ON THE ARITHMETIC OF GENUS 2 CURVES WITH (4,4)-SPLIT JACOBIANS

by

Kevin D. Doerksen
B.Sc., University of Winnipeg, 2001
M.Sc., University of Manitoba, 2004

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Summer 2011

APPROVAL

Name:	Kevin D. Doerksen
Degree:	Doctor of Philosophy
Title of thesis:	On the arithmetic of genus 2 curves with (4,4)-split Jacobians
Examining Committee:	Dr. Steve Ruuth Chair
	Dr. Nils Bruin Senior Supervisor, Simon Fraser University
	Dr. Imin Chen Supervisory Committee, Simon Fraser University
	Dr. Jason Bell Internal Examiner, Simon Fraser University
	Dr. Edward F. Schaefer External Examiner, Santa Clara University
Date Approved:	May 9, 2011

Declaration of
Partial Copyright Licence

Abstract

In this thesis, we study genus 2 curves whose Jacobians allow a decomposition into two elliptic curves. More specifically, we are interested in genus 2 curves C whose Jacobians admit a polarized $(4,4)$-isogeny to a product of elliptic curves. We restrict to base fields of characteristic distinct from 2 or 3, but we do not require them to be algebraically closed.

In the first half of the thesis, we obtain a full classification of principally polarized abelian surfaces that can arise from gluing two elliptic curves together along their 4-torsion and we derive the relation which their absolute invariants must satisfy. In the process, we derive a description of Richelot isogenies between Jacobians of genus 2 curves. Previous literature only considered Richelot isogenies whose kernels are pointwise defined over the base field. We also obtain a Galois theoretic characterization of genus 2 curves which admit multiple Richelot isogenies on their Jacobians. As a corollary to this classification, we obtain a model for the universal elliptic curve over the modular curve of elliptic curves with 4-torsion anti-isometric to $E[4]$.

The final chapter of the thesis considers elements of order m of the Shafarevich-Tate group of an elliptic curve E, denoted $Ш(E/k)[m]$. For a given elliptic curve, E, we consider the question of making $Ш(E/k)[4]$ visible in the sense of Mazur. We show that the visibility argument for $m = 4$ is less tractable than the arguments in the $m = 2$ and $m = 3$ cases. In the $m = 4$ case, we encounter a challenge of trying to find rational points on a K3 surface. We also show that finding the appropriate twist of this surface is a non-trivial problem. Nevertheless, in particular cases, one can proceed with this construction and we conclude the thesis by working through a couple of examples in detail.

Acknowledgments

I would like to express my deep gratitude to my advisor, Dr Nils Bruin, for his patient guidance and continuous support. His piercing questions and helpful comments have been, and continue to be, instrumental in my development as a mathematician.

I would like to thank the members of the Number Theory community in the Vancouver area. The biweekly seminars and regular discussions provide a stimulating environment for research and collaboration. I am particularly grateful to Dr Imin Chen for his initial recruitment and guidance, Dr Jason Bell for keeping me on my toes during our regular coffee breaks, and Dr Peter Borwein for his vision of interdisciplinary collaboration which became the IRMACS centre.

Finally, I would like to thank my parents for their ongoing support and unwavering confidence throughout my academic career.

Contents

List of Figures

Introduction

In this thesis, we study genus 2 curves whose Jacobians allow a decomposition into two elliptic curves. More specifically, we are interested in genus 2 curves C whose Jacobians admit a polarized $(4,4)$-isogeny to a product of elliptic curves $E_1 \times E_2$ (see Section 1.2 for complete definitions). Our aim is to characterize all such genus two curves and to use the corresponding isogeny $\Psi_4 : \mathrm{Jac}(C) \to E_1 \times E_2$ to make elements of order 4 of the *Shafarevich-Tate group* of E_1 visible (see Section 4.3 for definitions).

There are three main results in this thesis.

1. In the process of classifying the genus 2 curves with $(4,4)$-split Jacobians, we work with $(2,2)$-isogenies between Jacobians of genus 2 curves, also known as *Richelot isogenies*. We have a need to work with these isogenies in a more general setting than previous literature had considered. Proposition 2.6 gives us the necessary machinery to do so and is our first main result.

2. The classification of $(4,4)$-split principally polarized abelian surfaces is our second main result. This result is actually split into two theorems, Theorem 3.1 and Theorem 3.2. The first theorem gives models for all possible principally polarized abelian surfaces, J, which admit an optimal $(4,4)$-splitting, including all boundary cases where J is not the Jacobian of a genus 2 curve. The second theorem gives a relation on the absolute invariants of a genus 2 curve which determines whether its Jacobian is $(4,4)$-split.

   As a corollary to this result, in Lemma 3.15 we classify genus 2 curves whose Jacobians admit two polarized $(2,2)$-isogenies and in Proposition 3.12 we obtain a model for the universal elliptic curve over the modular curve of elliptic curves with 4-torsion anti-isometric to $E[4]$.

3. We present our final result in Section 4.6, where we consider elements of order m of

the Shafarevich-Tate group of an elliptic curve E, denoted $Ш(E/k)[m]$. For a given elliptic curve, E, we consider the question of making $Ш(E/k)[4]$ visible in the sense of Mazur [16, p. 16]. We show that the visibility argument for $m = 4$ is less tractable than the arguments in the $m = 2$ and $m = 3$ cases. In the case for $m = 4$, we encounter a challenge of trying to find rational points on a K3 surface. We do, however, show that it may be possible on a case-by-case basis to make elements visible and give a couple of specific examples where visibility occurs.

This thesis is divided into four chapters: one for each of the three key results, together with an introductory chapter.

In the first chapter, we take the reader on a rather gentle, if terse, introduction to arithmetic geometry. The goal of this chapter is to provide sufficient background such that the thesis is self-contained. All classic results and definitions required in later chapters are presented here, together with an appropriate level of context. Some major results would require a more in depth treatment than the few pages that this introduction can afford. In such cases, we state the main theorem(s) and cite appropriate literature where the fastidious reader can sate his or her curiosity.

Although no new results appear in this chapter, we do provide a succinct treatise of the many subtle variations of the notion of split Jacobians and decomposable Jacobians in Section 1.2. Such terminology has been adopted in previous literature (see for example [19, 28, 29, 42, 43]), but the usage of such terms varies subtly from reference to reference.

In Chapter 2, we prove our first main result. We begin by introducing Richelot isogenies as they have appeared in previous literature. Unlike previous literature, however, we do not require the kernels of our isogenies to be pointwise defined over the base fields. We determine the appropriate twist of the codomain necessary to correct for those Richelot isogenies whose kernels are not pointwise defined over the base field.

In Chapter 3, we classify $(4, 4)$-split principally polarized abelian surfaces. We begin by showing that an optimal $(4, 4)$-splitting must factor as a product of a $(2, 2)$-splitting and a polarized $(2, 2)$-isogeny. This leads us to classifying genus 2 curves whose Jacobians admit two polarized $(2, 2)$-isogenies in Section 3.3. With this intermediate step, we are able to finally give the proofs of Theorems 3.1 and 3.2 in Section 3.5.

In the final chapter, we present the problem of attempting to make visible elements of order 4 of the Shafarevich-Tate group of an elliptic curve. In order to do this, we begin

in Sections 4.1 and 4.3 with an introduction to the problem and definitions of the Selmer and Shafarevich-Tate groups of an elliptic curve. We then introduce the general technique of making elements of order m of the Shafarevich-Tate group visible. In Section 4.6 we point out various difficulties one runs into when one tries to apply this technique to the case where $m = 4$. For a given elliptic curve, E, there is a natural way to construct a surface $\mathcal{D}$ which covers the modular curve $X_E^-(4)$ of all elliptic curves E_s with 4-torsion anti-isometric to E such that each point of the surface carries information (as a fibre) of a specific 4-torsion subgroup (as a Galois module) and a particular E_s which has anti-isometric 4-torsion to E. Unfortunately, the class that the fibres represent in $\mathrm{H}^1(k, E[4])$ vary over $X_E^-(4)$. Nevertheless, for fixed values of s, one can proceed with this construction and we present a sample procedure in Section 4.7, together with a couple of examples where visibility occurs.

This thesis also contains two appendices. In Appendix A, we connect our characterization of genus 2 curves with $(4, 4)$-split Jacobians to a classic 1887 result by O. Bolza [1]. We show how his result, when put in modern terminology, is consistent with our characterization up to a twist. This twist can be accounted for the fact that Bolza works over $\mathbb{C}$ whereas our construction is valid over any base field of characteristic distinct from 2 and 3.

Appendix B has been added to improve the flow of previous chapters. Some of our results involved some lengthy equations, each of which take up an entire page to display. These equations have been placed in this appendix to spare the reader and improve the flow of the main text. One of the equations is even too long to display as an appendix, being a polynomial containing almost 5000 monomials with coefficients having over 100 digits. This equation has been supplied electronically [8].

Chapter 1

Preliminaries

1.1 An introduction to arithmetic geometry

In this section, we present a quick introduction to arithmetic geometry. The thesis is targeted at an audience who is already familiar with the field. This section is only intended to serve as a brief reminder of some fundamental definitions to readers with the intent of keeping the thesis self-contained. People who are interested in a more in-depth review of algebraic geometry are encouraged to refer to Hartshorne [22]; for a more in depth review of elliptic curves, see [45, 9].

Throughout the thesis, k will denote a field (usually a number field, but this will always be clarified in each context), $\bar{k}$ will denote the algebraic closure of k, and k^* will denote the group of invertible elements of k. The term *ring* will refer to a commutative ring with a multiplicative identity element.

1.1.1 Algebraic varieties and curves

Definition 1.1. *Affine n-space (over k)* is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \left\{ P = (x_1, \ldots, x_n) \mid x_i \in \bar{k} \right\}.$$

The *set of k-rational points in $\mathbb{A}^n$* is the set

$$\mathbb{A}^n(k) = \left\{ P = (x_1, \ldots, x_n) \mid x_i \in k \right\}.$$

Definition 1.2. *Projective n-space (over k)*, denoted $\mathbb{P}^n = \mathbb{P}^n(\bar{k})$, is the set of all $(n+1)$-tuples

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is non-zero, modulo the equivalence relation given by

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if there exists $\lambda \in \bar{k}^*$ such that $x_i = \lambda y_i$ for all $i \leq n$. An equivalence class

$$\left\{ (\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in \bar{k}^* \right\}$$

will be denoted $[x_0 : \cdots : x_n]$, and $x_0, \ldots, x_n$ are called the *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n(\bar{k})$. The *set of k-rational points in* $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(k) = \left\{ [x_0 : \cdots : x_n] \in \mathbb{P}^n(\bar{k}) \mid x_i \in k \text{ for all } i \leq n \right\}$$

Notice that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. For each $0 \leq i \leq n$, there is an inclusion map

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ (x_0, \ldots, x_n) &\longmapsto [x_0 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n] \end{aligned}$$

Conversely, if we let $U_i \subset \mathbb{P}^n$ be the set of all points with a non-zero i-th homogeneous coordinate,

$$U_i = \{ P = [X_0 : \cdots : X_n] \in \mathbb{P}^n \mid X_i \neq 0 \},$$

then there is a natural bijection

$$\begin{aligned} p_i : U_i &\longrightarrow \mathbb{A}^n \\ [X_0 : \cdots : X_n] &\longmapsto \left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i} \ldots, \frac{X_n}{X_i} \right). \end{aligned}$$

The bijection p_i is called the $i-th$ *affine patch* of $\mathbb{P}^n$.

The primary objects of interest in algebraic geometry are (affine or projective) algebraic varieties. Let $\bar{k}[X] = \bar{k}[X_1, \ldots, X_n]$ be a polynomial ring in n variables.

Definition 1.3. An *(affine) algebraic set* is a subset $V \subset \mathbb{A}^n$ for which there exist $f_1, \ldots, f_j \in \bar{k}[X]$ such that $V = \{ P = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid f_1(P) = \cdots = f_j(P) = 0 \}$. The set

$$I(V) = \left\{ f \in \bar{k}[X] \mid f(P) = 0 \text{ for all } P \in V \right\}$$

forms an ideal of $\bar{k}[X]$, called the *ideal of* V. An algebraic set is said to be *defined over* k if its ideal $I(V)$ can be generated by polynomials in $k[X]$. An affine algebraic set V is called an *(affine) algebraic variety* if $I(V)$ is a prime ideal in $\bar{K}[X]$. An affine algebraic variety, V, is *defined over* k, written V/k, if it is defined over k as an algebraic set. By $I(V/k)$, we mean $I(V) \cap k[X]$.

We can similarly define *(projective) algebraic varieties* by replacing $\mathbb{A}^n$ by $\mathbb{P}^n$ throughout Definition 1.3. In this case, V is called a projective algebraic variety and

$$I(V) = \left\{ f \in \bar{k}[X] \mid f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V \right\}$$

is called the *homogeneous ideal* of V.

An affine variety V can be completed to a projective variety in a very natural way by *homogenizing* the polynomials in the ideal of V. Let $f(x_0, \ldots, x_{n-1}) \in I(V)$ and suppose $\deg(f) = d$. Then

$$f^* = x^d f\left(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right)$$

is called the *homogenization of* f.

Definition 1.4. Let V be an affine algebraic set with ideal $I(V)$, and consider V as a subset of $\mathbb{P}^n$ via the map

$$V \subset \mathbb{A}^n \xrightarrow{\phi_n} \mathbb{P}^n.$$

The *projective closure of* V, denoted $\bar{V}$, is the projective algebraic set whose homogeneous ideal $I(\bar{V})$ is generated by

$$\{ f^*(X) \mid f \in I(V) \}.$$

Definition 1.5. Let V be a projective (affine) variety. A *subvariety* S of V is a subset of V which is itself a projective (affine) variety.

Definition 1.6. Let V be an affine variety. The *affine coordinate ring of* V/k is

$$k[V] := k[X]/I(V/k).$$

The *function field of* V/k is the field of fractions of $k[V]$, and is denoted $k(V)$. One can similarly define $\bar{k}[V]$ and $\bar{k}(V)$ by replacing k by $\bar{k}$ in the definition.

Definition 1.7. The *dimension* of an affine variety V, denoted $\dim(V)$, is the transcendence degree of $\bar{k}(V)$ over $\bar{k}$.

The *dimension* of a projective variety W, denoted $\dim(W)$, is the dimension of $W \cap \mathbb{A}^n$ for some $\mathbb{A}^n \subset \mathbb{P}^n$ for which $W \cap \mathbb{A}^n \neq \emptyset$. Note that the definition of dimension is well-defined: one can show that it is not dependent on the choice of $\mathbb{A}^n$.

Definition 1.8. Let V be an affine variety with generators $f_1, \ldots, f_m \in \bar{k}(X)$ for $I(V)$ and let $P \in V$. Then V is *non-singular* or *smooth at* P if the $m \times n$ matrix defined by

$$a_{ij} = \big(\partial/\partial X_j(P)\big) f_i$$

has rank $n - \dim(V)$. If V is non-singular at every point, then we say that V is *non-singular* or *smooth*.

A projective variety, V, is *non-singular* or *smooth* at a point P if $V \cap \mathbb{A}^n$ is non-singular at P for some $\mathbb{A}^n \subset \mathbb{P}^n$. One can show that this definition is independent of choice of affine patch $\mathbb{A}^n \subset \mathbb{P}^n$.

Throughout the thesis, all varieties will be projective varieties unless explicitly stated otherwise. For the ease of notation, we will often describe these varieties by giving affine models. Nevertheless, one should always keep in mind that we are working with the projective closure of this affine model.

Definition 1.9. The *local ring* of an affine variety V at a point P, denoted $\mathcal{O}_P(V)$, is the localization of $\bar{k}[V]$ at P. In other words,

$$\mathcal{O}_P(V) = \left\{ F \in \bar{k}(V) \mid F = f/g \text{ for some } f, g \in \bar{k}(V) \text{ with } g(P) \neq 0 \right\}.$$

The local ring of a projective variety V at a point P is the local ring of $V \cap \mathbb{A}^n$ at P. We will write $\mathcal{O}_P$ for $\mathcal{O}_P(V)$ where there is no confusion in identifying the underlying variety.

More generally, a local ring, R, is a ring with a unique maximal ideal, M. It is easy to show that the ring defined in Definition 1.9 is in fact a local ring. The maximal ideal of $\mathcal{O}_P(V)$ is given by

$$M_P = \left\{ f \in \bar{k}(V) \mid f(P) = 0 \right\},$$

and the units of $\mathcal{O}_P$ are $\mathcal{O}_P^* = \mathcal{O}_P \setminus M_P$.

Definition 1.10. Let $V_1, V_2 \subset \mathbb{P}^n$ be projective varieties. A *rational map* $\phi : V_1 \to V_2$ is a map of the form $\phi = [f_0, \ldots, f_n]$ where $f_0, \ldots, f_n \in \bar{k}(V_1)$ such that at every point P for which $f_0, \ldots, f_n$ are defined,

$$\phi(P) = [f_0(P), \ldots, f_n(P)].$$

If there exists some $\lambda \in \bar{k}^*$ such that $\lambda f_0, \ldots, \lambda f_n \in k(V_1)$, then ϕ is said to be *defined over* k.

Definition 1.11. A rational map $\phi : V_1 \to V_2$ with $\phi = [f_0, \ldots, f_n]$ is said to be *regular at a point* $P \in V_1$ if there exists some function $g \in \bar{k}(V_1)$ such that

1. For each i, the function gf_i is in the local ring of $V \cap \mathbb{A}^n$ at P (that is to say, it is *regular* at P), and

2. There exists some $j \leq n$ for which $gf_j(P) \neq 0$.

A rational map that is regular at every point is called a *morphism*. A surjective morphism is called a *cover*.

We will be working primarily with projective varieties of dimension 1 or 2.

Definition 1.12. An *(algebraic) curve* is a projective variety of dimension 1. An *(algebraic) surface* is a projective variety of dimension 2.

Let C be an algebraic curve and let $F(x, y) = 0$ be an affine plane model for C. Write

$$F = F_0 + F_1 + \cdots + F_d$$

where F_i is a homogeneous polynomial of degree i. Let n be the smallest number for which $F_n \neq 0$. Then $F_n = 0$ is called the *tangent cone* of F at $(0, 0)$. One can similarly define tangent cones at other points $P \in C$ by making a birational transformation which maps $P \mapsto (0, 0)$.

We close this section with a useful result on algebraic curves. A *plane curve* is an algebraic curve with a model in $\mathbb{P}^2$. An ordinary singularity is a singularity whose tangent cone is composed of distinct lines. Thus a node is an ordinary singularity whereas a cusp is not. The following theorem says that when considering algebraic curves, one can always consider a plane model with only ordinary singular points.

Theorem 1.13. *Every algebraic curve is birational to a plane projective curve with only ordinary singularities. Every algebraic curve is birational to a* unique *smooth projective curve up to isomorphism.*

Proof. See Fulton [20, Theorem VII.4.2] and [20, Theorem VII.5.3]. □

1.1.2 Schemes

In this subsection, we make a brief foray into the more general language of schemes. Although much of this thesis remains in the language of varieties, it is necessary to define some terminology in the more general language of schemes. The two important definitions in this subsection are the definitions of the spectrum of a ring R, denoted $\mathrm{Spec}(R)$, and the definition of a group scheme.

Definition 1.14 (Hindry–Silverman [23, p. 57])**.** Let X be a topological space. A *sheaf* $\mathcal{F}$ on X consists of

1. for every open subset $U \subset X$, a set $\mathcal{F}(U)$ and
2. for all open subsets $V \subset U \subset X$, a map $r_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$ satisfying

$$r_{U,U} = \mathrm{id}_{\mathcal{F}(U)} \qquad \text{and} \qquad r_{U,W} = r_{V,W} \circ r_{U,V}$$

such that for all open subsets $U \subset X$ and every open covering $U = \bigcup_i U_i$, the following two properties are satisfied:

1. Let $x, y \in \mathcal{F}(U)$ such that $r_{U,U_i}(x) = r_{U,U_i}(y)$ for all i. Then $x = y$.
2. Let $x_i \in \mathcal{F}(U)$ be a collection of elements such that for every pair of indices i, j we have $r_{U_i,U_i\cap U_j}(x_i) = r_{U_j,U_i\cap U_j}(x_j)$. Then there exists a unique $x \in \mathcal{F}(U)$ such that $r_{U,U_i}(x) = x_i$ for all i.

