since K'_1 is the compositum of all such subfields $K(R_w)$, and each $K(R_w)$ is the subfield of K_1 fixed by all automorphisms $\sigma \in \mathrm{Gal}(K_1/K)$ which stabilize N_w, it follows that K'_1 is the subfield of K_1 fixed by the elements of $\mathrm{Gal}(K_1/K)$ which stabilize all maximal Weil isotropic subgroups $N_w < J[2]$. But the only such Galois element is the identity, so $K'_1 = K_1$. This proves equality in the $n = 1$ case of the statement of part (b) (the equality in the $n = 0$ case is trivial). Thus, all claims are proved for $n = 1$.

Now assume inductively that for some $n \geq 1$ and all $w \in |T|_n$, ϕ_w is defined over $K(N_w)$ and $K_w \subseteq K(N_w)$. Choose any $w \in |T|_{n+1}$. We may apply the inductive assumption to $\tilde{w}$, since $\tilde{w} \in |T|_n$. Since N_w is defined over $K(N_w)$ and $\phi_{\tilde{w}}$ is defined over $K(N_{\tilde{w}}) \subseteq K(N_w)$, it follows that $\phi_{\tilde{w}}(N_w)$ is defined over $K(N_w)$. Now the Richelot isogeny $\psi_w : J_{\tilde{w}} \to J_w$ is defined

over $K_{\tilde{w}}(\phi_{\tilde{w}}(N_w)) \subseteq K(N_w)$ by Theorem 4.2.3(a), so $\phi_w = \psi_w \circ \phi_{\tilde{w}}$ is defined over $K(N_w)$. Moreover, since J_w is the image of $J_{\tilde{w}}$ under ψ_w, J_w is defined over $K(N_w)$. Since K_w is the extension of K over which C_w (and hence also J_w) are defined, it follows that $K_w \subseteq K(N_w)$, thus proving part (a).

Now part (a) and the fact that K'_n is the compositum of the fields K_w for all $w \in |T|_{\leq n} \backslash \{w_0\}$ imply that K'_n is contained in the compositum of the extensions $K(N_w)$ for all $w \in |T|_{\leq n} \backslash \{w_0\}$. Since $\{N_w\}_{w \in |T|_{\leq n}}$ clearly generates $J[2^n]$, this compositum is K_n. Thus, $K'_n \subseteq K_n$, which is the statement of (b).

□

4.2.3 The subfield fixed by the scalar subgroup

For any Galois element $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and any element $R = [(R_1, R_2, R_3)] \in \bar{\mathcal{R}}$, we define $R^\sigma = [(R_1^\sigma, R_2^\sigma, R_3^\sigma)] \in \bar{\mathcal{R}}$ by letting each R_i^σ be the cardinality-2 set obtained by letting σ act on the elements of R_i (with the convention that σ fixes ∞). It is clear that this action of $\mathrm{Gal}(\bar{K}/K)$ on $\bar{\mathcal{R}}$ is well defined.

We now characterize the compositum of the fields of definition of these isogenous Jacobians as the fixed subextension of K_∞/K corresponding to the scalar subgroup of G. In order to do so, we first want to determine how the absolute Galois group of K acts on the R_w's defined above. We will adopt the following notation. The automorphism group $\mathrm{GL}(T_2(J))$ acts on the set of rank-4 $\mathbb{Z}_2$-lattices in $V_2(J)$ by left multiplication, and this action stabilizes $|S|$ since $\mathrm{GL}(T_2(J))$ fixes $T_2(J)$). The Galois equivariance of the Weil pairing implies that the image under ρ_2 of G_K in $\mathrm{GSp}(T_2(J)) \subset \mathrm{Aut}_{\mathbb{Q}_2}(V_2(J))$ acts on $|S|$. It is straightforward to check that this action preserves adjacency of the vertices. Thus, the Galois group acts on the set of non-backtracking paths starting at v_0 in S, and so it acts on the vertices of the universal covering graph T; in particular, each $|T|_n$ is stable under this action. We will denote the action of $G \subset \mathrm{GSp}(T_2(J))$ on $|T|$ by $(s, w) \mapsto s \cdot w$ for an automorphism s and a vertex v. Note that this action of G, when restricted to $|T|_{\leq n}$, factors through $G \twoheadrightarrow \bar{G}^{(n)}$. We similarly denote the resulting action of $\bar{G}^{(n)}$ on the induced subtree whose set of vertices is $|T|_n$ by $(\bar{s}, w) \mapsto \bar{s} \cdot w$ for an automorphism $\bar{s}$ and a vertex w.