In the language of category theory, $\mathcal{F}$ is a *contravatiant functor* from open subsets of X with maps being inclusions to sets.

Definition 1.15. The *stalk* of a sheaf $\mathcal{F}$ at a point $x \in X$ is the direct limit of the $\mathcal{F}(U)$'s over all the open sets U containing x.

Definition 1.16 (Hindry–Silverman [23, p. 151])**.** Let R be a ring. The *spectrum* of R, denoted $\mathrm{Spec}(R)$, is a sheaf $\mathcal{O}$ together with a topological space (also denoted $\mathrm{Spec}(R)$). The topological space $\mathrm{Spec}(R)$ is the set of all proper prime ideals of R, imbued with a topology where closed sets are the sets $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subset \mathfrak{p}\}$ for any ideal I of R. The sheaf $\mathcal{O}$ is given by $\mathcal{O}(\mathrm{Spec}(R) \setminus V((f))) = R_f$ for any element $f \in R$, taken with the obvious restriction maps.

So for a ring R, the elements of $\mathrm{Spec}(R)$ are the (proper) prime ideals of R.

Definition 1.17. A *ringed space* is a pair $(X, \mathcal{O}_X)$ where X is a topological space and $\mathcal{O}_X$ is a sheaf on X. It is a *locally ringed space* if for every $x \in X$, $\mathcal{O}_x$ is a local ring.

In particular, note that for a ring R, the pair $(\mathrm{Spec}(R), \mathcal{O}_R)$ forms a locally ringed space (see Hartshorne [22, Proposition II.2.3]).

Definition 1.18. An *affine scheme* is a locally ringed space of the form $(\mathrm{Spec}(R), \mathcal{O}_R)$ for some ring R. A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ that can be covered by open subsets U such that $(U, \mathcal{O}_{X|U})$ is isomorphic to some affine scheme $(\mathrm{Spec}(R), \mathcal{O}_R)$.

For a common example of an affine scheme, consider any affine variety V over an algebraically closed field $\bar{k}$. To this variety, we can associate the scheme over $\bar{k}$ given by $\mathrm{Spec}(\bar{k}[V])$, denoted by V^{sch}. One can show that the maximal ideals of the coordinate ring of V (also called the closed points of the scheme) will correspond to the points of the variety. However, these are not the only points of V^{sch}. The other points of V^{sch} (also called the nonclosed points) correspond to the irreducible subvarieties of V.

Definition 1.19. A *morphism* of schemes is a morphism as locally ringed spaces, that is to say, it is a pair $(f, f^\sharp) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ such that $f : X \to Y$ is a continuous map and $f^\sharp$ satisfies the following two conditions:

1. $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$ is a morphism of sheaves, i.e. a map of sheaves of rings on Y, and
2. the map $f^\sharp$ induces induces a local ring homomorphism $f_x^\sharp : \mathcal{O}_{f(x)} \to \mathcal{O}_x$, that is to say, the inverse image of the maximal ideal is the maximal ideal.

Definition 1.20 (Hartshorne [22, p. 78])**.** Let S be a fixed scheme. A *scheme over* S is a scheme X, together with a morphism $X \to S$. If X and Y are schemes over S, then a *morphism over* S from X to Y is a morphism $X \to S$ which is compatible with the morphisms to S.

Definition 1.21 (Hartshorne [22, p. 275])**.** Let $f : X \to Y$ be a morphism of schemes of finite type. For $x \in X$, let $y \in Y$ such that $y = f(x)$ and let M_x and M_y denote the maximal ideals of the local rings $\mathcal{O}_x$ and $\mathcal{O}_y$ respectively. We say that f is *unramified* if for every $x \in X$, we have $M_y \cdot \mathcal{O}_x = M_x$, and $k(x)$ is a separable algebraic extension of $k(y)$.

A *flat module* of a ring R is an R-module, M, where the tensor product over R with M preserves exact sequences. A *flat map* is a homomorphism $f : R \to S$ between rings S such that S is a flat R-module, where the action of R on S is given by f.

Definition 1.22 (Hartshorne [22, p. 253])**.** Let $f : X \to Y$ be a morphism of schemes. Then f is a *flat* over Y at $x \in X$ if the stalk $\mathcal{F}_x$ is a flat $\mathcal{O}_{f(x),Y}$-module, where we consider $\mathcal{F}_x$ a $\mathcal{O}_{f(x),Y}$ module via the natural map $f^\sharp : \mathcal{O}_{f(x),Y} \to \mathcal{O}_{x,X}$. We say that f is a *flat morphism* over Y if it is flat at every point of X.

Definition 1.23 (Hartshorne [22, p. 324])**.** A *group scheme* is a scheme X, together with a morphism to another scheme S such that there is a section $e : S \to X$, a morphism $i : X \to X$ over S, and a morphism $m : X \times X \to X$ over S which satisfy

1. the composition $m \circ (\mathrm{id} \times i) : X \to X$ is equal to the projection $X \to S$ followed by e, and

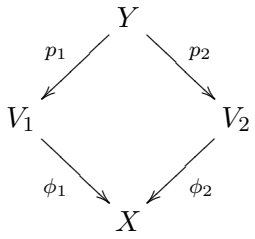
2. the two morphisms $m \circ (m \times \mathrm{id})$ and $\mu \circ (\mathrm{id} \times \mu)$ from $X \times X \times X \to X$ are the same.

The morphisms e, i, and m serve as the group identity, inverse, and multiplication operations. A common group scheme which we will encounter in this thesis will be the *Jacobian variety* of a curve (see Subsection 1.1.5 for a definition and discussion of Jacobians).

Fibre Products

Definition 1.24. Let X, V_1, and V_2 be schemes and let $\phi_1 : V_1 \to X$ and $\phi_2 : V_2 \to X$ be morphisms. A *fibre product* of V_1 and V_2 over X, denoted $V_1 \times_X V_2$, is a scheme Y with morphisms $p_1 : Y \to V_1$ and $p_2 : Y \to V_2$ satisfying the following two conditions:

1. The following diagram commutes



   and

2. If Z is another scheme with morphisms $q_1 : Z \to V_1$ and $q_2 : Z \to V_2$ then there exists a unique morphism $\psi : Z \to Y$ such that $q_1 = p_1 \circ \psi$ and $q_2 = p_2 \circ \psi$.

Note that fibre products need to be defined in the more general terminology of schemes. If V_1, V_2, and X are all varieties, then $Y := V_1 \times_X V_2$ need not be itself a variety. In this thesis, fibre product varieties will arise by observing that some variety Y is in fact the fibre product of two other varieties, and so for the purposes of this thesis, the fibre product will always be a variety.

Étale algebras

Let k be a field. A *k-algebra* (equivalently, and *algebra over k*) is a ring A (commutative, with unit) such that A is also a vector space over k using the same ring addition and such that the ring multiplication satisfies

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

for $a, b \in A$ and $\alpha \in k$.

Example 1.1. Let k be a field and let L/k be a finite extension. Then L is a k-algebra.

Example 1.2. Let $k = \mathbb{Q}$ and let $f(x) \in k[x]$ be squarefree. Define the extension

$$L = k(x)/(f(x)) := k(\alpha).$$

If f is irreducible over k then L is a field. One may be interested in defining this extension in more general cases where f may be reducible over k. In the cases where f is reducible over k, L is not a field. Nevertheless, L remains a k-algebra.

Definition 1.25. Let A be a k-algebra. Then A is an *étale algebra* (equivalently, A is *étale*) if $\mathrm{Spec}(A) \to \mathrm{Spec}(k)$ is an étale morphism (i.e. it is flat and unramified).

Equivalently, one can define an étale algebra, A, over a field k to be a product of finite separable field extensions of k and therefore

$$A \otimes_k \bar{k} \cong \bar{k} \times \cdots \times \bar{k}.$$

The two examples given above in fact are both examples of étale algebras.

1.1.3 Divisors

We follow Hartshorne [22]. He works in the more general language of schemes; we will modify it to fit in the language of varieties, in a similar manner to Hindry and Silverman [23]. There are two different ways of defining a divisor, depending on the context. The first is that of a *Weil divisor*. Weil divisors are the easiest to understand geometrically. The second notion of a divisor is called a *Cartier divisor* and can be used in a more general setting. Both notions coincide when one is working with nonsingular varieties (see Proposition 1.33 below). We present both definitions in this section.

We begin with Weil divisors. Let V be a nonsingular variety. A *prime Weil divisor* on V is a subvariety P of V of codimension 1.

Definition 1.26. The *Weil divisor group* of a nonsingular variety V, denoted $\mathrm{Div}(V)$, is the free abelian group generated by the prime Weil divisors of V.

Thus a *Weil divisor*, D, is a formal sum of codimension 1 subvarieties

$$D = \sum_{P \subset V} n_P P$$

where $n_P = 0$ for all but finitely many P. The collection of all subvarieties $P \subset V$ for which $n_P \neq 0$ is called the *support* of D.

Remark 1.27. Notice that in the case where the variety is a nonsingular curve, C, the prime Weil divisors of V are the k-rational points, $P \in V(k)$, together with the Galois orbits of the points $P \in V(\bar{k})$ which are not k-rational. Thus a Weil divisor is a formal sum of points of C. The definition of zeros and poles on prime Weil divisors has been made in such a way as to coincide with the usual notion of zeros and poles at points such that $\mathrm{ord}_P(f) = \nu_P(f)$.

Definition 1.28. A Weil divisor $D \in \mathrm{Div}(C)$ is *principal* if there exists some $f \in \bar{k}(C)^*$ such that

$$D = \sum_{P \in C} \nu_P(f)(P) := \mathrm{div}(f).$$

Two Weil divisors D_1 and D_2 are *linearly equivalent*, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is principal. An important group to study when considering a nonsingular variety is the group of divisors, modulo this linear equivalence.

Definition 1.29. The *divisor class group group of* V, denoted $\mathrm{Cl}(V)$, is the quotient of $\mathrm{Div}(V)$ by the subgroup of principal divisors.

We now consider Cartier divisors. Once again, let V be a nonsingular variety.

Definition 1.30. A *Cartier divisor* on V is an equivalence class of sets of pairs $\{ (U_i, f_i) \mid i \in I\}$ satisfying

1. the U_i are open subsets of V such that the collection $\{ U_i \mid i \in I\}$ forms an open cover of V,
2. the f_i are nonzero functions on the U_i, i.e. $f_i \in k(U_i)^* = k(V)^*$, and
3. for all $i, j \in I$, the function $f_i f_j^{-1}$ has no zeros or poles on $U_i \cap U_j$.

Two pairs $\{ (U_i, f_i) \mid i \in I\}$ and $\{ (V_j, g_j) \mid j \in J\}$ are *linearly equivalent* if $f_i(g_j)^{-1}$ has no zeros or poles on $U_i \cap V_j$ for any $i \in I$ and $j \in J$.

The Cartier divisors form an abelian group under composition of functions

$$\{(U_i, f_i)\} + \left\{(U'_j, f'_j)\right\} = \left\{(U_i \cap U'_j, f_i f'_j)\right\}.$$

We write $\mathrm{CaDiv}(V)$ for the group of Cartier divisors on V. The *support* of a Cartier divisor is the set of zeros and poles of the f_i.

Definition 1.31. A Cartier divisor D is *principal* if there exists a function $f \in k(V)^*$ such that

$$D = \{(V, f)\} := \mathrm{div}(f).$$

Two Cartier divisors D_1 and D_2 are *linearly equivalent*, denoted $D_1 \sim D_2$ if $D_1 - D_2$ is principal.

Definition 1.32. The *Picard group of* V, denoted $\mathrm{Pic}(C)$ is the quotient of $\mathrm{CaDiv}(C)$ by the subgroup of principal divisors.

Proposition 1.33. *Let* V *be a nonsingular variety. Then the groups* $\mathrm{Div}(V)$ *and* $\mathrm{CaDiv}(V)$ *are isomorphic. Similarly, the groups* $\mathrm{Cl}(V)$ *and* $\mathrm{Pic}(V)$ *are isomorphic.*

Proof. See [22, Proposition II.6.11] for a (more general) proof; see also [23, p. 38] for an explicit description of the isomorphism. □

As a result of Proposition 1.33, we will simply use the term divisor when we are working with a nonsingular variety V. In this case, we will refer to the divisor group as $\mathrm{Div}(V)$ and the Picard group (or divisor class group) as $\mathrm{Pic}(V)$.

Definition 1.34. Let $\phi : V \to W$ be a morphism of nonsingular varieties. We define the *pullback*

$$\phi^* : \mathrm{Div}(W) \to \mathrm{Div}(V)$$

(in terms of Cartier divisors), by

$$\phi^*(\{(U_i, f_i)\}) := \left\{(\phi^{-1}(U_i), f_i \circ \phi)\right\}.$$

By following through the isomorphism between Cartier divisors and Weil divisors, one can define the pullback of ϕ in terms of Weil divisors via

$$\phi^*\left(\sum_i n_i Q_i\right) = \sum_i n_i \sum_{P \in \phi^{-1}(Q_i)} \mathrm{ord}_P(t_{Q_i}) P$$

where t_{Q_i} denotes a uniformizer at the subvariety Q_i of V (i.e. a generator for the maximal ideal of the local ring at Q_i). One can show that the pullback takes principal divisors to principal divisors, and thus the pullback induces a pullback map on the Picard groups

$$\phi^* : \mathrm{Pic}(W) \to \mathrm{Pic}(V).$$

In a similar vein to Definition 1.34, one can define a push forward map on the divisors.

Definition 1.35. Let $\phi : V \to W$ be a morphism of nonsingular curves. We define the *push forward map*

$$\phi_* : \mathrm{Div}(V) \to \mathrm{Div}(W)$$

(in terms of Weil divisors), by

$$\phi_*((P)) \to (\phi(P)).$$

As with the pullback, the push forward map induces a push forward map on the Picard groups

$$\phi_* : \mathrm{Pic}(V) \to \mathrm{Pic}(W).$$

The Riemann-Roch theorem and the genus of a curve

We now consider divisors on algebraic curves. As we have already pointed out, in this case, divisors can be thought of as formal sums of points. Let

$$D = \sum_{P \in C} n_P \cdot P$$

be a divisor on a curve C. We define the *degree of* D to be

$$\deg(D) = \sum_{P \in C} n_P.$$

The set of divisors of degree 0, denoted $\mathrm{Div}^0(C)$, forms a subgroup of $\mathrm{Div}(C)$. The *degree* 0 *part of the Picard group of* C, denoted $\mathrm{Pic}^0(C)$, is the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. A divisor $D = \sum n_P(P) \in \mathrm{Div}(C)$ is *effective* if $n_P \geq 0$ for all $P \in C$. The set of effective divisors linearly equivalent to a divisor $D \in \mathrm{Div}(C)$ is a linear system, called the *complete linear system of* D and is denoted $|D|$.

Definition 1.36. Let C be a curve. The *space of differential forms* on C, denoted Ω_C, is the $\bar{k}(C)$-vector space generated by symbols of the form dx for $x \in \bar{k}(C)$, subject to

$$\begin{aligned} &(i)\ d(x+y) = dx + dy, && \text{for all } x, y \in \bar{k}(C); \\ &(ii)\ d(xy) = x\,dy + y\,dx && \text{for all } x, y \in \bar{k}(C); \\ &(iii)\ da = 0, && \text{for all } a \in \bar{k}. \end{aligned}$$

Proposition 1.37. *Let $P \in C$, and let $t \in \bar{k}(C)$ be a uniformizer at P.*

1. *For every $\omega \in \Omega_C$, there exists a unique function $g \in \bar{k}(C)$, depending on ω and t, such that*

   $$\omega = g\,dt.$$

   We denote g by ω/dt.

2. *The quantity $\mathrm{ord}_P(\omega/dt)$ depends only on ω and P and is independent of choice of uniformizer t. This value is called the* order of ω at P *and is denoted $\mathrm{ord}_P(\omega)$.*

3. For all but finitely many $P \in C$,

$$\mathrm{ord}_P(\omega) = 0$$

Proof. See Silverman [45, Proposition II.4.3] □

Definition 1.38. Let $\omega \in \Omega_C$. The *divisor associated to* ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P).$$

Definition 1.39. The *canonical divisor class on* C is the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any non-zero differential $\omega \in \Omega_C$. Any divisor in this class is called a *canonical divisor*.

Definition 1.40. For a fixed divisor, D, we define the *Riemann-Roch space of* D by

$$\mathcal{L}(D) = \left\{ f \in \bar{k}(C)^* \mid \mathrm{div}(f) + D \geq 0 \right\} \cup \{0\}.$$

For the dimension of $\mathcal{L}(D)$, we write $\ell(D) = \dim_{\bar{k}} \mathcal{L}(D)$.

Theorem 1.41 (Riemann-Roch)**.** *Let C be a smooth curve and let K_C be a canonical divisor on C. Then there is an integer $g \geq 0$ such that for every divisor $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

Remark 1.42. By taking $D = 0$, we see that $g = \ell(K_C)$.

Definition 1.43. The integer g defined in the Riemann-Roch theorem is called the *genus* of C.

The genus is a birational invariant of algebraic curves. One is often given a model of a curve and may wish to determine its genus. The following theorem proves useful in this regard.

Theorem 1.44. *Let C be a algebraic curve which has a smooth plane projective model of degree d. Then its genus is given by the formula*

$$g = \frac{(d-1)(d-2)}{2}.$$

Proof. See [23, Theorem A.4.2.6]. □

There is also a more general version of Theorem 1.44 which allows for nonsingular models of curves (see [20, Proposition VIII.3.5]). In this thesis, we will be considering algebraic curves of genus 1 and 2. Notice that by Theorem 1.44, if a genus 1 curve is birational to a smooth projective plane model, then it will have degree 3. On the other hand, a genus 2 curve does not have a smooth projective plane model as there is no degree d which satisfies $\frac{(d-1)(d-2)}{2} = 2$.

1.1.4 Principally polarized abelian varieties

We need some results about principally polarized abelian varieties. For further reading on abelian varieties, see [32, 35]; for further reading on Jacobian varieties, see [33].

Definition 1.45. A *group variety* is an algebraic variety V over k, together with morphisms

$$m : V \times V \to V$$
$$i : V \to V$$

defined over k and an element $O \in V(k)$ such that the structure on $V(\bar{k})$ defined by m and i forms a group with identity O where m is group multiplication and i is taking inverses. An *abelian variety* is a complete group variety.

Notice that the definition of a group variety coincides with the earlier definition of a group scheme (Definition 1.23) by setting $S = \mathrm{Spec}(k)$ and letting the scheme X be a variety V. One can show that the group structure on abelian varieties is commutative.

Proposition 1.46 ([32, Corollary 2.4])**.** *The group law on an abelian variety A is commutative.*

Definition 1.47. Let A and B be abelian varieties. An *isogeny* $\phi : A \to B$ is a surjective morphism on abelian varieties which is also a group homomorphism with finite kernel. If an isogeny exists between A and B, then we say that A and B are *isogenous*.

The *degree* of an isogeny ϕ, denoted $\deg(\phi)$, is the degree of the kernel of ϕ as a finite group scheme. By working with the language of schemes, one can allow for ϕ to be either separable or non-separable. In the context of this thesis, however, all isogenies will be separable. This will allow us to remain in the language of varieties. In this case, the degree of an isogeny, ϕ, is simply the number of points in the kernel of ϕ.

Through our discussion of divisors on nonsingular varieties, we have already shown how we can associate to each variety V, a group $\mathrm{Pic}(V)$. Since an abelian variety A already has an associated group structure defined on it, one may ask whether it is possible to construct another abelian variety B such that $\mathrm{Pic}(B) \cong A$. It turns out that if we consider an appropriate subgroup of the Picard group, then it is always possible. Such a variety will be called the *dual variety of* A. We use Hindry and Silverman's definition [23, Definition A.7.3.4] (other definitions are in the more general language of sheafs – see [32, Section 9] for example).

Let A be an abelian variety with $a \in A$, and let t_a denote the translation-by-a morphism on A. Define $\mathrm{Pic}^0(A)$ to be the translation-invariant subgroup of the Picard group

$$\mathrm{Pic}^0(A) = \{\, D \in \mathrm{Pic}(A) \mid t^*(D) = D \text{ for all } a \in A \}\,.$$

It turns out $\mathrm{Pic}^0(A)$ is the appropriate group to form into the dual abelian variety. For two abelian varieties A and B and for $a \in A$ and $b \in B$, let i_a and i_b denote the inclusion maps

$$\begin{aligned} &i_a : B \longrightarrow A \times B && \text{and} && i_b : A \longrightarrow A \times B \\ &i_a(b) = (a, b) && && i_b(a) = (a, b) \end{aligned}$$

We now define the dual abelian variety.

Definition 1.48. An abelian variety $A^\vee$ is the *dual abelian variety of* A if there exists a divisor class $\mathcal{P}$ on $A \times A^\vee$ such that the maps

$$\begin{aligned} &A^\vee \longrightarrow \mathrm{Pic}^0(A), && \text{and} && A \longrightarrow \mathrm{Pic}^0(A^\vee) \\ &a^\vee \longmapsto i_{a^\vee}^*(\mathcal{P}) && && a \longmapsto i_a^*(\mathcal{P}) \end{aligned}$$

are both bijections. The divisor class $\mathcal{P}$ is called the *Poincaré divisor class.*

Theorem 1.49. *The dual abelian variety $A^\vee$ exists and is unique up to isomorphism. Similarly, the Poincaré class is unique up to isomorphism.*

Proof. See Hindry and Silverman [23, Theorem A.7.3.4]. □

As is expected, one can easily see by the symmetry of the definition that $A^{\vee\vee} = A$.

Definition 1.50. The *Néron–Severi group of* A, denoted $\mathrm{NS}(A)$ is the quotient group

$$\mathrm{NS}(A) = \mathrm{Pic}(A)/\,\mathrm{Pic}^0(A).$$

Definition 1.51. A linear system on a projective variety V is *very ample* if the associated rational map $\phi_L : X \to \mathbb{P}^n$ is a morphism that maps X isomorphically onto its image $\phi_L(X)$. A divisor D is *very ample* if the complete linear system $|D|$ of D is very ample. A divisor D is *ample* if some positive multiple of D is very ample.

Proposition 1.52 (Milne [32, Corollary 12.8])**.** *The Néron-Severi group of an abelian variety is a torsion-free $\mathbb{Z}$-module of finite rank.*

Let A be an abelian variety with $a \in A$ and let t_a denote the translation-by-a map. Consider the map

$$\begin{aligned} \lambda_D : A &\longrightarrow \mathrm{Pic}(A) \\ a &\longmapsto t_a^*(D) - D. \end{aligned}$$

Theorem 1.53 (Theorem of the square)**.** *For any divisor class $D \in \mathrm{Pic}(A)$, the map λ_D is a group homomorphism.*

Proof. See Hindry and Silverman [23, Theorem A.7.2.9]. □

We can use the map $\lambda_D : A \to \mathrm{Pic}(A)$ to induce a map $\lambda_D : A \to A^\vee$ by observing that the image of λ_D lies in $\mathrm{Pic}^0(A)$. By Theorem 1.53, we know that this will be an isogeny whenever λ_D has finite kernel. One can show that this will occur if and only if D is ample (cf. [23, Theorem A.7.2.10]). As D may not exist over k, one defines a *polarization* to be an isogeny $\lambda : A \to A^\vee$ such that over $\bar{k}$, $\lambda = \lambda_D$ for some ample $D \in \mathrm{Pic}^0(A/\bar{k})$. If a polarization is an isomorphism, then we say it is a *principal polarization*.

Definition 1.54. A *principally polarized abelian variety* is a pair (A, λ), where A is an abelian variety and λ is a principal polarization on A.

Let μ_n denote the group of n-th roots of unity. A principal polarization induces, for each n prime to the characteristic, an alternating non-degenerate, bilinear pairing

$$e_{A[n]} \colon A[n] \times A[n] \to \mu_n,$$

called a *Weil pairing*.

We need two main results on principally polarized abelian varieties from Milne [32]. The first result is [32, Proposition 16.2] which describes the interaction between homomorphisms between abelian varieties and Weil pairings. Paraphrased, it yields in our situation

Lemma 1.55 (Milne [32, Proposition 16.2]). *Let (A, λ_A) and (B, λ_B) be principally polarized abelian varieties and let $f : A \to B$ be a homomorphism. Then*

$$e_{A[m]}\big(a, f^\vee(b)\big) = e_{B^\vee[m]}(f(a), b),$$

for all $a \in A_m$ and $b \in B_m$.

The second result is [32, Proposition 16.8], which describes isogenies that respect polarizations. Paraphrased, it yields in our particular situation

Lemma 1.56. *Let (A, λ_A) be a principally polarized abelian variety and let $\Phi\colon A \to B$ be an isogeny with $\ker(\Phi) \subset A[n]$. A necessary and sufficient condition for the existence of a polarization $\lambda_B\colon B \to B^\vee$ such that the diagram*

$$\begin{array}{ccc} A & \xrightarrow{n\lambda_A} & A^\vee \\ {\scriptstyle\Phi}\downarrow & & \uparrow{\scriptstyle\Phi^\vee} \\ B & \xrightarrow{\lambda_B} & B^\vee \end{array}$$

commutes, is that $\ker(\Phi)$ is isotropic *with respect to $e_{A[n]}$, which means that $e_{A[n]}$ restricted to $\ker(\Phi) \times \ker(\Phi)$ is trivial.*

1.1.5 Jacobian varieties

Principally polarized abelian varieties play an important role in the study of algebraic curves. Let C be an algebraic curve. By Theorem 1.13, every algebraic curve is birational to a smooth projective curve, so we will consider the smooth projective model for C over k. One can construct an abelian variety J over k such that over the closure, $J(\bar{k}) \cong \mathrm{Pic}^0(C)(\bar{k})$. Over k we define

$$J(k) \cong \mathrm{Pic}^0(C)(\bar{k})^{\mathrm{Gal}(\bar{k}/k)},$$

or in other words, it is all classes in $\mathrm{Pic}^0(C)(\bar{k})$ which are invariant with respect to Galois transformations. Such an abelian variety is called the *Jacobian variety of C*, or just the *Jacobian of C* and is written $\mathrm{Jac}(C)$.

If C has a degree 1 divisor class defined over k, then Hindry and Silverman give a theorem which nicely summarizes the construction and some properties of Jacobians. Note that if C does not have a degree 1 divisor class defined over k, then the Jacobian variety still exists and is defined over k but we do not obtain an injection $j : C \hookrightarrow \mathrm{Jac}(C)$ over k.

Theorem 1.57 ([23, Theorem A.8.1.1] and [23, Corollary A.8.2.3.a]). *Let C be a smooth projective curve over k of genus $g \geq 1$, together with a degree 1 divisor class defined over k. Then there exists an abelian variety $J = \mathrm{Jac}(C)$, called the* Jacobian *of C and an injection $j : C \hookrightarrow \mathrm{Jac}(C)$ called the* Jacobian embedding *of C, with the following properties:*

1. *One can extend j linearly to divisors on C to obtain a group isomorphism between $\mathrm{Pic}^0(C/\bar{k})$ and $\mathrm{Jac}(C)/\bar{k}$.*

2. *Define a subvariety $W_r \subset J$ by $W_0 = \{0\}$ and for $r > 0$,*

$$W_r = \underbrace{j(C) + \cdots + j(C)}_{r \text{ copies}}.$$

   Then $\dim(W_r) = \min(r, g)$ and $W_g = \mathrm{Jac}(C)$. In particular, $\mathrm{Jac}(C)$ has dimension g.

3. *Let $\Theta = W_{g-1}$. Then Θ is an irreducible ample divisor on $\mathrm{Jac}(C)$ and gives a principal polarization*

$$\lambda_\Theta : J \xrightarrow{\sim} \mathrm{Pic}^0(J) \cong J^\vee.$$

Remark 1.58. Suppose C is an algebraic curve over k of genus $g > 0$, and let D be a degree 1 divisor class of C. Then we define the injection by

$$\begin{aligned} j : C &\hookrightarrow \mathrm{Pic}^0(C) \cong \mathrm{Jac}(C) \\ j(P) &\mapsto [P] - D. \end{aligned}$$

In the proof of Theorem 1.57 one defines

$$J = \{\text{linear systems of degree } n \text{ on } C\},$$

and then defines an appropriate group law on J, eventually showing that J is an algebraic variety and making the identification $J = \mathrm{Jac}(C)$ (see [23, pp. 136–137]). In the case where there is a point $P_0 \in C(k)$, then we can set $D = [P_0]$ to get a map j which is defined over k. Let n be an integer with $n \geq 2g - 1$ and $D_0 = n[P_0]$. To construct the map j in this case, we then define

$$\begin{aligned} j : C &\longrightarrow J \\ P &\longmapsto |[P] + (n-1)[P_0]| \end{aligned} \tag{1.1.1}$$

and extend j linearly to get a map

$$\begin{aligned} j : \mathrm{Pic}^0(C) &\longrightarrow J \\ D &\longmapsto |D + D_0| \,. \end{aligned}$$

In general, this construction will suffice for our purposes in this thesis. See Milne [33] for a more general discussion of Jacobians.

So the Jacobian of a curve C is the principally polarized abelian variety whose points correspond to the elements of $\mathrm{Pic}^0(C)$ and whose dimension is equal to the genus of C. By Theorem 1.57, we know that a smooth projective curve uniquely determines the Jacobian variety $\mathrm{Jac}(C)$ and the corresponding theta divisor class. The converse is also true and is called Torelli's theorem (see Milne [33, Theorem 12.1] for a statement and proof).

Notice that the Jacobian, $\mathrm{Jac}(C/k)$, of a curve C over k can be viewed as a group scheme over k (cf. Definition 1.23). Similarly, the finite group of n-torsion points (that is to say, the elements of order n in $\mathrm{Jac}(C/k)$) also forms a group scheme over k.

We will be working with Jacobians of curves of genus 1 and 2.

Genus 1 curves and their Jacobians

Let E be a curve of genus 1 over k. By Theorem 1.57, we know that $\mathrm{Jac}(E)$ is a principally polarized abelian variety of dimension 1. If E has a k-rational point $O \in E(k)$, then we can follow (1.1.1) to embed E into its Jacobian by $j : E \hookrightarrow \mathrm{Jac}(E)$ by sending $P \mapsto |[P] - [O]|$. But by the second part of that Theorem 1.57, we know $\mathrm{Jac}(E) = j(E)$ and therefore $E \cong \mathrm{Jac}(E)$. These curves are called elliptic curves.

Definition 1.59. An *elliptic curve* is a pair (E, O) where E is a curve of genus 1 and $O \in E$.

Our discussion in the first paragraph yields

Proposition 1.60. *Let (E, O) be an elliptic curve. Then* $\mathrm{Jac}(E) \cong E$.

We often write E for an elliptic curve with the point O being understood. The elliptic curve E is *defined over* k, written E/k if E is defined over k as a curve and $O \in E(k)$.

Let k be a field. Then every elliptic curve (E, O) has a model in $\mathbb{P}^2(\bar{k})$ given by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad \text{and} \quad O = [0 : 1 : 0]$$

with $a_1, \ldots, a_6 \in \bar{k}$ (cf. Silverman [45, Proposition 3.1]). This model is called a *Weierstrass model* for E. We use $j : E \to \mathrm{Jac}(E)$ with $P \mapsto |[P] - [O]|$ as the canonical embedding of E into its Jacobian. As before, if $a_1, \ldots, a_6 \in k$ then E is defined over k.

For ease of notation, we will generally write all equations by using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

$$y^2 + a_2xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

keeping in mind the extra point $O = [0 : 1 : 0]$, called the *point at infinity*.

In this thesis, we will be considering fields k for which $\mathrm{char}(k) \neq 2, 3$. With this added restriction, we can express the Weierstrass form of E as

$$E : y^2 = x^3 + ax + b$$

for $a, b \in \bar{k}$.

Genus 2 curves and their Jacobians

Let C be a curve of genus 2 over a field k and let K_C be a canonical divisor on C. Then $\deg(K_C) = 2$ (cf. Fulton [20, Section 8.5]) and the linear system $|K_C|$ gives a map $C \to \mathbb{P}^1$ of degree 2 (c.f. Hindry and Silverman [23, Theorem A.4.5.1] and the discussion after the proof). We say that C is a *double cover* of $\mathbb{P}^1$.

Definition 1.61. Algebraic curves of genus $g > 1$ which are double covers of $\mathbb{P}^1$ are called *hyperelliptic curves*.

Thus all genus 2 curves are hyperelliptic curves. Let $h_C : C \to \mathbb{P}^1$ be the double cover given by $|K_C|$. Then it induces a quadratic extension of function fields $k(C)/k(\mathbb{P}^1)$. If we restrict our discussion to a base field k where $\mathrm{char}(k) \neq 2$ then C has an affine plane model

$$C : y^2 = f(x)$$

where f is a squarefree polynomial of degree 5 or 6 (cf. Cassels and Flynn [10, Section 1.3] and Chevalley [11, p. 77]). The double cover h_C acts on the plane model by $(x, y) \mapsto x$ and is ramified at 6 points (over $\bar{k}$), called the *Weierstrass points* of C. When f has degree 6, these points are exactly the points $(w_i, 0)$ where $w_1, \ldots, w_6$ are the six (distinct) roots of $f(x)$ over $\bar{k}$. In the case where f has degree 5, the Weierstrass points are the the five points

$(w_i, 0)$ where $w_1, \ldots, w_5$ are the five (distinct) roots of $f(x)$ over $\bar{k}$, together with the point at infinity $w_6 = \infty$. The double cover also gives rise to a *hyperelliptic involution* ι_C on C, which acts on the plane model by $(x, y) \mapsto (x, -y)$.

Now consider the Jacobian $J = \mathrm{Jac}(C)$ of C. By Theorem 1.57, we know that it is a principally polarized abelian variety of dimension 2, that is to say, it is a *principally polarized abelian surface.*

1.2 Decomposable Jacobians

In this section, we introduce the notion of split Jacobians. We introduce some terminology used throughout the remainder of the thesis.

Definition 1.62. Let A be an abelian surface over a field k. We say that A is *decomposable* if there exist elliptic curves E_1, E_2 over k such that A is isogenous to $E_1 \times E_2$ over k.

We begin with a lemma that we believe to be common knowledge but were unable to find a reference to in earlier literature.

Lemma 1.63. *Let C be a curve of genus 2 over a field k. If $\mathrm{Jac}(C)$ is decomposable over k then there exists an elliptic curve E such that C admits a finite cover $\phi : C \to E$.*

Proof. Let $J = \mathrm{Jac}(C)$. As noted in Theorem 1.57, if we have a k-rational degree 1 divisor class, then we can construct an injection $j : C \hookrightarrow J$, which allows us to consider C as a subvariety of J. In general, consider the k-rational canonical divisor K_C on C. Points on the Jacobian correspond to degree 0 divisor classes on C, so consider the map $\gamma : C(k) \to \mathrm{Pic}^0(C/\bar{k})$ by mapping $P \mapsto ([2P] - \kappa)$. Then the image of γ is birational to C. For a Weierstrass point P note that we have $[2P] = \kappa$, so we see that the identity $0_J \in J$ lies in the image of γ.

Now suppose J is decomposable. Then there exist elliptic curves E_1 and E_2 over k and an isogeny $\Phi : J \to E_1 \times E_2$ over k. Let $\pi_1 : E_1 \times E_2 \to E_1$ be the projection onto E_1 and consider the composition $\Phi_1 = \pi_1 \circ \Phi : J \to E_1$. We claim that $\gamma \circ \Phi_1$ is not constant. If it were, then $\gamma(C)$ would have to lie in the connected component of $\ker(\Phi_1)$ that contains 0_J. But that is a 1-dimensional subgroup scheme of J, so cannot contain a singular model of a curve of genus 2. It follows that $\phi = \gamma \circ \Phi_1 \colon C \to E_1$ is a non-constant morphism between (complete, non-singular) irreducible curves and hence a finite cover. □

The cover constructed in the proof of Lemma 1.63 is by no means unique and may not be of minimal degree. This leads us to consider *optimal covers*. Other literature uses the term *minimal covers* [26] and *maximal covers* [19].

Definition 1.64. A finite cover $\phi_1 : C \to E_1$ is said to be *optimal* if for any factorization

$$C \xrightarrow{\phi_1'} D \xrightarrow{\psi} E_1.$$
$$\phi_1$$

we must have $\deg(\phi_1') = \deg(\phi_1)$ or $\deg(\phi_1') = 1$.

Lemma 1.65. *Let $\psi : C \to E$ be a finite cover where C is a curve of genus 2 and E is an elliptic curve. Then ψ factors through an optimal cover ϕ.*

Proof. Suppose $\psi : C \to E$ is a finite cover, and suppose

$$C \xrightarrow{\phi_1} D \xrightarrow{\phi_2} E_1.$$
$$\psi$$

is a factorization of ψ through ϕ_1 and ϕ_2. Then $\deg(\psi) = \deg(\phi_1)\deg(\phi_2) < \infty$. So either ψ is optimal, or it factors into a product of two covers of smaller degree. In the latter case, $\deg(\phi_1) > 1$, so by Riemann-Hurwitz, D must have a lower genus than C and hence have genus 1 or 0. But E has genus 1 and D covers E, so D must have genus 1. An inductive argument on the degree of ψ quickly completes the proof. □

Let $n = \deg(\phi_1)$. We need our maps to be separable, hence we assume $\mathrm{char}(k) \nmid n$. In the case $n = 4$ which we focus on in subsequent chapters, this contributes to us requiring $\mathrm{char}(k) \neq 2$. Consider the induced maps $\phi_1^* : E_1 \to J$ and $\phi_{1,*} : J \to E_1$.

Lemma 1.66. *Let C be a curve of genus 2 over k, let E_1 be an elliptic curve over k, and let $\phi_1 : C \to E_1$ be a degree n cover where* $\mathrm{char}(k) \nmid n$. *Then*

1. *The cover ϕ_1 is optimal if and only if* $\ker(\phi_{1,*})$ *is connected, and*

2. *If ϕ_1 is optimal, then the map ϕ_1^* is injective and* $\ker(\phi_{1,*})$ *is an elliptic curve.*

Remark 1.67. Serre [40, pp. 124–129] proves a similar result to Lemma 1.66 (see in particular [40, Propositions VI.12 and VI.13]), but he does so in the language of algebraic groups. Frey and Kani [19] and Kuhn [28, Section 2] adapt it to its current context of optimal covers of elliptic curves. We provide a sketch of the argument.