For any Galois element $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and vertex $w \in |T|$, let $w^\sigma := \rho_2(\sigma) \cdot w$. If $w \in |T|_{\leq n}$ for some $n \geq 1$, then let $w^{\sigma|K_n} = \bar{\rho}_2^{(n)}(\sigma) \cdot w$.

Lemma 4.2.10. *For any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $w \in |T|$, we have $R_w^\sigma = R_{w^\sigma}$ up to permutation equivalence. If $w \in |T|_{\leq n}$, then $R_w^{\sigma|_{K_n}} = R_{w^{\sigma|_{K_n}}}$.*

Proof. Choose any $\sigma \in \mathrm{Gal}(\bar{K}/K)$. We will prove that $R_w^\sigma = R_{w^\sigma}$ for all $w \in |T|_n$ for each $n \geq 1$.

First, let $w \in |T|_1$. Then N_w is the maximal Weil isotropic subgroup of $J[2]$ corresponding to R_w; in other words, if $R_w = (R_1, R_2, R_3)$, then $N_w = \{e_\varnothing, e_{R_1}, e_{R_2}, e_{R_3}\}$, using the notation given in Proposition 1.2.1. Note that $e_{R_i}^\sigma = e_{R_i^\sigma}$. So

$$N_{w^\sigma} = N_w^\sigma = \{e_\varnothing, e_{R_1^\sigma}, e_{R_2^\sigma}, e_{R_3^\sigma}\}, \tag{4.14}$$

and $R_w^\sigma = [(R_1^\sigma, R_2^\sigma, R_3^\sigma)]$ is the corresponding element of $\bar{\mathcal{R}}$. This proves the first statement for $n = 1$. From the construction in Theorem 4.2.3, this implies that $C_{w^\sigma} = C_w^\sigma$, and so $J_{w^\sigma} = J_w^\sigma$. Moreover, one can check from the explicit definition of the Richelot isogeny in §4.2.1 that $\phi_{w^\sigma} = \phi_w^\sigma$.

Now choose $n \geq 2$ and assume inductively that for all $w \in |T|_{n-1}$, $R_{w^\sigma} = R_w^\sigma$, as well as the analogous statements for C_{w^σ}, J_{w^σ}, and ϕ_{w^σ}. Choose $w \in |T|_n$; then $\tilde{w} \in |T|_{n-1}$ and we may apply the inductive assumptions to $\tilde{w}$. Then we have

$$\phi_{\tilde{w}^\sigma}(N_{w^\sigma}) = \phi_{\tilde{w}}^\sigma(N_w^\sigma) = (\phi_{\tilde{w}}(N_w))^\sigma. \tag{4.15}$$

So ψ_{w^σ} is the Richelot isogeny corresponding to the maximal Weil isotropic subgroup $(\phi_{\tilde{w}}(N_w))^\sigma < J_{\tilde{w}}^\sigma[2]$. Then by a similar argument as was used in the $n = 1$ case, $R_{w^\sigma} = R_w^\sigma$. Again, from the construction in Theorem 4.2.3, this implies that $C_{w^\sigma} = C_w^\sigma$, and so $J_{w^\sigma} = J_w^\sigma$. Moreover, again one can check from the explicit definition of the Richelot isogeny in §4.2.1 that $\psi_{w^\sigma} = \psi_w^\sigma : J_{\tilde{w}}^\sigma \to J_w^\sigma$. Thus, $\phi_{w^\sigma} = \psi_{w^\sigma} \circ \phi_{\tilde{w}^\sigma} = \psi_w^\sigma \circ \phi_{\tilde{w}}^\sigma = \phi_w^\sigma$, as desired.