Proof. Define $E_2^* = \ker(\phi_{1,*})$ and let $D \subset E_2^*$ be the connected component of 0. We know that E_2^* has dimension 1, and so D must have dimension 1 as well. We can factor $\phi_{1,*}$ through J/D

$$J \xrightarrow{f} J/D \xrightarrow{g} J/E_2^* \cong E_1.$$
$$\phi_{1,*}$$

We know D has dimension 1, so J/D is an elliptic curve. By Lemma 1.63, we obtain a cover $\phi_1' : C \to J/D$. We can argue geometrically that our cover ϕ_1 must factor. Working over the algebraic closure, we can choose some point $P_0 \in C$ and then embed C into its Jacobian $j : C \to J$ by mapping P to $[P] - [P_0]$. Using the image of P_0 in E_1 under ϕ_1, we can also define an isomorphism $j_1 : E_1 \to \mathrm{Jac}(E_1)$ by

$$Q \mapsto [Q] - [\phi_1(P_0)].$$

Notice

$$(\phi_{1,*} \circ j)(P) = \phi_{1,*}([P] - [P_0]) = [\phi_1(P)] - [\phi_1(P_0)] = j_1(\phi_1(P)) = (j_1 \circ \phi_1)(P)$$

which shows that the following diagram

$$\begin{array}{ccc} J & \xrightarrow{\phi_{1,*}} & J/E_2^* \\ {\scriptstyle j}\uparrow & & \downarrow{\scriptstyle j_1^{-1}} \\ C & \xrightarrow[\phi_1]{} & E_1 \end{array}$$

commutes. But now consider that the composition

$$C \xrightarrow{j} J \longrightarrow J/D \longrightarrow E_1$$
$$\phi_{1,*}$$

fits into the upper arc of the commutative diagram by factoring $\phi_{1,*}$

$$\begin{array}{ccccc} & & \overset{\phi_{1,*}}{\frown} & & \\ J & \xrightarrow[f]{} & J/D & \xrightarrow[g]{} & J/E_2^* \\ {\scriptstyle j}\uparrow & & & & \downarrow{\scriptstyle j_1^{-1}} \\ C & & \xrightarrow[\phi_1]{} & & E_1. \end{array}$$

Define intermediate maps $\phi_1' = f \circ j'$ and $\psi = j_1^{-1} \circ g$ respectively to obtain

$$C \xrightarrow{\phi_1'} J/D \xrightarrow{\psi} E_1.$$
$$\phi_1$$

If ϕ_1 is an optimal cover and J/D is an elliptic curve, then ψ has degree 1, and so it is an isomorphism. Conversely, if $\ker(\phi_{1,*})$ is connected, then our only choice for D is $D = E_2^*$ and so $J/D \cong J/E_2^* \cong E_1$. Therefore ψ is an isomorphism and has degree 1 and so ϕ_1 is optimal.

To prove the second part of the Lemma, suppose $\phi_1 : C \to E_1$ is an optimal cover. By the first half of the proof, we know that the kernel of $\phi_{1,*}$ is connected and is itself an elliptic curve. Finally, to show ϕ_1^* is injective, see Serre [40, Proposition VI.12]. He proves that it is injective by using the fact that an optimal cover does not lift to any non-trivial isogeny. □

Let $\phi_1 : C \to E_1$ be an optimal cover. By Lemma 1.66, or by Serre [40, Proposition VI.12], we know that ϕ_1^* is injective. Write $E_1^* = \phi_1^*(E_1)$. We follow a similar argument to the one given in the proof of Lemma 1.66. Working over the algebraic closure, let P_0 be a point of C and embed C into its Jacobian J by $j : C \to J$ via $P \mapsto [P] - [P_0]$. By Lemma 1.66, the following sequence

$$0 \longrightarrow E_1 \xrightarrow{\phi_1^*} J \xrightarrow{f'} E_2^* \longrightarrow 0 \tag{1.2.1}$$

is exact for some f'. We can use f' to define a cover

$$\phi_2 := j \circ f' : C \longrightarrow J/E_1^* =: E_2.$$

By (1.2.1), we have $E_1 \cong E_1^* = \ker(\phi_2^*)$, so we know that the kernel of ϕ_2^* is connected. By Lemma 1.66, we conclude ϕ_2 is optimal. In [28, Section 2], Kuhn proves that this cover is in fact defined over the ground field. We call $\phi_2 : C \to E_2$ the *complementary cover* to the optimal cover $\phi_1 : C \to E_1$.

The maps ϕ_1, ϕ_2 give rise to a map

$$\phi_1^* + \phi_2^* \colon E_1 \times E_2 \to J,$$

with kernel Δ defined by the exact sequence

$$0 \to \Delta \to E_1 \times E_2 \to J \to 0.$$

To determine Δ, consider the following diagram

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\phi_1^*+\phi_2^*} & J \\ & \searrow^{[n]} & \downarrow{\scriptstyle \phi_{1,*}\times\phi_{2,*}} \\ & & E_1 \times E_2. \end{array}$$

The composition $(\phi_{1,*} \times \phi_{2,*}) \circ (\phi_1^* + \phi_2^*)$ is multiplication-by-n on $E_1 \times E_2$ (see Lemma 1.70 and the first few lines of its proof for an explicit justification), and so the kernel of the composition map is the n-torsion of $E_1 \times E_2$. Therefore, in particular, we see that $\Delta \subset (E_1 \times E_2)[n]$ and so it is finite and $\phi_1^* + \phi_2^*$ is an isogeny.

By Lemma 1.66, we know that ϕ_1^* injects into J and by symmetry, ϕ_2^* also injects into J. Notice that

$$E_1[n] \cong E_1[n] \times 0_{E_2} \subset (E_1 \times E_2)[n].$$

Furthermore, we know that ϕ_1^* is injective, so we have an injection

$$\phi_1^* : E_1[n] \to \Delta. \tag{1.2.2}$$

Consider the isogenies $\phi_{1,*} \times \phi_{2,*}$ and $\phi_1^* + \phi_2^*$. We know that the kernel of the composition is $(E_1 \times E_2)[n]$, and so it has order n^4. By the injection in (1.2.2), we know that Δ has order greater than or equal to n^2. Conversely,

$$E_1 \cong (\phi_{1,*} \times \phi_{2,*})\,(E_1 \times 0_{E_2})\,,$$

and so an image of $E_1[n]$ must lie in the kernel of $\phi_{1,*} \times \phi_{2,*}$. Therefore $\ker(\phi_{1,*} \times \phi_{2,*})$ also has order greater than or equal to n^2. But we know

$$\deg(\phi_{1,*} \times \phi_{2,*}) \deg(\phi_1^* + \phi_2^*) = n^4,$$

and so we conclude that $\phi_1^* + \phi_2^*$ has degree n^2 and that the injection in (1.2.2) is an isomorphism. By a similar argument, we find an isomorphism

$$\phi_2^* : E_2[n] \to \Delta.$$

Therefore Δ identifies an isomorphism

$$\alpha \colon E_1[n] \to E_2[n]$$

by $\alpha = (\phi_2^*)^{-1} \circ \phi_1^*$; in such a case, we say that Δ is the *graph* of the isomorphism α.

Both J and $E_1 \times E_2$ are principally polarized abelian varieties (see Section 1.1.4). We investigate how the isogenies $\phi_1^* + \phi_2^*$ and $\phi_{1,*} \times \phi_{2,*}$ interact with these polarizations.

Let (A, λ_A) be a principally polarized abelian variety and let $\Phi : A \to B$ be an isogeny with $\ker(\Phi) \subset A[n]$. Then by Lemma 1.56, a polarization $\lambda_B : B \to B^\vee$ will exist if and only if $\ker(\Phi)$ is isotropic with respect to the Weil pairing $e_{A[n]}$. Suppose A is g-dimensional.

Then $\deg(n\lambda_A) = n^{2g}$. Since $\deg(\Phi) = \deg(\Phi^\vee)$, we can use the commutative diagram in Lemma 1.56 to calculate the degree of λ_B:

$$\begin{aligned} n^{2g} &= \deg(\Phi)\deg(\lambda_B)\deg(\Phi^\vee) \\ &= \deg(\Phi)^2\deg(\lambda_B). \end{aligned}$$

In order for λ_B to be principal, we need $\deg(\lambda_B) = 1$;. Thus λ_B will be principal if and only if $\deg(\Phi) = n^g$. The nondegeneracy of $e_{A[n]}$ implies that in that case $\ker(\Phi) \subset A[n]$ is a *maximal* isotropic subgroup.

Definition 1.68. Let (A, λ_A) and (B, λ_B) be principally polarized abelian varieties of dimension g. We say that an isogeny $\Phi\colon A \to B$ is a *polarized* $(n_1, \ldots, n_r)$*-isogeny* if $\ker(\Phi)(\bar{k}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ and $\Phi^\vee \circ \lambda_B \circ \Phi = n\lambda_A$, where $n^g = \prod_{i=1}^r n_i$.

Lemma 1.69. *Let $\Phi : A \to B$ be a polarized (n,n)-isogeny between principally polarized abelian surfaces (A, λ_A) and (B, λ_B). Then the dual isogeny $\Phi^\vee : B^\vee \to A^\vee$ is a polarized (n,n)-isogeny between $(B^\vee, \lambda_B^{-1})$ and $(A^\vee, \lambda_A^{-1})$.*

Proof. Let $\Phi : A \to B$ be a polarized (n,n)-isogeny between principally polarized abelian surfaces. Then $\ker(\Phi) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over $\bar{k}$ and $\Phi^\vee \circ \lambda_B \circ \Phi = n\lambda_A$.

Since A and B are both principally polarized, λ_A and λ_B are both isomorphisms. Therefore λ_A^{-1} and λ_B^{-1} both exist and are principal polarizations on $A^\vee$ and $B^\vee$ respectively. Since $B^\vee$ is principally polarized and since a polarization $A^\vee \to A$ exists, then by Lemma 1.56, the following diagram

$$\begin{array}{ccc} A & \xleftarrow{\lambda'} & A^\vee \\ {\scriptstyle\Phi}\downarrow & & \uparrow{\scriptstyle\Phi^\vee} \\ B & \xleftarrow[n\lambda_B^{-1}]{} & B^\vee \end{array}$$

commutes. From this diagram, we obtain

$$\Phi \circ \lambda' \circ \Phi^\vee = n\lambda_B^{-1}. \tag{1.2.3}$$

To show that $\lambda' = \lambda_A^{-1}$, by Proposition 1.52, note that the Néron-Severi group of an abelian variety is torsion-free. Therefore $n\lambda' = n\lambda_A^{-1}$ directly implies $\lambda' = \lambda_A^{-1}$.

By (1.2.3), it is immediate that $\ker(\Phi^\vee) \subset B^\vee[n]$. Since $\deg(\Phi) = \deg(\Phi^\vee)$ and $\deg(\Phi) = n^g = n^2$, we have $\deg(\Phi^\vee) = n^2$. Thus we can only have $\ker(\Phi^\vee) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over $\bar{k}$.

Now let $Q_1, Q_2 \in \ker(\Phi^\vee)$. To complete the proof, it remains to show $e_{B^\vee[n]}(Q_1, Q_2) = 1$. The composition $\lambda_B \circ \Phi : A \to B^\vee$ is an isogeny with dual $\lambda_A^{-1} \circ \Phi^\vee : B^\vee \to A$. Since $Q_1 \in B[\Phi^\vee]$, there exists $P \in A[n]$ such that $\lambda_B \circ \Phi(P) = Q_1$. So

$$\begin{aligned} e_{B^\vee[n]}(Q_1, Q_2) &= e_{B^\vee[n]}\big(\lambda_B \circ \Phi(P), Q_2\big) \\ &= e_{A[n]}\big(P, \lambda_A^{-1} \circ \Phi^\vee(Q_2)\big) && \text{by Lemma 1.55(1) with } f = \lambda_B\Phi \\ &= e_{A[n]}(P, 0_A) = 1 && \text{since } Q_2 \in \ker(\Phi^\vee) \end{aligned}$$

Therefore the pairing is trivial on the kernel of $\Phi^\vee$, completing the proof. □

Now suppose λ' is another polarization on B such that $\Phi^\vee \circ \lambda' \circ \Phi = n\lambda_A$. Then $\lambda' = \lambda_B$. This follows from the same argument given in the proof of the above lemma.

Lemma 1.70. *Let C be a genus 2 curve, let $\phi_1 \colon C \to E_1$ be an optimal cover of degree n and let $\phi_2 \colon C \to E_2$ be a complimentary cover. Then*

$$\phi_1^* + \phi_2^* \colon E_1 \times E_2 \to J$$

is a polarized (n, n)-isogeny, with dual isogeny

$$\phi_{1,*} \times \phi_{2,*} \colon J \to E_1 \times E_2$$

Proof. The duality statement is immediate. To prove that the isogeny is polarized, we just have to verify that

$$(\phi_{1,*} \times \phi_{2,*}) \circ (\phi_1^* + \phi_2^*) = (n \operatorname{id}_{E_1} \times n \operatorname{id}_{E_2})$$

which follows because $\phi_{i,*} \circ \phi_j^* = 0$ and $\phi_{i,*} \circ \phi_i^* = n \operatorname{id}_{E_i}$ for $(i, j) = (1, 2), (2, 1)$. Finally, it is an (n, n) isogeny because the kernel, being the graph of an isomorphism $\alpha : E_1[n] \to E_2[n]$, indeed has the structure $E_1[n](\bar{k}) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

So the maps ϕ_1, ϕ_2 give rise to an isogeny

$$\phi_1^* + \phi_2^* \colon E_1 \times E_2 \to J,$$

where the kernel Δ is given by

$$\Delta = \ker(\phi_1^* + \phi_2^*) = \{\, (P, \alpha(P)) \mid P \in E_1[n] \}$$

and is the graph of an isomorphism

$$\alpha \colon E_1[n] \to E_2[n].$$

For Δ to be maximally isotropic, we need for all $P, Q \in E_1[n]$ that

$$1 = e_{(E_1 \times E_2)[n]}\big((P, \alpha(P), (Q, \alpha(Q))\big) = e_{E_1[n]}(P, Q) e_{E_2[n]}(\alpha(P), \alpha(Q)).$$

We therefore consider the action of the isomorphism α on the corresponding Weil pairings.

Proposition 1.71. *Let $e_{E_1[n]}(P, Q)$ be a primitive n-th root of unity. Then $e_{E_2[n]}(\alpha(P), \alpha(Q))$ is a primitive n-th root of unity.*

Proof. We know $E_i[n](\bar{k}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $i = 1, 2$. To ease notation, write

$$e_1(\cdot, \cdot) \text{ for } e_{E_1[n]}(\cdot, \cdot) \qquad \text{and} \qquad e_2(\cdot, \cdot) \text{ for } e_{E_2[n]}(\cdot, \cdot).$$

Let S and T be generators for $E_1[n](\bar{k})$ and let ζ_n be a primitive n-th root of unity. By [45, Corollary III.8.1.1], there exist $P, Q \in E_2[n](\bar{k})$ such that $e_1(P, Q) = \zeta_n$ and by non-degeneracy of the Weil pairing, we can take $P = S$ and $Q = T$.

Since α is a group isomorphism, $\alpha(S)$ and $\alpha(T)$ will be generators of $E_2[n](\bar{k})$. Once again, we must have $e_2(\alpha(S), \alpha(T))$ be a primitive n-th root of unity. Therefore, there exists some $k \in \mathbb{N}$ with $(k, n) = 1$ such that $e_2(\alpha(S), \alpha(T)) = \zeta_n^k$. □

Thus we can look at the behaviour of an isomorphism $\alpha : E_1[n] \to E_2[n]$ by studying its action on the Weil pairing.

Definition 1.72. Let $\alpha : E_1[n] \to E_2[n]$ be an isomorphism. Then we say that α is an *isometry* if

$$e_{E_2[n]}(\alpha(P), \alpha(Q)) = e_{E_1[n]}(P, Q) \quad \text{for all } P, Q \in E_1.$$

We say that $E_1[n]$ and $E_2[n]$ are *isometric* if an isometry exists.

We say that α is an *anti-isometry* if

$$e_{E_2[n]}(\alpha(P), \alpha(Q)) = e_{E_1[n]}(P, Q)^{-1} \quad \text{for all } P, Q \in E_1.$$

We say that $E_1[n]$ and $E_2[n]$ are *anti-isometric* if an anti-isometry exists.

So Δ will be maximally isotropic if and only if α is an anti-isometry.

Definition 1.73. Let E_1, E_2 be elliptic curves and let A be a principally polarized abelian surface. Suppose that $\Phi\colon E_1 \times E_2 \to A$ is a polarized isogeny. We say that Φ is an *optimal polarized (n, n)-splitting* if $\Delta = \ker(\Phi)$ is the graph of an anti-isometry $\alpha\colon E_1[n] \to E_2[n]$.

A principally polarized abelian surface A equipped with an optimal polarized (n, n)-splitting is an *optimally (n, n)-split* principally polarized abelian surface.

Proposition 1.74. *Let C be a genus 2 curve over a field k of characteristic 0. If* $\mathrm{Jac}(C)$ *is decomposable then for some n it admits an optimal (n,n)-splitting.*

Proof. Lemma 1.63 guarantees that there exists a finite cover $C \to E_1'$, and by Lemma 1.65, there is an optimal cover $\phi_1 : C \to E_1$ as well. By Lemma 1.70, this gives rise to a polarized (n,n)-isogeny $\Phi : E_1 \times E_2 \to \mathrm{Jac}(C)$ and we have already established that its kernel is the graph of an anti-isometry. □

Note that an (n,n)-splitting does not have to map to a Jacobian. See Proposition 3.5 in Chapter 3 for an example of an (n,n)-splitting which maps to a product of elliptic curves.

1.3 $(2,2)$-Split Jacobians

This is a brief outline characterizing genus 2 curves with $(2,2)$-split Jacobians. See also [21] or [10, Chapter 14].

Lemma 1.75. *Let k be a field with* $\mathrm{char}(k) \neq 2$ *and let*

$$E_1 \colon V^2 = f(U)$$

be an elliptic curve over k, where $f(U) \in k[U]$ is a monic square-free cubic. Specifying (E_2, α), where E_2 is an elliptic curve over k and $\alpha : E_1[2] \to E_2[2]$ is an anti-isometry is equivalent to specifying $a \in k \cup \{\infty\}$ with $f(a) \neq 0$ and $d \in k^\times$ representing an element in $k^\times/k^{\times 2}$ such that

$$E_2 : \begin{cases} W^2 = -df(U) & \text{if } a = \infty \\ W^2 = d(U-a)f(U) & \text{otherwise} \end{cases}$$

where $0_{E_2} \in E_2(k)$ is the unique point with $U(0_{E_2}) = a$ and the anti-isometry is given by $\alpha(0_{E_1}) = 0_{E_2}$ and $\alpha((u,0)) = (u,0)$ for any $(u,0) \in E_1[2](\bar{k}) \setminus \{0_{E_1}\}$.

Proof. First note that any group scheme isomorphism $\alpha \colon E_1[2] \to E_2[2]$ is automatically both an isometry and an anti-isometry. This statement immediately follows from the fact that the Weil pairing on the 2-torsion maps to $\mathbb{Z}/2\mathbb{Z}$, whose non-identity element is its own inverse. Also note that any scheme isomorphism $\alpha' \colon E_1[2] \setminus \{0_{E_1}\} \to E_2[2] \setminus \{0_{E_2}\}$ can be extended uniquely to an isometry.

We first prove that if $\alpha\colon E_1[2] \to E_2[2]$ is a group scheme homomorphism, then E_2 and α can be represented as stated. Consider the projection map

$$\begin{aligned} U: \quad E_1 &\longrightarrow \mathbb{P}^1 \\ (U,V) &\longmapsto U. \end{aligned}$$

By [45, Algorithm 2.3 and Corollary 2.3.1], we see that it represents the quotient $E_1 \to E_1/\langle -1\rangle$ and that it is ramified over exactly $\pi_1(E_1[2]) = \{f(U) = 0\} \cup \{\infty\}$. Similarly, we have $U'\colon E_2 \to E_2/\langle -1\rangle$ and α induces a scheme isomorphism $\gamma\colon \{f(U) = 0\} \to U'(E_2[2] \setminus \{0_{E_2}\}$. This is an isomorphism of étale degree 3 subschemes of $\mathbb{P}^1$, and so it extends uniquely to an isomorphism $\mathbb{P}^1 \to \mathbb{P}^1$. That is to say, γ is an isomorphism which sends the three points $A := \{f(U) = 0\} \in \mathbb{P}^1(\bar{k})$ to the three points $B := U'(E_2[2] \setminus \{0_{E_2}\}) \in \mathbb{P}^1(\bar{k})$ such that $\mathrm{Gal}(k[A]/k) \cong \mathrm{Gal}(k[B]/k)$. But an isomorphism which determines the images of three distinct points of a $\mathbb{P}^1$ extends uniquely to an isomorphism $\mathbb{P}^1(\bar{k}) \to \mathbb{P}^1(\bar{k})$. Hence $\gamma^{-1} \circ U'\colon E_2 \to \mathbb{P}^1$ is a degree 2 cover ramified over $\{f(U) = 0\}$ and some fourth point $\gamma^{-1}(U'(0_{E_2})) = a$ (hence $f(a) \neq 0$). It follows that E_2 admits a model as stated and that α is a map as advertised.