Now let $w \in |T|_{\geq n}$. Then R_w is fixed by all elements of $\mathrm{Gal}(\bar{K}/K_n)$, and one checks from the definitions that $w_\sigma = w_{\sigma|_{K_n}}$ for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Thus, the second statement follows from the first.

□

The statement of the following proposition is identical to that of Proposition 3.2.12, but is now claimed and proved in the case of genus 2.

Proposition 4.2.11. *For all $n \geq 1$, the image of $\mathrm{Gal}(K_n/K_n')$ under $\bar{\rho}_2^{(n)}$ coincides with the subgroup of scalar automorphisms in $\bar{G}^{(n)}$.*

Proof. Fix $n \geq 1$. Since $K'_n \supseteq K_1$ for each $n \geq 1$, we only need to consider the Galois subgroup $\mathrm{Gal}(K_n/K_1)$. Part (a) of Proposition 4.2.8, with the help of Lemma 4.2.5, implies that K'_n is generated over K_1 by the entries of the matrices $M(R_w)$ for all $w \in |T|_{\leq n} \setminus \{w_0\}$. Note that a Galois automorphism fixes all the entries of $M(R_w)$ if and only if it fixes R_w. Therefore, the elements of $\mathrm{Gal}(K_\infty/K_1)$ which fix K'_n are exactly those which fix all of the permutation equivalence classes $R_w \in \bar{\mathcal{R}}$ for all $w \in |T|_{\leq n} \setminus \{v_0\}$. Lemma 4.2.10 implies that, for any $\sigma \in \mathrm{Gal}(K_n/K_1)$, $R_w^{\sigma|_{K_n}} = R_{w^{\sigma|_{K_n}}}$, so the Galois automorphisms in $\mathrm{Gal}(K_n/K_1)$ which fix R_w for all $w \in |T|_{\leq n}$ are the ones sent by $\bar{\rho}_2^{(n)}$ to the elements of $\mathrm{GSp}(J[2^n])$ that fix all vertices in $|T|_{\leq n}$. Let $\zeta \in \mathrm{GSp}(J[2^n])$ be such an automorphism. Then all maximal Weil isotropic subgroups of $J[2^n]$ are stable under ζ. Let P be an element of order 2^n in $J[2^n]$. Then ζ stabilizes the intersection of all maximal Weil isotropic subgroups of $J[2^n]$ which contain P, which is $\langle P \rangle$. So ζ takes P to an odd scalar multiple of P for all P of order 2^n in $J[2^n]$ (and hence for all $P \in J[2^n]$). But the endomorphisms of the $\mathbb{Z}/2^n\mathbb{Z}$-module $J[2^n]$ which take every element to an odd scalar multiple of itself are scalar automorphisms in $\mathrm{GSp}(J[2^n])$. Conversely, scalar automorphisms of G fix all vertices of T, and so $\bar{\rho}_2^{(n)}$ maps $\mathrm{Gal}(K_n/K'_n)$ onto the subgroup of scalar automorphisms in G.

□

With the help of Lemma 3.2.14, which was used to prove Theorem 3.2.1, it is now easy to prove the analogous Theorem 4.2.1.

Proof (of Theorem 4.2.1) . The statement of Theorem 4.2.1 follows directly from Lemma 3.2.14 with the degree taken to be $d = 5$ or $d = 6$, together with Lemmas 4.2.8 and 4.2.11.

4.3 Subextensions associated to the Kummer surface

We retain all notation of the previous sections; in addition, assume that we have chosen $i, j \in \{1, 2, ..., 5\}$ with $i \neq j$ and an element $a_{i,j} \in \bar{K}$ as in the statement of Theorem 4.2.1. Since J is a Jacobian surface, there is an associated quartic surface $\mathcal{K}$ over K, known as the *Kummer surface*, and a morphism $\mathfrak{x} : J \to \mathcal{K}$ defined over K. This surface $\mathcal{K}$ and the morphism $\mathfrak{x}$ are defined explicitly in Chapter 3 of [9]. It is also shown there that for

points $P, Q \in J(\bar{K})$, $\mathfrak{x}(P) = \mathfrak{x}(Q)$ if and only if $Q = \pm P$; in other words, $\mathfrak{x}$ is a quotient map of the obvious multiplicative action of $\{\pm 1\}$ on J. In this way, $\mathfrak{x} : J \to \mathcal{K}$ is analogous to the degree-2 map of an elliptic curve onto the projective x-line. Therefore, it is not surprising that we have an analog of Proposition 3.3.1 for J.