Conversely, it is clear that as long as $f(a) \neq 0$, the model for E_2 describes an elliptic curve and α describes a scheme isomorphism $E_1[2] \to E_2[2]$ sending 0_{E_1} to 0_{E_2}, so it does define an anti-isometry. □

Theorem 1.76. *Let k be a field with $\mathrm{char}(k) \neq 2$. Let E_1, E_2 be elliptic curves given by models*

$$\begin{aligned} E_1\colon V^2 &= f(U) \\ E_2\colon W^2 &= d(U-a)f(U) \end{aligned}$$

and let $\alpha\colon E_1[2] \to E_2[2]$ be the isometry induced by the identification $U(E_1[2] \setminus \{0_{E_1}\}) = U(E_2[2] \setminus \{0_{E_1}\})$. If $a \neq \infty$ then the fibre product $C_2 = E_1 \times_{\mathbb{P}^1} E_2$ is a curve of genus 2 admitting a model

$$C_2\colon Y^2 = f(\frac{1}{d}X^2 + a),$$

where the double covers $\phi_1\colon C_2 \to E_1$ and $\phi_2\colon C_2 \to E_2$ are induced by the relations

$$U = \frac{1}{d}X^2 + a, \quad V = Y, \quad W = XY.$$

Furthermore, the isogeny

$$\phi_1^* + \phi_2^*\colon E_1 \times E_2 \to \mathrm{Jac}(C_2)$$

is the $(2,2)$*-splitting corresponding to* α*.*

Proof. That C_2 is a model of the fibre product of E_1 and E_2 over the U-line can be verified immediately. If we establish that ϕ_1 is an optimal cover and that ϕ_2 is a complimentary cover then Lemma 1.70 establishes that $\phi_1^* + \phi_2^*$ is a $(2,2)$-splitting. Optimality follows because ϕ_1 and ϕ_2 are of prime degree. It follows that $\phi_1^* : E_1 \to \mathrm{Jac}(C_2)$ is injective.

To show that ϕ_2 is complimentary we need that $\phi_{2,*} \circ \phi_1^* = 0$. But these are maps that come from a fibre product, so we can compute the composition by taking a divisor on E_1, push it down to $\mathbb{P}^1_U$ and pull it back to E_2. Since we map through a $\mathbb{P}^1$, any degree 0 divisor must map into the principal class on E_2, which establishes that $\phi_{2,*} \circ \phi_1^* = 0$.

It is straightforward to check that $\phi_1^* + (\phi_2^* \circ \alpha) : E_1[2] \to \mathrm{Jac}(C_2)$ is zero and hence that the kernel of $\phi_1^* + \phi_2^*$ is indeed the graph of α. □

Definition 1.77. Let E be an elliptic curve over a separable quadratic extension L/k. We write $\Re_{L/k}(E)$ for the *Weil restriction of scalars* of E with respect to L/k, in the sense of [2, §7.6].

For the purposes here, it is sufficient to know that $A = \Re_{L/k}(E)$ is an abelian surface over k that over L is isomorphic to $E \times E^\sigma$, where σ is a non-trivial automorphism of L over k. The product polarization on the latter descends to a k-rational principal polarization on A.

Proposition 1.78. *Let* k *be a field with* $\mathrm{char}(k) \neq 2$*. Let* E *be an elliptic curve over* k*, let* $d \in k^\times$ *represent a class in* $k^\times/k^{\times 2}$ *and let* $\alpha : E[2] \to E^{(d)}[2]$ *be the obvious isometry. Let* $\Delta \subset E[2] \times E^{(d)}[2]$ *be the graph of* α*. Then*

$$(E \times E^{(d)})/\Delta \cong \begin{cases} E \times E & \text{if } d \text{ is a square} \\ \Re_{k(\sqrt{d})/k)}(E) & \text{otherwise.} \end{cases}$$

Proof. If d is square, then Proposition 3.5 will apply with $n = 1$ and we find the $(2,2)$-isogeny given by $\Phi\colon (P,Q) \mapsto (P+Q, P-Q)$.

If d is not a square, the first case at least gives us a description of Φ over $k(\sqrt{d})$. We just have to check that Φ descends to a morphism over k with the twisted Galois actions on domain and codomain. Both $(E \times E^{(d)})(\bar{k})$ and $\Re_{k(\sqrt{d})/k)}(E)(\bar{k})$ are isomorphic to $E(\bar{k}) \times E(\bar{k})$ as groups, but have twisted Galois actions. Let $\chi_d\colon \mathrm{Gal}(\bar{k}/k) \to \{\pm 1\}$ be the quadratic

character belonging to $k(\sqrt{d})/k$. The Galois action on $E(\bar{k})\times E(\bar{k})$ corresponding to $E\times E^{(d)}$ is

$$(P,Q)^\sigma = (P^\sigma, \chi_d(\sigma)Q^\sigma)$$

and the action corresponding to $\Re_{k(\sqrt{d})/k)}(E)$ is

$$(P,Q)^\sigma = \begin{cases} (P^\sigma, Q^\sigma) & \text{if } \chi_d(\sigma) = 1 \\ (Q^\sigma, P^\sigma) & \text{if } \chi_d(\sigma) = -1. \end{cases}$$

We want to test that the isogeny $\Phi\colon E(\bar{k}) \times E(\bar{k}) \to E(\bar{k}) \times E(\bar{k})$ defined by $(P,Q) \mapsto (P+Q, P-Q)$ descends to k when we twist domain and codomain to $E \times E^{(d)}$ and $\Re_{k(\sqrt{d})/k)}(E)$ respectively. So we must establish that $(\Phi(P,Q))^\sigma = \Phi((P,Q)^\sigma)$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$, with the appropriately interpreted twisted action. It is immediate that this is the case if $(\sqrt{d})^\sigma = \sqrt{d}$. In the other case we verify that

$$\begin{aligned}(\Phi(P,Q))^\sigma = (P+Q, P-Q)^\sigma = (P^\sigma - Q^\sigma, P^\sigma + Q^\sigma) = \\ (P^\sigma + \chi_d(\sigma)Q^\sigma, P^\sigma - \chi_d(\sigma)Q^\sigma) = \Phi(P^\sigma, \chi_d(\sigma)Q^\sigma) = \Phi((P,Q)^\sigma).\end{aligned}$$

This confirms that the isogeny is indeed defined over k. It also shows that the product polarization on $E \times E$ over $k(\sqrt{d})$ descends to a principal polarization on $\Re_{k(\sqrt{d})/k)}(E)$ over k such that Φ is a polarized $(2,2)$-isogeny. □

Chapter 2

Richelot Isogenies

Introduction

In this chapter, we discuss polarized $(2,2)$-isogenies between Jacobians of genus 2 curves. Such isogenies are also known as *Richelot isogenies*. Much work has been done on Richelot isogenies, see [46, Chapter 8], [10, Chapter 9] [4], and [17, Section 4]. These papers focus on Richelot isogenies over algebraically closed base fields. The new contribution in this thesis is Proposition 2.6, where we determine the appropriate twist of the codomain for Richelot isogenies that have a kernel that is not pointwise defined over the base field.

2.1 Polarized (2,2)-Isogenies on Jacobians of genus 2 curves

Let k be a field of odd characteristic, let $\bar{k}$ be an algebraic closure of k and let C be a curve of genus 2 over k. Then C admits a model of the form

$$C : Y^2 = f(X) = f_6X^6 + f_5X^5 + \cdots + f_1X + f_0, \tag{2.1.1}$$

where $f(X) \in k[X]$ is a square-free polynomial of degree 5 or 6. If k has at least 6 elements, then we can assume that $f_6 \neq 0$. There are some curves over $k = \mathbb{F}_3, \mathbb{F}_5$ that escape our analysis. In fact, one can show that such curves have Richelot isogenies defined over k to be of the type that is already covered in existing literature. See Remark 2.7 for a full discussion of these curves. Note that $(f_6Y)^2 = f_6^2 f(X)$ is also a model of C over k, so it is not a restriction to insist that the leading coefficient is a cube. We assume that $f_6 = q_2^3$ for some $q_2 \in k$.

We begin by describing $\mathrm{Jac}(C)[2]$, the Weil pairing on it, and its maximal isotropic subgroups. Let $w_1, \ldots, w_6$ be the roots of $f(X)$ in $\bar{k}$. The Weierstrass points of C are the six points $T_i = (w_i, 0)$. The non-zero two-torsion points in $\mathrm{Pic}^0(C/\bar{k})$ are exactly the divisor classes $T_{\{i,j\}} = [T_i - T_j] = [T_j - T_i]$, and the Weil pairing is given by

$$e_{J[2]}(T_{\{i,j\}}, T_{\{k,l\}}) = (-1)^{\#\{i,j,k,l\}}.$$

Proposition 2.1. *Let $J = \mathrm{Jac}(C)$. The maximal isotropic subgroups of $J[2]$ are exactly of the form*

$$\{0, T_{\{i_1,i_2\}}, T_{\{i_3,i_4\}}, T_{\{i_5,i_6\}}\},$$

where the indices are given by a partition $\{\{i_1,i_2\},\{i_3,i_4\},\{i_5,i_6\}\}$ of $\{1,\ldots,6\}$ into three disjoint pairs.

Proof. For a subgroup $A \subset J[2]$ to be isotropic with respect to the Weil pairing, we need

$$e_{J[2]}(P, Q) = 1$$

for all $P, Q \in A$.

Let $M = \{0, T_{\{i_1,i_2\}}, T_{\{i_3,i_4\}}, T_{\{i_5,i_6\}}\}$. Notice that $\#\{i_1, i_2, i_3, i_4\} = 4$ and so

$$e_{J[2]}(T_{\{i_1,i_2\}}, T_{\{i_3,i_4\}}) = (-1)^4 = 1.$$

Performing similar calculations on the other pairs of elements of M yield the same result, hence M is an isotropic subgroup of $J[2]$.

Now suppose $T_{\{i,j\}} \in J[2]$ is not an element of M. Without loss of generality, suppose $i = i_1$. Then $j \neq i_2$ and so $\#\{i, j, i_1, i_2\} = 3$, hence $e_{J[2]}(T_{\{i,j\}}, T_{\{i_1,i_2\}}) = (-1)^3 = -1$. Therefore M is a maximal isotropic subgroup.

Now suppose $A \subset J[2]$ is a maximal isotropic subgroup. Then $0 \in A$ because A is a subgroup. Notice that this also implies that any set of the form $\{0, T\} \subset J[2]$ is isotropic with respect to the Weil pairing, so a maximal isotropic subgroup has at least one non-zero element. Let $T_{\{i,j\}} \in A$ be non-zero and let $\{k, l\} \subset \{1, \ldots, 6\}$ be disjoint from $\{i, j\}$. Then $e_{J[2]}(T_{\{i,j\}}, T_{\{k,l\}}) = 1$, so any maximal isotropic subgroup contains at least 2 non-zero elements. Since $T_{\{i,j\}} + T_{\{k,l\}} = T_{\{m,n\}}$ with $\{i, j, k, l, m, n\} = \{1, \ldots, 6\}$, we see that any maximal isotropic subgroup is contained in one of the form M, completing the proof. □

For ease of notation, we assume that $(i_1, \ldots, i_6) = (1, \ldots, 6)$.

Proposition 2.2. *The maximal isotropic subgroup in Proposition 2.1 corresponds to specifying a factorization*

$$F_j(X) = q_2X^2 + q_{1,j}X + q_{0,j} = q_2(X - w_{2j-1})(X - w_{2j})$$

such that

$$f(X) = F_1(X)F_2(X)F_3(X).$$

Proof. This proposition follows immediately from the fact that every non-zero two-torsion point of J corresponds to two Weierstrass points of C whose coordinates are the roots of $f(X)$ over $\bar{k}$. □

Definition 2.3. We say that $\{F_1(X), F_2(X), F_3(X)\} \subset \bar{k}[X]$ is a *quadratic splitting* of f. We say that $\{F_1(X), F_2(X), F_3(X)\}$ is a quadratic splitting *over* k if it is stable under $\mathrm{Gal}(\bar{k}/k)$. Note that the $F_i(X)$ do not have to be individually defined over k.

Lemma 2.4. *Let k be a field of odd characteristic with $\#k > 5$ and let C be a curve of genus 2 over k. Suppose $\Delta \subset \mathrm{Jac}(C)[2]$ is a maximal isotropic subgroup scheme over k. Let L be the coordinate ring of $\Delta \setminus \{0\}$. Then there is a quadratic polynomial $Q(X) \in L[X]$ such that C admits a model of the form*

$$C : Y^2 = f(X) = \mathrm{Norm}_{L[X]/k[X]}(Q(X)). \tag{2.1.2}$$

Conversely, for any cubic étale algebra L/k, any such representation gives rise to a maximal isotropic subgroup scheme $\Delta \subset \mathrm{Jac}(C)[2]$ with $\Delta \setminus \{0\} = \mathrm{Spec}(L)$.

Proof. We choose a model of the form (2.1.1) with $f_6 = q_2^3$. We label the roots $w_1, \ldots, w_6$ of $f(X)$ in $\bar{k}$ such that

$$\Delta(\bar{k}) = \{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$$

Let $F_j(X)$ be defined as in Proposition 2.2. The group $\mathrm{Gal}(\bar{k}/k)$ acts by permutation on $\{T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$ and the identification $F_j(X) \mapsto T_{\{2j-1,2j\}}$ is Galois-covariant, so $\{F_1(X), F_2(X), F_3(X)\}$ is a quadratic splitting of $f(X)$ over k. It follows that there is a polynomial $Q(X) \in L[X]$ that maps to each of the F_j under the three k-algebra homomorphisms $L \to \bar{k}$. This yields that C is indeed of the form (2.1.2).

For the converse, note that the three images $F_j(X)$ of $Q(X)$ under the three maps $L[X] \to \bar{k}[X]$ give rise to a quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$ of $f(X)$ over k and hence to a maximal isotropic subscheme $\Delta \subset \mathrm{Jac}(C)[2]$ over k with $\Delta \setminus \{0\} = \mathrm{Spec}(L)$. □

We now describe the codomain of a Richelot isogeny. Suppose that $\Delta \subset \mathrm{Jac}(C)[2]$ is a maximal isotropic subgroup scheme over k and let $\{F_1(X), F_2(X), F_3(X)\}$ be the corresponding quadratic splitting. We will describe the principally polarized abelian surface $B = \mathrm{Jac}(C)/\Delta$ when it is a Jacobian itself. We define the *determinant* of the quadratic splitting to be

$$\delta = \det \begin{pmatrix} q_{0,1} & q_{1,1} & q_2 \\ q_{0,2} & q_{1,2} & q_2 \\ q_{0,3} & q_{1,3} & q_2 \end{pmatrix} \tag{2.1.3}$$

(see [46, page 117] or [10, page 89]). If $\delta = 0$ then we say that the quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$ is *singular*. In this case, B is a product of elliptic curves over $\bar{k}$. Otherwise, B is the Jacobian of a genus 2 curve over $\bar{k}$ and we say $\{F_1(X), F_2(X), F_3(X)\}$ is *nonsingular*. We will determine B.

For a non-singular quadratic splitting, the following classical construction gives a curve $\tilde{C}_1$ such that $B = \mathrm{Jac}(\tilde{C}_1)$ over $\bar{k}$. Suppose $\{F_1(X), F_2(X), F_3(X)\}$ is nonsingular. Then for $(i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$ we define

$$G_i(X) = \delta^{-1} \det \begin{pmatrix} \frac{d}{dX} F_j(X) & \frac{d}{dX} F_k(X) \\ F_j(X) & F_k(X) \end{pmatrix}$$

It is straightforward to check that $\{G_1(X), G_2(X), G_3(X)\} \subset \bar{k}[X]$ is again stable under $\mathrm{Gal}(\bar{k}/k)$. For $d \in k^*$, we consider the curve

$$\tilde{C}_d : d\tilde{Y}^2 = g(\tilde{X}) = G_1(\tilde{X})G_2(\tilde{X})G_3(\tilde{X}). \tag{2.1.4}$$

Lemma 2.5. *The polynomial g is squarefree of degree 5 or 6.*

Proof. This follows by direct computation; see [46, Page 122]. □

We now review the Richelot isogeny. From [46, Theorem 8.4.11] or [4, Section 3.1] we know that over $\bar{k}$ we have $B = \mathrm{Jac}(\tilde{C}_1)$ and that the isogeny is described by a *Richelot correspondence* defined by a curve $\Gamma_d \subset C \times \tilde{C}_d$ over $\bar{k}$ given by

$$\Gamma_d : \begin{cases} F_1(X)G_1(\tilde{X}) + F_2(X)G_2(\tilde{X}) &= 0 \\ F_1(X)G_1(\tilde{X})(X - \tilde{X}) &= \sqrt{d}\,\tilde{Y}Y \\ F_2(X)G_2(\tilde{X})(X - \tilde{X}) &= -\sqrt{d}\,\tilde{Y}Y \end{cases}$$

The curve Γ_d covers both C and $\tilde{C}_d$ by

$$\pi : (X, Y, \tilde{X}, \tilde{Y}) \longmapsto (X, Y) \qquad \text{and} \qquad \pi_d : (X, Y, \tilde{X}, \tilde{Y}) \longmapsto (\tilde{X}, \tilde{Y}).$$

Notice that over $\bar{k}$, the curve Γ_d is birational to

$$\Gamma_1 \colon \begin{cases} F_1(X)G_1(\tilde{X}) + F_2(X)G_2(\tilde{X}) &= 0 \\ F_1(X)G_1(\tilde{X})(X-\tilde{X}) &= \tilde{Y}Y \\ F_2(X)G_2(\tilde{X})(X-\tilde{X}) &= -\tilde{Y}Y \end{cases}$$

by sending $\sqrt{d}Y \mapsto Y$. The first equation in Γ_1 gives $F_2(X)G_2(\tilde{X}) = -F_1(X)G_1(\tilde{X})$ and therefore the third equation is redundant, leaving

$$\Gamma_1 \colon \begin{cases} F_1(X)G_1(\tilde{X}) + F_2(X)G_2(\tilde{X}) &= 0 \\ F_1(X)G_1(\tilde{X})(X-\tilde{X}) &= \tilde{Y}Y \end{cases}$$

We obtain the *Richelot correspondence* given by Smith [46, Definition 8.4.7]. Here, the term correspondence refers to a curve $\Gamma \subset C \times \tilde{C}_1$ which covers both C and $\tilde{C}_1$, together with a means of relating their corresponding divisors. So Γ_d is a twist of the correspondence used in other literature on Richelot isogenies. They have shown that the correspondence Γ_1 leads to a Richelot isogeny on the Jacobians. We follow the same argument for Γ_d.

The Richelot isogeny can be computed by taking divisor classes on C, pulling back to Γ_d and then pushing down to $\tilde{C}_d$. In particular,

$$\pi^* : \mathrm{Pic}(C) \to \mathrm{Pic}(\Gamma_d) \qquad \text{and} \qquad (\pi_d)_* : \mathrm{Pic}(\Gamma_d) \to \mathrm{Pic}(\tilde{C}_d),$$

and so $(\pi_d)_* \circ \pi^* : \mathrm{Pic}(C) \to \mathrm{Pic}(\tilde{C}_d)$. Therefore, $(\pi_d)_* \circ \pi^*$ induces an isogeny between $\mathrm{Jac}(C)$ and $\mathrm{Jac}(\tilde{C}_d)$ by restricting each map to the degree zero part of the Picard groups $\bar{k}$. Depending on our choice of the twist d, this isogeny may be defined over k.

There are two cases where it is easy to see for which twist d we have $\mathrm{Jac}(\tilde{C}_d) = B$. In the first case, if $F_1, F_2, F_3 \in k[X]$ and $d = 1$, then Γ_d is defined over k and hence $B = \mathrm{Jac}(\tilde{C}_1)$ over k.

In the second case, if F_1 and F_2 are quadratic conjugate, say over an extension $k(\sqrt{d})$, then F_3 is necessarily defined over k. Then the set of defining equations for Γ_d is $\mathrm{Gal}(\bar{k}/k)$-stable, and hence Γ_d is defined over k. Since over $\bar{k}$, the curves $\tilde{C}_d$ and Γ_d are isomorphic to $\tilde{C}_1$ and Γ_1, it follows from the above discussion that Γ_d describes a correspondence giving rise to an isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_d)$ of the desired type. Note that $d = \mathrm{disc}(L)$.

Proposition 2.6. *Let C be a genus 2 curve as in (2.1.2). Let $\Delta \subset \mathrm{Jac}(C)[2]$ be the maximal isotropic subgroup scheme over k with $\delta \neq 0$ and $\Delta \setminus \{0\} = \mathrm{Spec}(L)$. Let $d = \mathrm{disc}(L)$. Then $\mathrm{Jac}(C)/\Delta = \mathrm{Jac}(\tilde{C}_d)$.*

Proof. The cases where $\mathrm{Gal}(\bar{k}/k)$ acts non-transitively on $\Delta(\bar{k}) \setminus \{0\}$ have been dealt with above. For the general case we consider a generic model. We will prove it there and all special cases follow by specialization.

We consider the field $K = k(h_0, h_1, h_2, q_{i,j})$ with $i, j \in \{0, 1, 2\}$ and let $L = K[T]/(T^3 + h_2T^2 + h_1T + h_0)$ and let $Q(X) \in L[X]$ be defined by

$$Q = \sum_{i,j=0}^{2} q_{i,j} T^j \, X^i.$$

We now consider the curve $C\colon Y^2 = f(X) = \mathrm{Norm}_{L[X]/k[X]}(Q(X))$ over K.

We have that L/K is a cubic extension with Galois closure $L(\sqrt{d})$ over K. Using the discussion above, we know that $B = \mathrm{Jac}(\tilde{C}_d)$ over L. However, we know that B itself is defined over K as a principally polarized variety, so B must be some twist of $\mathrm{Jac}(\tilde{C}_d)$ that trivializes over the cubic extension L. However we have $\mathrm{Aut}_{\overline{K}}(\mathrm{Jac}(\tilde{C}_d)) = \mathrm{Aut}_{\overline{K}}(\tilde{C}_d) = \{\pm 1\}$, so both only have quadratic twists. It follows the twist must be trivial.

Specialization now yields that for any curve C of the stated form, a polarization preserving isomorphism $\mathrm{Jac}(C)/\Delta \simeq \mathrm{Jac}(\tilde{C}_d)$ over k exists. □

With Proposition 2.6, we can now always determine the appropriate twist d of the codomain. Over algabraically-closed base fields or in cases where $F_1, F_2, F_3 \in k[X]$, we use $d = 1$. Otherwise, we twist by the discriminant of L.

Remark 2.7. In the opening paragraph of Section 2.1, we simplified our discussion by assuming that the genus 2 curve $C : Y^2 = f(X)$ had a model in which f was squarefree of degree 6. There are some specific cases where this is not true. We conclude this chapter by considering genus 2 curves which are given by a model $C : Y^2 = f(X)$, where f is a polynomial of degree 5. We show in general how one obtains a model $Y^2 = g(X)$ which is birational to C but where g has degree 6. In doing so, we discuss the special cases where this construction fails and show that in all of these special cases, the Richelot isogenies on the Jacobians of these genus 2 curves is already covered by existing literature.

Suppose C is a genus 2 curve over k with a model $Y^2 = f(X)$ where f is a squarefree polynomial of degree 5. Then the Weierstrass points of C are the five points $(w_i, 0)$ for $i = 1$ to 5 where w_i are the five roots of f over $\bar{k}$, together with the point at infinity. If there exists $a \in k$ such that $a \neq w_i$ for all $i = 1$ to 5, then one can make the birational transformation

$$\varphi : X \longmapsto \frac{aX}{X - a}$$

which sends the point at infinity to the point a and the point a to the point at infinity. Since the point $(a, 0)$ is not a Weierstrass point of C, this birational transformation ends up swapping the Weierstrass point at infinity with another k-rational point. In this way, we obtain a model where all the Weierstrass points are moved away from infinity and so this model would be given by a squarefree polynomial in X of degree 6.

The problem arises when the points of the form $(a, 0)$ are all Weierstrass points for all $a \in k$. This can obviously only happen when $\#k < 6$ and therefore can only happen for $k = \mathbb{F}_3$ or $\mathbb{F}_5$. The curves to consider are

$$k = \mathbb{F}_5 \text{ and } C_1 : Y^2 = f(X) = X(X-1)(X-2)(X-3)(X-4)$$
$$k = \mathbb{F}_3 \text{ and } C_2 : Y^2 = g(X) = X(X-1)(X-2)p(X)$$

where $p(X) \in \mathbb{F}_3[X]$ is an irreducible polynomial of degree 2.

In the first case, $C_1(\mathbb{F}_5)$ has five $\mathbb{F}_5$-rational Weierstrass points $(0, 0), \ldots, (4, 0)$, together with the point at infinity. So, in this case, all the Weierstrass points are $\mathbb{F}_5$-rational and the classic interpretation of the Richelot isogeny is applicable (in this case, one of the polynomials in a quadratic splitting would be linear). See [46, Section 8.4], in particular, note that Lemmas 8.4.2 and 8.4.3 include the possibility of having (at most) one linear term among the three polynomials in a quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$.

In the second case, $C_2(\mathbb{F}_3)$ has three $\mathbb{F}_3$-rational Weierstrass points $(0, 0)$, $(1, 0)$, and $(2, 0)$, together with the point at infinity. This leaves two Weierstrass points which are not $\mathbb{F}_3$-rational, but are instead quadratic conjugates. Let $(w_1, 0)$ and $(w_2, 0)$ be these two Weierstrass points of C_2 which are not $\mathbb{F}_3$-rational and consider the possible quadratic splittings of $g(X)$.

Suppose first that $c(X - w_1)(X - w_2)$ is one of the three polynomials in the quadratic splitting for some $c \in k$. Then once again this case is covered by existing literature. The footnote on page 114 of Smith [46]) allows for the possibility that the polynomials in a given quadratic splitting were k-rational, but were irreducible over k (that is to say, the individual Weierstrass points corresponding to that polynomial need not be k-rational).

The other possibility is that w_1 and w_2 are roots of distinct polynomials in the quadratic splitting. Without loss of generality, consider a quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$

where $(X - w_1)$ is a factor of $F_1(X)$ and $(X - w_2)$ is a factor of $F_2(X)$. In this case,

$$F_1(X) = (X - w_1)L_1(X)$$
$$F_2(X) = (X - w_2)L_2(X)$$

where $L_1(X), L_2(X) \in \{1, X, (X-1), (X-2)\}$ with $L_1(X) \neq L_2(X)$. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$ be an element of the Galois group which swaps w_1 and w_2. Then

$$F_1^\sigma(X) = (X - w_2)L_1(X)$$
$$F_2^\sigma(X) = (X - w_1)L_2(X)$$

so $F_1^\sigma \notin \{F_1(X), F_2(X), F_3(X)\}$ and the quadratic splitting is not Galois stable as required.

Chapter 3

Characterization of genus two curves with $(4,4)$-split Jacobians

Introduction

In this chapter, we classify all principally polarized abelian surfaces J which admit an optimal $(4,4)$-splitting. We provide models through which one can obtain all such principally polarized abelian surfaces J through an appropriate specialization. In particular, we prove in Section 3.5

Theorem 3.1. *Let J be a principally polarized abelian surface over a field k with $\mathrm{char}(k) \nmid 6$ and $\#k > 5$. Then J admits an optimal $(4,4)$-splitting*

$$\Phi_4 \colon E_1 \times E_2 \to J$$

if and only if one of the following holds.

1. *$J = \mathrm{Jac}(C_4)$ where C_4 is a genus 2 curve admitting a model of the form given in Appendix B.2,*
2. *$J = \mathrm{Jac}(C_4')$ and $E_2 = E_1^{(D)}$, where $D = \mathrm{disc}(E_1)$, and where C_4' admits a model*

$$C_4' \colon Y^2 = -64bc\frac{1}{D^3}X^6 + \frac{64}{3}b\frac{1}{D^2}X^5 + 16bc\frac{1}{D^2}X^4 + \frac{224}{27}b\frac{1}{D}X^3 + 4bc\frac{1}{D}X^2 + \frac{4}{3}bX - bc,$$

3. *$J = E_1 \times E_2$ and there is a 3-isogeny $E_1 \to E_2$,*

4. $J = E_1/\langle T_2\rangle \times E_1/\langle T_3\rangle$, *where* $E_1 = E_2$ *is an elliptic curve with* $E_1[2](k) = \{0, T_1, T_2, T_3\}$

5. $J = \Re_{k(\sqrt{D})/k}(E_1/\langle T_2\rangle)$, *where* $D = \mathrm{disc}(E_1)$ *is a non-square,* $E_1[2](k) = \{0, T_1\}$ *and* $E_1[2](k(\sqrt{D})) = \{0, T_1, T_2, T_3\}$ *and* $E_2 = E_1^{(D)}$.

The model C_4' can be obtained as an appropriate specialization of a model which is isomorphic to C_4 (see Proposition 3.16).

We use the model (B.2.1) to describe a birational model of the 2-dimensional locus of optimally $(4,4)$-split Jacobians in the moduli-space of curves of genus 2. The *Igusa invariants* I_2, I_4, I_6, I_8, and I_{10} (see [24]) of a genus 2 curve C classify the isomorphism class of C over an algebraically closed field. As we will be working over fields k where $\mathrm{char}(k) \neq 2$, it suffices to use I_2, I_4, I_6, and I_{10} to classify the isomorphism class of C. These invariants are homogeneous polynomials of degrees 2, 4, 6, and 10 respectively in the coefficients of the defining polynomial for a model of the genus two curve. This moduli-space is birational to affine 3-space, as given by the *absolute invariants* of a genus two curve [25]:

$$i_1 = 144\frac{I_4}{I_2^2}, \quad i_2 = -1728\frac{(I_2 I_4 - 3I_6)}{I_2^3}, \quad i_3 = 486\frac{I_{10}}{I_2^5}. \tag{3.0.1}$$

Theorem 3.2. *The absolute invariants* i_1, i_2, i_3 *of a genus* 2 *curve with optimally* $(4,4)$*-split Jacobian satisfy an equation* $\mathcal{L}$*, of weighted degree* 90*, where* i_1, i_2, i_3 *are given weights* $2, 3, 5$ *respectively.*

The equation $\mathcal{L}$ is too large to reproduce in this thesis: it consists of 4574 monomials with coefficients having up to 138 digits. We have therefore made a copy available electronically (see [8]). The surface described by $\mathcal{L}$ is the *Humbert surface* of discriminant 16 (see [26, Corollary 1.7]).

3.1 $(4,4)$-split principally polarized abelian varieties

Let J be an optimally $(4,4)$-split principally polarized abelian variety as defined in Definition 1.73 and let $\Phi_4 : E_1 \times E_2 \to J$ be an optimal $(4,4)$-splitting for J. Then $\Delta_4 = \ker(\Phi_4)$ is the graph of an anti-isometry $\alpha_4 : E_1[4] \to E_2[4]$. But $E_i[2] \subset E_i[4]$, so we also have $\alpha_2 := \alpha_4|_{E_1[2]} : E_1[2] \to E_2[2]$. The subgroup $\Delta_2 = \Delta_4 \cap (E_1 \times E_2)[2]$ is the graph of α_2, so we see that Φ_4 factors through an optimal $(2,2)$-splitting $E_1 \times E_2 \to A = (E_1 \times E_2)/\Delta_2$. We use the principal polarizations to identify $E_1 \times E_2$, A, and J with their duals. We obtain

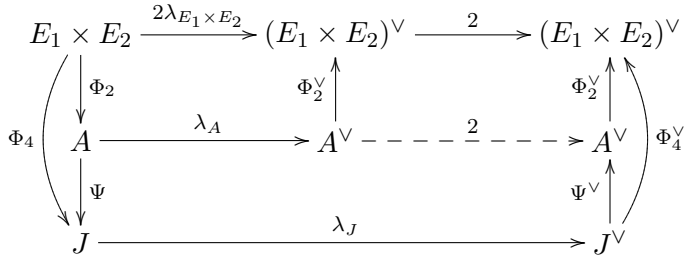


Figure 3.1: Factorization of Φ_4 through an optimal $(2,2)$-splitting.

the diagram shown in Figure 3.1. We want to establish that the diagram in the figure is commutative when we add the dashed arrow. To lighten our notation, we avoid explicitly referring to the polarizations as much as possible. To this end we introduce the shorthand notation

$$\begin{aligned}\Psi^* =& \lambda_A^{-1} \circ \Psi^\vee \circ \lambda_J,\\ \Phi_2^* =& \lambda_{E_1\times E_2}^{-1} \circ \Phi_2^\vee \circ \lambda_A,\\ \Phi_4^* =& \lambda_{E_1\times E_2}^{-1} \circ \Phi_4^\vee \circ \lambda_J.\end{aligned}$$

Lemma 3.3. *The isogeny $\Psi : A \to J$ is a polarized $(2,2)$-isogeny. Furthermore,* $\ker(\Psi) \cap \ker(\Phi_2^*) = \{0\}$.

Proof. From Lemma 1.55, it follows that for $P, Q \in (E_1 \times E_2)[4]$, we have that

$$e_{(E_1\times E_2)[4]}(P,Q) = e_{A[2]}(\Phi_2(P), \Phi_2(Q)).$$

Hence we see that $\ker(\Psi) = \Phi_2(\Delta_4) \subset A[2]$ is maximal isotropic, so by Lemma 1.56 there is a principal polarization $\lambda' \colon J \to J^\vee$ such that $2\lambda_A = \Psi^\vee \circ \lambda' \circ \Psi$. It follows that

$$\Phi_2^\vee \circ \Psi^\vee \circ \lambda' \circ \Psi \circ \Phi_2 = 4\lambda_{E_1\times E_2} = \Phi_4^\vee \circ \lambda_J \circ \Phi_4,$$

so the image of $(\lambda' - \lambda_J) \circ \Phi_4$ is contained in $\ker(\Phi_4^\vee)$, which is finite. On the other hand, Φ_4 is surjective and J is connected, so $\lambda' - \lambda_J$ is constant and hence $\lambda' = \lambda_J$. This establishes that Ψ is indeed a polarized $(2,2)$-isogeny.

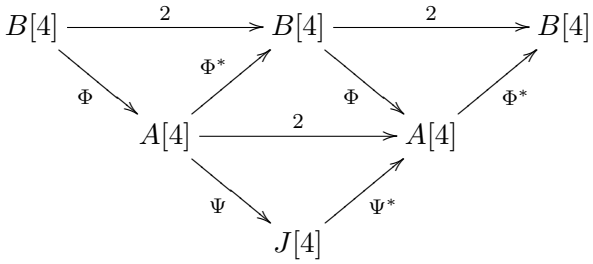
In order to see that $\ker(\Psi) \cap \ker(\Phi_2^*) = \{0\}$, note that Φ_2 is injective on $E_1[2] \times \{0\}$ and maps it onto $\ker(\Phi_2^*)$, because $\Phi_2^* \circ \Phi_2 = 2$. Since $\Psi \circ \Phi_2$ is injective on $E_1[4] \times \{0\}$, it follows that Ψ is also injective on $\Phi_2(E_1[2] \times \{0\}) = \ker(\Phi_2^*)$. This shows that $\ker(\Psi) \cap \ker(\Psi_2^*) = \{0\}$. □

In fact, whether $\Psi \circ \Phi$ is a $(4,4)$-isogeny is completely determined by $\ker(\Psi) \cap \ker(\Phi)$.

Lemma 3.4. *Let A, B, J be polarized abelian surfaces over k with $\mathrm{char}(k) \neq 2$. Suppose that $\Phi^*\colon A \to B$ and $\Psi\colon A \to J$ are polarized $(2,2)$-isogenies. Then*

1. *$\Psi \circ \Phi\colon B \to J$ is a polarized $(4,4)$-isogeny if and only if $\ker(\Psi) \circ \ker(\Phi^*) = \{0\}$,*
2. *$\Psi \circ \Phi\colon B \to J$ is a polarized $(2,2,2,2)$-isogeny if and only if $\ker(\Psi) = \ker(\Phi^*)$, and*
3. *$\Psi \circ \Phi\colon B \to J$ is a polarized $(4,2,2)$-isogeny if and only if $\ker(\Psi) \cap \ker(\Phi^*) \simeq \mathbb{Z}/2\mathbb{Z}$.*

Proof. It is immediate that $\Psi \circ \Phi$ is a polarized isogeny. The nature of the isogeny can be read off from the kernel, so we investigate what these isogenies do on the 4-torsion. The isogenies we consider fit in the following commutative diagram.



Since $\mathrm{char}(k) \neq 2$, each of $B[4](\bar{k}), A[4](\bar{k}), J[4](\bar{k})$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^4$ as a $\mathbb{Z}$-module. We normalize choice of basis such that the Weil pairing on each is given by

$$e(\underline{v}, \underline{w}) = \underline{v}^T \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \underline{w}$$

The following are matrices that correspond to polarized $(2,2)$-isogenies,

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ M^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},\ N = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ N^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

where $MM^* = NN^* = 2\mathrm{id}$. It is straightforward to check that $\ker(NM) \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$ and that $\ker(MM) = (\mathbb{Z}/4\mathbb{Z})^2$. Correspondingly, we find $\ker(N) \cap \ker(M^*) \simeq (\mathbb{Z}/2\mathbb{Z})$ and

that $\ker(M) \cap \ker(M^*) = 0$, so only the $(4,4)$-isogeny gives rise to trivially intersecting kernels.

It remains to check that these isogenies represent all possibilities. To that end, we observe that a $(2,2)$-isogeny is determined up to isomorphism by its kernel, and that there are 15 maximal isotropic subgroups in $(\mathbb{Z}/2\mathbb{Z})^4$. It is straightforward to check that if we choose two such subgroups K_1, K_2 then there is a transformation $T \in \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ such that (TK_1, TK_2) is one of

$$\big(\ker(M^*)[2], \ker(M^*)[2]\big), \big(\ker(M^*)[2], \ker(M)[2]\big), \big(\ker(M^*)[2], \ker(N)[2]\big).$$

This shows that by choice of basis, one can ensure that the isogenies considered are indeed represented by the matrices given. □

Lemma 1.75 and Theorem 1.76 imply that if $j(E_1) \neq j(E_2)$ then $A = \mathrm{Jac}(C_2)$ for some genus 2 curve C_2. Similarly, we expect J to be a Jacobian outside some special conditions. Remark 3.6 and Proposition 3.7 describe such special conditions. In fact, Theorem 3.1 establishes that these describe all cases where J is not a Jacobian.

Proposition 3.5. *An $(n-1)$-isogeny $\phi\colon E_1 \to E_2$ gives rise to an optimal polarized (n,n)-splitting*

$$\begin{array}{rccccccc} \Phi\colon & E_1 & \times & E_2 & \to & E_1 & \times & E_2 \\ & (\ P & , & Q\ ) & \mapsto & (\ \phi^*(Q) + P & , & \phi(P) - Q\ ) \end{array}$$

where $\phi^*\colon E_2 \to E_1$ is an isogeny such that $\phi^* \circ \phi$ is multiplication-by-$(n-1)$.

Proof. Note that the restriction $\phi|_{E_1[n]}\colon E_1[n] \to E_2[n]$ yields an anti-isometry. It is straightforward to check that $\Phi \circ \Phi$ is multiplication-by-n and that $\ker(\Phi)$ consists of points $(P, \phi(P))$, with $P \in E[n]$, so the kernel of Φ is indeed that graph of an anti-isometry. □

Remark 3.6. A 3-isogeny $\phi\colon E_1 \to E_2$ induces an anti-isometry $\alpha_4\colon E_1[4] \to E_2[4]$. By Proposition 3.5, we have $J = E_1 \times E_2$ in this case.

If $j(E_1) \neq 0$ then $j(E_2) \neq j(E_1)$, so $A = \mathrm{Jac}(C_2)$. The 3-isogeny $-\phi$ gives rise to the same A, J but a different $(4,4)$-splitting, so we find that C_2 is a genus 2 curve that is a double cover of E_1 and of E_2 in 3 different ways, see also [21]. If $j(E_1) = j(E_2) = 0$ we find that A is not a Jacobian.