Proposition 4.3.1. *Write $K(\mathfrak{x}(J[2^n]))$ (resp. $K(\mathfrak{x}(J[2^\infty]))$) for the extension of K obtained by adjoining the coordinates of the images under $\mathfrak{x}$ of all elements of $J[2^n]$ (resp. $J[2^\infty]$). Then*

a) $K_n = K(\mathfrak{x}(J[2^n]))(a_{i,j})$ for all $n \geq 2$;
b) $K_n'(\zeta_{2^n}) \subseteq K(\mathfrak{x}(J[2^n]))$ for all $n \geq 1$; and
c) $K_\infty'(\mu_2) = K(\mathfrak{x}(J[2^\infty]))$.

Proof. The Galois equivariance of the Weil pairing implies that $K_n \supset K(\zeta_{2^n})$ for each $n \geq 0$ and that $K_\infty \supset K(\mu_2)$. For any $n \geq 1$, the subgroup of $\mathrm{Gal}(K_n/K)$ which fixes the images under $\mathfrak{x}$ of the points in $J[2^n]$ can be identified with the elements of $G \subset \mathrm{GSp}(T_2(J))$ which send each point $P \in J[2^n]$ either to P or to $-P$. The only such automorphisms in $\mathrm{GSp}(T_2(J))$ are the scalars ± 1. Thus, $K(\mathfrak{x}(J[2^n]))$ is the subextension of K_n corresponding to the subgroup $\bar{G}^{(n)} \cap \{\pm 1\} \lhd \bar{G}^{(n)} \cap \mathrm{GSp}(J[2^n])$, and similarly, $K(\mathfrak{x}(J[2^\infty]))$ is the subextension of K_∞ corresponding to the subgroup $G \cap \{\pm 1\} \lhd G \cap \mathrm{Sp}(T_2(J))$. Part (b) now follows from the fact that, by Galois invariance and Proposition 3.2.12, $K_n'(\zeta_{2^n})$ is the fixed field corresponding to the subgroup of scalars in $G \cap \mathrm{Sp}(T_2(J))$, which contains $G \cap \{\pm 1\}$. Part (c) follows similarly. Note that $a_{i,j} \in K_2$ by Theorem 1.2.2. Therefore, we already have part (a) if $G \cap \{\pm 1\}$ is trivial, so we assume that $-1 \in G$. Then K_n is a quadratic extension of $K(\mathfrak{x}(J[2^n]))$, and a generator is any element in K_n which is not fixed by -1. It follows from Theorem 2.4.1 and Proposition 2.6.4 that $a_{i,j} \in K_2 \subseteq K_n$ is not fixed by -1, hence the statement of part (a).

□

Bibliography

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

[2] Emil Artin. *Geometric algebra. Interscience Tracts in Pure and Applied Mathematics*, (3), 1957.

[3] Peter R. Bending. Curves of genus 2 with sqrt2 multiplication. *arXiv preprint math/9911273*, 1999.

[4] Joan S. Birman. *Braids, links, and mapping class groups. Annals of Mathematical Studies*, (82), 1974.

[5] Glen E. Bredon. *Topology and Geometry. Graduate Texts in Mathematics*, 139, 1993.

[6] Anna Cadoret and Akio Tamagawa. A uniform open image theorem for ℓ-adic representations, I. *Duke Mathematical Journal*, 161(13):2605–2634, 2012.

[7] Edward Fadell and Lee Neuwirth. Configuration spaces. *Math. Scand.*, 10(111-118):4, 1962.

[8] Benson Farb and Dan Margalit. *A Primer on Mapping Class Groups (PMS-49)*. Princeton University Press, 2011.