Proposition 3.7. *Let E be an elliptic curve with discriminant D. Suppose that E has a rational point $T_1 \in E[2](k)$ of order two.*

If D is a square then $E[2](k) = \{0, T_1, T_2, T_3\}$ and E has three 2-isogenies $\phi_i \colon E \to E/\langle T_i \rangle$. The morphism

$$\begin{array}{rccccccc} \Phi\colon & E & \times & E & \to & E/\langle T_2\rangle & \times & E/\langle T_3\rangle \\ & (\ P & , & Q\ ) & \mapsto & (\ \phi_2(P+Q) & , & \phi_3(P-Q)\ ) \end{array} \tag{3.1.1}$$

is an optimal $(4,4)$-splitting.

If D is not a square then $E[2](k(\sqrt{D})) = \{0, T_1, T_2, T_3\}$ and (3.1.1) descends to a $(4,4)$-splitting over k denoted by

$$\Phi' \colon E \times E^{(D)} \to \Re_{k(\sqrt{D})/k}(E/\langle T_2\rangle)$$

where $\Re_{k(\sqrt{D})/k}(E/\langle T_2\rangle)$ denotes the Weil restriction of E (cf. Definition 1.77).

Proof. If E has square discriminant then we know that the extension generated by $E[2](\bar{k})$ is either k or a cyclic cubic extension. The assumption that $T_1 \in E[2](k)$ implies it is the former.

In this case, it is clear that Φ is an isogeny of degree 16, defined over k. To check that Φ is an optimal $(4,4)$-splitting, we determine $\ker(\Phi)(\bar{k})$. Suppose that $(P,Q) \in \ker(\Phi(\bar{k}))$. Then $Q = P$ if $2P = 0$ or $2P = T_2$ and $Q = -P$ if $2P = T_3$ or $2P = T_2 + T_3$.

We fix generators $E[4](\bar{k}) = \langle P_2, P_3\rangle$ with $2P_2 = T_2$ and $2P_3 = T_3$. Then $Q = \alpha(P)$ where $\alpha \colon E[4](\bar{k}) \to E[4](\bar{k})$ is defined by $P_2 \mapsto P_2$ and $P_3 \mapsto -P_3$. This is indeed an anti-isometry.

If D is a non-square then we can still define Φ over $k(\sqrt{D})$. The domain and codomain of Φ' are isomorphic over $k(\sqrt{D})$ to those of Φ. Checking that Φ descends to Φ' over k is a straightforward exercise in checking Galois actions. □

3.2 2-level structure on curves of genus 2

In the last section, we showed that an optimal $(4,4)$-splitting $\Phi_4 : E_1 \times E_2 \to J$ factors through an optimal $(2,2)$-splitting $\Phi_2 : E_1 \times E_2 \to A$. In this section, we consider the case where A is the Jacobian of a genus 2 curve. We begin by stating and proving the main result of the section. We end the section with an analysis of this result from a perspective of moduli spaces of genus 2 curves.

Theorem 3.8. *Let k be a field of characteristic distinct from 2. The Jacobian of a genus 2 curve*

$$C : Y^2 = f(X)$$

has two $(2,2)$-isogenies Φ and Ψ over k if and only if the Galois group of $f(X)$ is contained in $C_2 \times V_4 \subset S_6$ or $\tilde{S}_3 = \langle (1,3,5)(2,4,6), (12)(36)(45) \rangle \subset S_6$. In the first case, $\Phi \circ \Psi^*$ is a $(4,2,2)$-isogeny. In the second case, $\Phi \circ \Psi^*$ is a $(4,4)$-isogeny.

Proof. Let $C : Y^2 = f(X)$ be a curve of genus 2 over a field k of odd characteristic and let $J = \mathrm{Jac}(C)$. Recall from Chapter 2 that $J[2](\bar{k})$ can be represented by differences of Weierstrass points of C. It follows that the action of $\mathrm{Gal}(\bar{k}/k)$ on $J[2](\bar{k})$, which is through $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$, factors through the action on the 6 Weierstrass points, which is through S_6. This yields a homomorphism $S_6 \to \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ and it is straightforward to check that it is an isomorphism.

We have also seen that maximal isotropic subgroups of $J[2]$ correspond to quadratic splittings of $f(X)$. It is straightforward to check that S_6 acts transitively on the quadratic splittings of $f(X)$. If $J[2]$ has a polarized $(2,2)$-isogeny over k, then $f(X)$ must have a Galois-stable quadratic splitting. We have

$$\mathrm{Stab}_{S_6}(\{\{1,2\},\{3,4\},\{5,6\}\}) \simeq (C_2)^3 \rtimes S_3$$

Furthermore, the remaining 14 quadratic splittings have two orbits under $(C_2)^3 \rtimes S_3$, one of length 6 and one of length 8. If $J[2]$ is to have two k-rational polarized $(2,2)$-isogenies then $\mathrm{Gal}(\bar{k}/k)$ should act through the stabilizer subgroup of a representative of one of those orbits. If we pick a stabilizer subgroup of the first orbit, we obtain

$$C_2 \times C_4 = \langle (12), (34)(56), (35), 46) \rangle$$

stabilizing 3 quadratic splittings

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,2\},\{3,5\},\{4,6\}\big\},\ \big\{\{1,2\},\{3,6\},\{4,5\}\big\} \tag{3.2.1}$$

and for the second orbit we obtain

$$\tilde{S}_3 = \langle (135)(246), (12)(36)(45) \rangle$$

stabilizing

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,4\},\{2,5\},\{3,6\}\big\},\ \big\{\{1,6\},\{2,3\},\{4,5\}\big\}. \tag{3.2.2}$$

Combining this with Lemma 3.4 yields that (3.2.1) corresponds to isogenies that combine to $(4,2,2)$-isogenies and that (3.2.2) corresponds to isogenies that combine to $(4,4)$-isogenies, completing the proof of Theorem 3.8. □

Lemma 3.9. *Let k be a field with $\mathrm{char}(k) \neq 2$. Let $\Phi_4 \colon E_1 \times E_2 \to J$ be an optimal $(4,4)$-splitting over k that factors through the $(2,2)$-splitting $\Phi_2 \colon E_1 \times E_2 \to A$. Suppose that $A = \mathrm{Jac}(C_2)$ where C_2 is a curve of genus 2. Then C_2 admits a model of the form*

$$C_2 \colon Y^2 = g(X) = f(X^2) = c_3X^6 + c_2X^4 + c_1X^2 + c_0,$$

such that $g(X)$ and $f(X)$ have the same splitting field, K, and $\mathrm{Gal}(K/k)$ is isomorphic to a subgroup of a conjugate of $\tilde{S}_3$.

Proof. By Theorem 1.76, the curve C_2 admits a model of the given form, where $V^2 = f(U)$ is a model of E_1. It remains to prove that $g(X)$ and $f(X)$ have the same splitting field.

Let L denote the splitting field of g and let K denote the splitting field of f. Then K is an extension of k, and either L is a degree two extension of K or $L = K$. By Theorem 3.8 we know that $\mathrm{Gal}(L/k) \leq \tilde{S}_3$.

The three kernels of the $(2,2)$-isogenies that are fixed by $\tilde{S}_3$ are given by the partitionings in (3.2.2). A simple verification shows that $\tilde{S}_3$ acts faithfully on each of these kernels. In particular, if $\{0, T_1, T_2, T_3\}$ is the kernel of the polarized $(2,2)$-isogeny $\mathrm{Jac}(C_2) \to E_1 \times E_2$, then $\tilde{S}_3$ has the canonical S_3-action on $\{T_1, T_2, T_3\}$. Thus, $\tilde{S}_3$ has the usual S_3 action on the roots of f. It follows f and g have the same splitting field. □

While the proof of and the condition given in Theorem 3.8 are Galois-theoretic, specifying multiple $(2,2)$-isogenies on $\mathrm{Jac}(C)$ amounts to specifying partial level structure, so one expects that the structure of the result is reflected in covers of moduli spaces as well. We will sketch how one can obtain such a formulation.

Let k be a field of characteristic different from 2. Any curve of genus 2 can be obtained by specializing $(g_0, \ldots, g_6)$ in the curve

$$C_{\underline{g}} : Y^2 = g(X) = g_6X^6 + g_5X^5 + \cdots + g_0$$

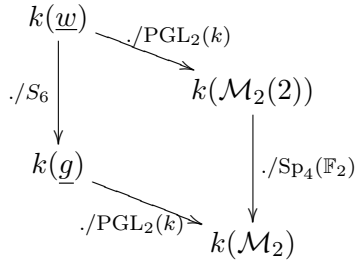
over $k(\underline{g}) = k(g_6, g_5, \ldots, g_0)$. Similarly, any curve of genus 2 with all of its Weierstrass points labeled can be obtained by specializing $(w_1, \ldots, w_6, g_6)$ in the curve

$$C_{\underline{w}} : Y^2 = g_6(X - w_1) \cdots (X - w_6)$$

over $k(\underline{w}) = k(g_6, w_1, \ldots, w_6)$. Of course, one can just forget a labelling to obtain a curve $C_{\underline{f}}$ from $C_{\underline{w}}$. This allows us to express $k(\underline{w})$ as a finite extension of $k(\underline{g})$ via

$$\begin{aligned} g_5 &= -g_6(w_1 + \cdots + w_6) \\ g_4 &= g_6(w_1w_2 + w_1w_3 + \cdots + w_5w_6) \\ &\vdots \\ g_0 &= g_6w_1 \cdots w_6. \end{aligned}$$

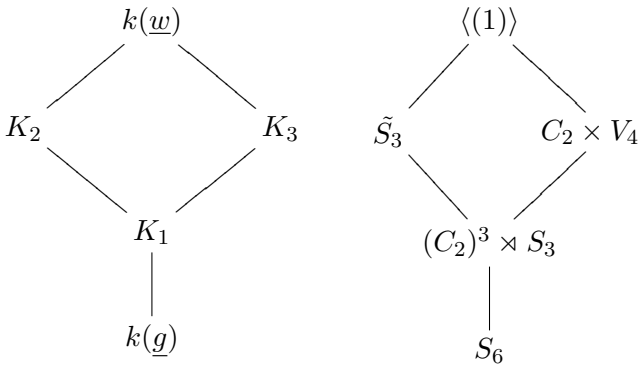
In fact, $k(\underline{w})$ is a splitting-field of $g(X)$ over $k(\underline{g})$ and $\mathrm{Gal}(k(\underline{w})/k(\underline{g})) = S_6$. As we observed in the proof of Theorem 3.8, $k(\underline{w})$ is also the splitting field of $\mathrm{Jac}(C_{\underline{g}})[2]$ over $k(\underline{g})$. The fractional linear transformations on the X-line below C induce a $\mathrm{PGL}_2(k)$-action on $k(\underline{g})$ and $k(\underline{w})$. If we divide out by this action, we obtain a relation with the function fields of the coarse moduli spaces $\mathcal{M}_2$ of curves of genus 2 and $\mathcal{M}_2(2)$ of curves of genus 2 with full level 2-structure on their Jacobians, which is an $\mathrm{Sp}_4(\mathbb{F}_2)$-cover of $\mathcal{M}_2$



The subgroups identified in Theorem 3.8 give rise to intermediate fields K_1, K_2, K_3 as depicted in Figure 3.2 and, by dividing out by $\mathrm{PGL}_2(\mathbb{F}_2)$, also moduli spaces between $\mathcal{M}_2$ and $\mathcal{M}_2(2)$. One of the interesting phenomena here, that does not occur for elliptic curves, is that there are two non-conjugate ways of specifying two maximal isotropic subgroups of $\mathrm{Jac}(C)[2]$ and hence that there are multiple partial level 2 structures that can be imposed on $\mathrm{Jac}(C)[2]$.

3.3 Bielliptic genus 2 curves with S_3 as a Galois group

In Section 3.1 we saw that a $(4,4)$-splitting $E_1 \times E_2 \to J$ gives rise to a $(2,2)$-splitting $E_1 \times E_2 \to A$, where A is a principally polarized abelian surface admitting two rational polarized $(2,2)$-isogenies with trivially intersecting kernels.



$$\begin{aligned}(C_2)^3 \rtimes S_3 &= \langle (12),(34),(56),(13)(24),(15)(26)\rangle \\ \tilde{S}_3 &= \langle (135)(246),(12)(36)(45)\rangle \\ C_2 \times V_4 &= \langle (12),(34)(56),(35)(46)\rangle\end{aligned}$$

Figure 3.2: Galois groups associated to intermediate 2-level structure

In this section, we give something close to a universal model for the genus 2 curve C_2 from Lemma 3.9. We are trying to parametrize an algebraic object (in this case, genus 2 curves with $(4,4)$-split Jacobians). Specifically, we would like to find a *universal model* for the *moduli space* of genus 2 curves with $(4,4)$-split Jacobians. A universal model, however, is only available when working with a *fine moduli space*.

Definition 3.10 (Mumford [34])**.** Let M be a collection of isomorphism classes of algebraic varieties. A *coarse moduli space for* M is a variety $\mathcal{M}$ such that if $\mathcal{X} \to T$ is a family of elements of M, that is to say, each fibre $f^{-1}(t)$ is in $\mathcal{M}$, then there is a morphism $h : T \to \mathcal{M}$ such that $h(s) = h(t)$ if and only if $f^{-1}(s) \cong f^{-1}(t)$.

A *fine moduli space for* M is a variety $\mathcal{M}$ together with a *universal family* $\pi : \mathcal{U} \to \mathcal{M}$ such that if $f : \mathcal{X} \to T$ is a family of elements of M satisfying the condition given in the coarse moduli space definition, then there is a morphism $\Phi : T \to \mathcal{M}$ such that $\mathcal{X}$ is the pullback of $\mathcal{U}$ via Φ such that $\Phi(s) = \Phi(t)$ if and only if $f^{-1}(\Phi(s)) = f^{-1}(\Phi(t))$.

Since the moduli space of genus 2 curves with $(4,4)$-split Jacobians is not a fine moduli space (indeed, the space $\mathcal{M}_2(2)$ of genus 2 curves with full level 2-structure on their Jacobians is not even a fine moduli space), a universal curve does not exist. However, by allowing extra parameters, we can still give a family that covers all possible C_2 by specialization, similar to how any elliptic curve can be obtained by specializing a general Weierstrass model $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.

Let k be a field of characteristic distinct from 2 or 3. Let C_2 be a genus 2 curve over k with a $(2,2)$-split Jacobian and let E_1 be a degree 2 subcover of C_2. Then E_1 has a model $V^2 = f(U) = U^3 + bU + c$ and $\mathrm{Gal}(f)$, the Galois group of f, is a subgroup of S_3. In order to produce the family, we concentrate on the most general case $\mathrm{Gal}(f) = S_3$. We will argue later that other cases are also parametrized.

By Theorem 1.76, the curve C_2 admits a model $Y^2 = g(X)$ where

$$g(X) = f\left(\frac{X^2}{d} + a\right)$$

with $a, d \in k$.

Working in the extension $k[U]/(f(U)) = k[r]$, the polynomials f and g factor as

$$\begin{aligned} f(U) &= (U - r)\left(U^2 + rU + \left(r^2 + b\right)\right) \\ g(X) &= \frac{1}{d^3}\left(X^2 + ad - rd\right) h(X), \end{aligned} \tag{3.3.1}$$

where

$$h(X) = X^4 + (dr + 2ad)X^2 + d^2\left(r^2 + ar + a^2 + b\right). \tag{3.3.2}$$

By Lemma 3.9, we know that g and f have the same splitting field. This means that h must be reducible over $k(r)$. Otherwise h would be irreducible and we would require a degree 4 extension over $k(r)$ to split h. The following lemma gives a testable condition.

Lemma 3.11 (Kappe and Warren [27])**.** *Let $h(x) = x^4 + bx^2 + d$ be a polynomial over a field k of characteristic $\neq 2$ and let $\pm\alpha$, $\pm\beta$ be its roots. Then the following conditions are equivalent:*

1. *$h(x)$ is irreducible over k;*
2. *The following are not squares in k:*
   - *(i) $b^2 - 4d$,*
   - *(ii) $-b + 2\sqrt{d}$, and*
   - *(iii) $-b - 2\sqrt{d}$.*

We can use Lemma 3.11 to determine the conditions on a and d such that h factors as a product of two quadratics over $k(r)$. In our case, the polynomial h will be reducible over $k(r)$ if one of the following is true:

(i) $(dr+2ad)^2 - 4d^2\left(r^2+ar+a^2+b\right)$ is a square in $k(r)$, or

(ii) $-(dr+2ad) + 2d\sqrt{r^2+ar+a^2+b}$ is a square in $k(r)$, or

(iii) $-(dr+2ad) - 2d\sqrt{r^2+ar+a^2+b}$ is a square in $k(r)$.

Taking the conditions one at a time, in case (i), after simplification, we require $-3r^2-4b$ to be a square. Observe that this is the discriminant of $x^2+rx+(r^2+b)$ and hence occurs exactly when our original polynomial $f(x)$ splits over $k(r)$. This contradicts $\mathrm{Gal}(f) = S_3$, so we ignore this possibility for now.

In the remaining two cases, we require r^2+ar+a^2+b to be a square in $k(r)$. Let $t \in k(r)$ such that $r^2+ar+a^2+b = t^2$. Since $k(r)$ is a cubic extension of k, we can set $t = t_2r^2+t_1r+t_0$. It follows that

$$\begin{aligned} r^2+ar+a^2+b &= \left(t_2r^2+t_1r+t_0\right)^2 \\ &= t_2^2r^4 + 2t_1t_2r^3 + \left(t_1^2+2t_0t_2\right)r^2 + 2t_0t_1r + t_0^2 \\ &= \left(t_1^2+2t_0t_2-bt_2^2\right)r^2 + \left(2t_0t_1-2bt_1t_2-ct_2^2\right)r + \left(t_0^2-2ct_1t_2\right). \end{aligned}$$

Equating coefficients, we obtain the system of three equations:

$$\begin{aligned} t_1^2+2t_0t_2-bt_2^2-1 &= 0 \\ -a+2t_0t_1-2bt_1t_2-ct_2^2 &= 0 \\ a^2+b-t_0^2+2ct_1t_2 &= 0. \end{aligned} \tag{3.3.3}$$

We obtain an affine variety X in $\mathbb{A}^4$ with parameters b and c. This variety has two components, interchanged by $(a,t_0,t_1,t_2) \mapsto (a,-t_0,-t_1,-t_2)$, which can be found either using a primary decomposition of a polynomial ideal (e.g., `PrimaryComponents` in Magma [3]), or by eliminating variables (say a and t_0) via resultants and multivariate GCD, and a multivariate polynomial factorization. Each component is a genus 0 curve in $\mathbb{A}^4$. Using for instance Magma, we can parametrize this curve. Writing s for the parameter, we obtain

$$\begin{aligned} a &= \frac{s^4 - 2bs^2 - 8cs + b^2}{4\left(s^3 + bs + c\right)} \\ t_0 &= \frac{-s^4 - 6bs^2 - 4cs - b^2}{4\left(s^3 + bs + c\right)} \\ t_1 &= \frac{-s^3 + bs + 2c}{2\left(s^3 + bs + c\right)} \\ t_2 &= \frac{-3s^2 - b}{2\left(s^3 + bs + c\right)}. \end{aligned} \tag{3.3.4}$$

For any $s \in k$, this parametrization gives a value for a such that $r^2 + ar + a^2 + b$ is a square in $k(r)$. Using the parametrization, we can express the square root of $r^2 + ar + a^2 + b$ as:

$$\frac{-3s^2 - b}{2\left(s^3 + bs + c\right)} r^2 + \frac{-s^3 + bs + 2c}{2\left(s^3 + bs + c\right)} r + \frac{-s^4 - 6bs^2 - 4cs - b^2}{4\left(s^3 + bs + c\right)}.$$

This allows us to evaluate the expressions in (ii) and (iii).