[9] Eugene Victor Flynn and John William Scott Cassels. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, 1996.

[10] Alexander Grothendieck. Revêtements étales et géométrie algébrique (SGA 1). *Lecture Notes in Math*, 224, 1971.

[11] Serge Lang. *Abelian varieties*. Springer, 1983.

[12] Serge Lang. *Elliptic functions*. Springer, 1987.

[13] James S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer, 1986.

[14] James S. Milne. Jacobian varieties. In *Arithmetic geometry*, pages 167–212. Springer, 1986.

[15] David Mumford. A note of Shimura's paper "Discontinuous groups and abelian varieties". *Mathematische Annalen*, 181(4):345–351, 1969.

[16] David Mumford. *Abelian varieties*, volume 108. Oxford Univ Press, 1974.

[17] David Mumford. Tata lectures on theta I. *Progress in Mathematics*, 28, 1983.

[18] David Mumford. Tata lectures on theta II. *Progress in Mathematics*, 43, 1984.

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

[20] Rutger Noot. On Mumford's families of abelian varieties. *Journal of Pure and Applied Algebra*, 157(1):87–106, 2001.

[21] Vladimir Platonov, Andrei Rapinchuk, and Rachel Rowen. *Algebraic Groups and Number Theory. Pure and Applied Mathematics*, 139, 1993.

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

[23] Jean-Pierre Serre. Lettre à Ken Ribet. *Œuvres. Collected papers, vol. IV.*, 1998, 1985.

[24] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. Addison-Wesley, Advanced Book Program (Redwood City, Calif.), 1989.

[25] 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.

[26] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, pages 492–517, 1968.

[27] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics*, 151, 1994.

[28] Joseph H. Silverman. *The arithmetic of elliptic curves. Graduate Texts in Mathematics*, 106, 2009.

[29] Benjamin Smith. Explicit endomorphisms and correspondences. *Bulletin of the Australian Mathematical Society*, 74(03):479–480, 2006.

[30] Jeffrey Yelton. Dyadic torsion of elliptic curves. *arXiv preprint arXiv:1310.6447*, 2013.

[31] Jeffrey Yelton. Dyadic torsion of 2-dimensional hyperelliptic Jacobians. *arXiv preprint arXiv:1410.8110*, 2014.

[32] Jeffrey Yelton. Images of 2-adic representations associated to hyperelliptic Jacobians. *Journal of Number Theory*, 151:7–17, 2015.

[33] Jiu-Kang Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. *Université Bordeaux I-A2X*, 351, 1996.

[34] Yuri G. Zarhin. Very simple 2-adic representations and hyperelliptic Jacobians. *Moscow Math. J*, 2(2):403–431, 2002.

[35] Yuri G. Zarhin. Families of absolutely simple hyperelliptic Jacobians. *Proceedings of the London Mathematical Society*, 100(1):24–54, 2010.

Vita

Research Interests

Arithmetic Geometry, Abelian Varieties, Elliptic Curves

Education

- Ph.D., The Pennsylvania State University, August 2015
- B.S. in Mathematics, The University of Florida, May 2009

Academic Achievements

- GPA of 3.98 at University of Florida
- GPA of 4.00 at The Pennsylvania State University
- passed all qualifying exams at The Pennsylvania State University upon entrance in August 2009
- passed comprehensive exam at The Pennsylvania State University in November 2011
- passed dissertation defense at The Pennsylvania State University in April 2015

Honors and Awards

- Kermit Sigmon Scholarship, spring 2009
- University Graduate Fellowship at The Pennsylvania State University, for the 2009-2010 academic year
- Raymond and Christine Ayoub Award for outstanding doctoral thesis in algebra or number theory, spring 2015

Preprints and Publications

- "Dyadic Torsion of Elliptic Curves". *arXiv preprint arXiv:1310.6447* (2014), accepted for publication in *European Journal of Mathematics*
- "Images of 2-adic representations associated to hyperelliptic Jacobians". *Journal of Number Theory* (2015)
- "Dyadic torsion of 2-dimensional hyperelliptic Jacobians" *arXiv preprint arXiv:1410.8110* (2014)