In case (ii) we find that $-(dr + 2ad) + 2d\sqrt{r^2 + ar + a^2 + b}$ becomes

$$\left(-\frac{1}{4\left(s^3 + bs + c\right)}\right) \cdot d \cdot F_1,$$

where $F_1 = \left(6s^3 + 2bs\right) r^2 - \left(6s^3 + 2bs\right) r - \left(3s^4 + 2bs^2 - 12cs + 3b^2\right)$. This is a square in $k(r)$ if and only if

$$d = -\left(s^3 + bs + c\right) \cdot \square \tag{3.3.5}$$

where $\square$ represents a square in k. Using (3.3.4) and (3.3.5), we find that $g(X) = f(X^2/d + a)$ has the same splitting field as f. The Galois group of g is indeed isomorphic to S_3 but its representation in S_6 is $S_3'' = \langle (123)(456), (23)(56) \rangle$ which is not conjugate to $\tilde{S}_3$ from Section 3.2. Therefore, $C\colon Y^2 = g(X)$ is not of the form predicted by Lemma 3.9.

In case (iii), using the paramatrization for a, we find $-(dr + 2ad) - 2d\sqrt{r^2 + ar + a^2 + b}$ becomes:

$$\left(-\frac{1}{4\left(s^3 + bs + c\right)}\right) \cdot d \cdot F_2$$

where $F_2 = \left(6s^2 + 2b\right) r^2 - \left(2s^3 + 6bs + 8c\right) r - \left(s^4 + 10bs^2 - 20cs + b^2\right)$. This will be a square in $k(r)$ if and only if

$$\begin{aligned} d &= \left(4b^3 + 27c^2\right)\left(s^3 + bs + c\right) \cdot \square \\ &= -D \cdot f(s) \cdot \square \end{aligned} \tag{3.3.6}$$

where $\square$ represents any square and D is the discriminant of f.

Using this parametrization, our hyperelliptic curve C_2 is given by $Y^2 = g(X)$ where:

$$\begin{aligned} g = &\frac{1}{(s^3+bs+c)^3}\left(\frac{1}{(4b^3+27c^2)^3}X^6 + \frac{3\left(s^4-2bs^2-8cs+b^2\right)}{4\left(4b^3+27c^2\right)^2}X^4\right. \\ &\left. + \frac{P(b,c,s)}{16\left(4b^3+27c^2\right)}X^2 + \frac{\left(s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2\right)^2}{64}\right) \end{aligned} \tag{3.3.7}$$

and where P is given by

$$P = 3s^8 + 4bs^6 - 48cs^5 + 50b^2s^4 + 128bcs^3 + 4b^3s^2 + 192c^2s^2 - 16b^2cs + 3b^4 + 16bc^2.$$

As desired, we find that g has the same splitting field as f and that $\mathrm{Gal}(g) \simeq \tilde{S}_3$ as found in Section 3.2. The factorization for g over its splitting field is given in appendix B.1.

Let $\phi_1 \colon C_2 \to E_1$ be the cover arising from $(X,Y) \mapsto (U,V) = (X^2/d + a, Y)$. Let $\Psi \colon \mathrm{Jac}(C_2) \to B$ be one of the other polarized $(2,2)$-isogenies we have by construction on $\mathrm{Jac}(C_2)$. Let

$$E_s \colon W^2 = -\operatorname{disc}(f) \cdot f(s) \cdot (U-a) \cdot f(U)$$

be the complementary curve and $\phi_2 \colon C_2 \to E_s$ the corresponding cover. It is straightforward to check that $\Psi \circ \phi^* \colon E_1 \to B$ is injective and hence that $\Phi_4 = \Psi \circ (\phi_1^* + \phi_2^*) \colon E_1 \times E_s \to B$ is an optimal $(4,4)$-splitting of B. This means that the data we have specified (s and Ψ) should also determine an anti-isometry $\alpha_s \colon E_1[4] \to E_s[4]$. The ambiguity of choice in Ψ corresponds to the fact that if $\alpha_s \colon E_1[4] \to E_s[4]$ is an anti-isometry, then so is $-\alpha_s$.

Let $X^-_{E_1}(4)$ be the completion of the moduli space of elliptic curves with prescribed 4-torsion structure anti-isometric to $E_1[4]$ modulo multiplication by $(\mathbb{Z}/4\mathbb{Z})^\times$. This is a cover of the j-line $X(1)$ with

$$\mathrm{Aut}_{\bar{k}}(X^-_{E_1}(4)/X(1)) = \mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z}),$$

so $X^-_{E_1}(4) \to X(1)$ is a degree 24 cover.

On the open part of the s-line where the equation for E_s defines an elliptic curve, the map $s \mapsto E_s$ provides a map from the s-line to $X^-_{E_1}(4)$. This map cannot be constant, since $a(s)$ is not constant in s, so we can interpret the s-line as a cover of $X^-_{E_1}(4)$. We will show in the proof of Proposition 3.12 that it turns out to be an isomorphism, and so E_s provides a model of the universal elliptic curve over $X^-_{E_1}(4)$. This provides an alternative construction to the one given by Silverberg [44]. Our formulas are shorter.

Proposition 3.12. *Let $b, c \in k$ such that $4b^3 + 27c^2 \neq 0$ and let*

$$E\colon V^2 = f(U) = U^3 + bU + c$$

be an elliptic curve. Let s be a parameter on $\mathbb{P}^1$ and consider

$$E_s\colon W^2 = -\operatorname{disc}(f)\left(4(s^3+bs+c)U - (s^4 - 2bs^2 - 8cs + b^2)\right) f(U),$$

with $(U,W) = (\frac{s^4-2bs^2-8cs+b^2}{4(s^3+bs+c)}, 0)$ taken to be the identity element. Then E_s is isomorphic to

$$\begin{aligned}
\tilde{E}_s\colon y^2 &= x^3 + a_4 x + a_6 \text{ with}\\
a_4 &= (4b^3+27c^2)^2(s^8b + 12s^7c - 28/3s^6b^2 - 28s^5bc - 14/3s^4b^3 - 84s^4c^2\\
&\quad + 28/3s^3b^2c - 28/3s^2b^4 - 56s^2bc^2 - 44/3sb^3c - 96sc^3 + b^5 + 20/3b^2c^2)\\
a_6 &= -(4b^3+27c^2)^3(s^{12}c - 8/3s^{11}b^2 - 22s^{10}bc + 88/27s^9b^3 - 88s^9c^2 + 55s^8b^2c\\
&\quad - 176/9s^7b^4 - 308/9s^6b^3c - 176/9s^5b^5 - 176s^5b^2c^2 - 649/9s^4b^4c - 528s^4bc^3\\
&\quad + 88/27s^3b^6 - 704/9s^3b^3c^2 - 704s^3c^4 + 154/9s^2b^5c + 352/3s^2b^2c^3 - 8/3sb^7\\
&\quad - 248/9sb^4c^2 - 64sbc^4 - 5/3b^6c - 560/27b^3c^3 - 64c^5)
\end{aligned}$$

with

$$j(\tilde{E}_s) = \frac{256}{4b^3+27c^2}\frac{\left(\begin{array}{r} 3bs^8 + 36cs^7 - 28b^2s^6 - 84bcs^5 - 14(b^3+18c^2)s^4 + 28b^2cs^3\\ -28b(b^3+6c^2)s^2 - 4c(11b^3+72c^2)s + 3b^5 + 20b^2c^2\end{array}\right)^3}{(s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2)^4}.$$

The map $s \mapsto E_s$ induces an isomorphism $\mathbb{P}^1 \to X_E^-(4)$ and $\tilde{E}_s$ provides a model of the universal curve over $X_E^-(4)$. For $s = \infty$ we find that $\tilde{E}_\infty$ is isomorphic to the quadratic twist $E^{(D)}$ of E by $D = \operatorname{disc}(E)$.

Proof. The computation of the model $\tilde{E}_s$ and its j-invariant are straightforward. It establishes that $s \mapsto j(E_s)$ induces a degree 24 cover $\mathbb{P}^1 \to X(1)$. We have already established that $s \mapsto E_s$ induces a cover $\mathbb{P}^1 \to X_{E_1}^-(4)$. The map induced by $s \mapsto j(E_s)$ factors through $j\colon X_{E_1}^-(4) \to X(1)$, which also has degree 24, so the first map must be of degree 1 and hence an isomorphism.

The only point where the curve defined by $\tilde{E}_s$ might not be immediately clear is for $s = \infty$. However, we can consider the isomorphic model $y^2 = x^3 + a_4/s^8 x + a_6/s^{12}$. Then we find that

$$\left.\frac{a_4}{s^8}\right|_{s=\infty} = (4b^3+27c^2)^2 b \text{ and } \left.\frac{a_6}{s^{12}}\right|_{s=\infty} = -(4b^3+27c^2)^3 c$$

which confirms that $E_\infty = E^{(D)}$ with $D = -16(4b^3 + 27c^2) = \mathrm{disc}(E)$. □

Note that the description of E_s is even shorter than that of $\tilde{E}_s$, but E_s has the drawback of not being a Weierstrass-form and not specializing to an elliptic curve for $s^3 + bs + c = 0$. It does show very nicely where the denominator of $j(\tilde{E}_s)$ comes from. This denominator vanishes exactly when $f(\frac{s^4-2bs^2-8cs+b^2}{4(s^3+bs+c)}) = 0$.

Corollary 3.13. *Let $E_1 \colon V^2 = U^3 + bU + c$ be an elliptic curve. The affine variety $\mathbb{P}^1_s \setminus \{s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2\}$ parametrizes principally polarized abelian surfaces J_s together with a pair of optimal $(4,4)$-splittings $\pm\Phi_4 \colon E_1 \times E_s \to J_s$.*

Corollary 3.14. *Let E be an elliptic curve over a field k with $\mathrm{char}(k) \neq 2$. Let D be the discriminant of E. Then there is an anti-isometry $\alpha_4 \colon E[4] \to E^{(D)}[4]$.*

In Sections 1.3 and 3.1, we already observed that the abelian variety A in Figure 3.1 is generally a Jacobian, a sufficient condition being that $j(E_1) \neq j(E_2)$. We now establish that the model $C_2 \colon Y^2 = g(X)$ with $g(X)$ as in Figure 3.1 specializes to a genus 2 curve such that $A = \mathrm{Jac}(C_2)$ whenever A is a Jacobian.

Lemma 3.15. *Let $\Phi_4 \colon E_1 \times E_2 \to J$ be an optimal $(4,4)$-splitting and let $\Phi_2 \colon E_1 \times E_2 \to A$ be the induced $(2,2)$-splitting as in Figure 3.1. Suppose we have a model $E_1 \colon V^2 = U^3 + bU + c$. If $A = \mathrm{Jac}(C_2)$, where C_2 is some genus 2 curve, then for some $s \in k$ we obtain a model*

$$C_2 \colon Y^2 = g(X) \text{ with } g(x) \text{ as in } (3.3.7). \tag{3.3.8}$$

Conversely, any C_2 of this form admits a $(2,2)$-splitting Φ_2 and a further polarized $(2,2)$-isogeny $\Psi \colon \mathrm{Jac}(C_2) \to J$ such that $\Psi \circ \Phi_2 \colon E_1 \times E_2 \to J$ is an optimal $(4,4)$-splitting.

Proof. An optimal $(4,4)$-splitting is specified by an anti-isometry $\alpha_4 \colon E_1[4] \to E_2[4]$. It follows from Proposition 3.12 that $E_2 \simeq E_s$ for some value of $s \in k \cup \{\infty\}$. If $s = \infty$ or $s^3 + bs + c = 0$, we have $j(E_1) = j(E_2)$ and the induced isometry $E_1[2] \to E_2[2]$ is the obvious one. In this case, $A \simeq E_1 \times E_1$ or $A \simeq \Re_{k(\sqrt{d})/k}(E_1)$, see Section 1.3. For all the other cases, the discriminant of the polynomial $g(X)$ defined in (3.3.7) is square-free as long as $j(E_s) \neq \infty$.

For the converse, $\mathrm{Jac}(C_2)$ admits an obvious $(2,2)$-splitting $\Phi_2 \colon E_1 \times E_2 \to \mathrm{Jac}(C_2)$. Moreover, there are two further $(2,2)$-isogenies Ψ defined on $\mathrm{Jac}(C_2)$ by construction. Let $\phi_1 \colon C_2 \to E_1$ be the corresponding double cover. It is straightforward to check that $\phi_1^*(E_1[2]) \cap \ker(\Psi) = 0$ and hence that $\Psi \circ \Phi_2$ is an optimal $(4,4)$-splitting. □

3.4 A model for genus 2 curves with $(4,4)$-split Jacobians

The next step is to describe a model for a genus 2 curve C_4 with a $(4,4)$-split Jacobian. From Section 3.1 we know that $\mathrm{Jac}(C_4)$ is the image under a $(2,2)$-isogeny of a $(2,2)$-split principally polarized abelian surface A, admitting three $(2,2)$-isogenies with pairwise trivially intersecting kernels. Whenever $A = \mathrm{Jac}(C_2)$, then Lemma 3.15 gives us a model for C_2. Chapter 2 provides an explicit description of $(2,2)$-isogenies between Jacobians of genus 2 curves.

In this section, we will identify the $(2,2)$-isogenies of $\mathrm{Jac}(C_2)$ defined over k and derive a description of the codomain, if it is a Jacobian. This provides us with a description of C_4 with $(4,4)$-split Jacobian in case $A = \mathrm{Jac}(C_2)$.

We consider all 15 different quadratic splittings as in Section 2.1 over $k[r,R]$ and see which are defined over the base field. As expected, we find that one of the quadratic splittings is singular. The singular quadratic splitting is

$$\{q_2(X-w_1)(X-w_2), q_2(X-w_3)(X-w_4), q_2(X-w_5)(X-w_6)\}$$

where w_i are the roots of g over $k[r,R]$ as listed in Appendix B.1 and $q_2^3 = f_6$ is the leading coefficient of g. This singular splitting is due to the $(2,2)$-isogeny $\Phi_2^*\colon \mathrm{Jac}(C_2) \longrightarrow E_1 \times E_2$. We also find that applying the Richelot correspondence (2.1.4) to the 14 generically non-singular quadratic splittings produces only two k-rational sextics, with the remaining twelve defined over $\bar{k}$, but not over k. The two quadratic splittings which yield the k-rational sextics are

$$\{q_2(X-w_1)(X-w_6), q_2(X-w_2)(X-w_3), q_2(X-w_4)(X-w_5)\} \text{ and} \tag{3.4.1}$$

$$\{q_2(X-w_1)(X-w_4), q_2(X-w_2)(X-w_5), q_2(X-w_3)(X-w_6)\}. \tag{3.4.2}$$

Notice that the singular quadratic splitting, together with the two quadratic splittings (3.4.1) and (3.4.2) come from the three partitionings that are fixed by $\tilde{S_3}$, given by (3.2.2).

Let G_1 and G_2 denote the sextics obtained by applying Richelot's construction (2.1.4) of f to the quadratic splittings (3.4.1) and (3.4.2) respectively. We find that $G_2(X) = G_1(-X)$, and therefore that both models are isomorphic. This reflects that $E_1 \times E_2$ has an extra automorphism $[1] \times [-1]$, so if Φ_4 is an optimal $(4,4)$-splitting then $\Phi_4 \circ ([1] \times [-1])$ is another one, with the the same codomain.

Proposition 2.6 allows us to select the right twist

$$C_4\colon Y^2 = DG_1(X) = F(X) \text{ where } D = \mathrm{disc}(f) = -4b^3 - 27c^2$$

(see Appendix B.2 for $F(X)$, with the extraneous factor f_6^2 removed). Looking at the denominators and the discriminant of the sextic given in Appendix B.2, we find

$$\operatorname{disc}(F) = \frac{2^6\left(s^3+bs+c\right)^{22}\left(s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2\right)}{\left(4b^3+27c^2\right)^{14}\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^{18}}$$

and hence

Proposition 3.16. *The model $C_4 : Y^2 = F(X)$ with $F(X)$ as defined in B.2 describes a genus 2 curve unless one of the following holds:*

1. $4b^3+27c^2=0$,
2. $s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2=0$,
3. $3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2=0$,
4. $s^3+bs+c=0$, *or*
5. $s=\infty$.

The cases (1) *and* (2) *correspond to situations where either E_1 or E_s is not an elliptic curve. The cases* (3) *and* (4) *correspond to* $(4,4)$*-split principally abelian surfaces that are not Jacobians, as described by Propositions 3.5 and 3.7 respectively.*

If $j(E_1)\neq 0$ then the case (5) *corresponds to a* $(4,4)$*-splitting $\Phi\colon E_1\times E_1^{(D)}\to \operatorname{Jac}(C_4')$, where*

$$C_4'\colon Y^2 = -64bc\frac{1}{D^3}X^6+\frac{64}{3}b\frac{1}{D^2}X^5+16bc\frac{1}{D^2}X^4+\frac{224}{27}b\frac{1}{D}X^3+4bc\frac{1}{D}X^2+\frac{4}{3}bX-bc, \quad (3.4.3)$$

is a curve of genus 2. If $j(E_1)=0$ then case (5) *is part of case* (3).

Proof. (1) In this case E_1 is not an elliptic curve.

(2) In Proposition 3.12 we have already seen that this relation implies $j(E_s)=\infty$.

(3) Let δ denote the determinant of the quadratic splitting (3.4.1). Then

$$N_{k[r,R]/k}(\delta) = \left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^2,$$

and we know that if (2.1.3) vanishes, then the codomain of the $(2,2)$-isogeny is a product of elliptic curves over $\bar{k}$. Proposition 3.17 explains this degeneracy.

(4) If $s^3+bs+c=0$ then $(s,0)\in E_1[2]$ is a point of order two. Furthermore, from (3.3.4) we have $a(s)=\infty$, so the $(2,2)$-splitting Φ_2 through which our $(4,4)$-splitting factors is known to be $E_1\times E_1 \to E_1\times E_1$ or $E_1\times E_1^{(D)} \to \Re_{k(\sqrt{R})/k}(E_1)$, depending on whether $D=\operatorname{disc}(E_1)$ is a square or not. Since $\#\operatorname{SL}_2(\mathbb{Z}/4\mathbb{Z}) = 8\cdot\#\operatorname{SL}_2(\mathbb{Z}/2\mathbb{Z})$, there are 8 ways over $\bar{k}$ to extend a $(2,2)$-isogeny to a $(4,4)$ isogeny. This also follows from the computation in the proof of Lemma 3.4, where one finds 8 possible kernels for Ψ trivially intersecting $\ker(\Phi^*)$. Since every value of s gives rise to two $(4,4)$-isogenies, we see that with $s=\infty$ and $s^3+bs+c=0$, all possible $(4,4)$-splittings factoring through Φ_2 must occur for these values of s. Proposition 3.7 describes six $(4,4)$ splittings of this type, so together with the two coming from $s=\infty$, these must be all.

(5) The model for C_4 as presented does not specialize well for $s=\infty$, but the isomorphic model

$$C'_{4,s}\colon (s^3Y)^2 = F(xs^2)/s^6$$

does if $b\neq 0$ and for $s=\infty$ we obtain C'_4. Note that for generic s we have a $(4,4)$-splitting

$$\Phi_4\colon E_1\times E_s \to \operatorname{Jac}(C'_{4,s})$$

where the kernel is the graph of an anti-isogeny $E_1[4]\to E_s[4]$ that is independent of s. Since domain and codomain specialize well at $s=\infty$, so must the $(4,4)$-isogeny. If $b=0$ we have $j(E_1)=0$ and we have a 3-isogeny $E_1\to E_1^{(D)}$, so case (3) applies.

□

Proposition 3.17. *Let E and E_s be the elliptic curves described in Proposition 3.12. The relation $3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2=0$ corresponds to the existence of a 3-isogeny $\phi\colon E\to E_s$.*

Proof. Note that $J_1=j(E)$ and $J_2=j(E_s)$ are rational functions in s,b,c. We can express the given information in weighted homogeneous polynomial relations in s,b,c with weights $(1,2,3)$ and obtain

$$\begin{aligned} 1728b^3-(b^3+27c^2/4)J_1 &= 0\\ N(b,c,s)-D(b,c,s)J_2 &= 0\\ 3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2 &= 0. \end{aligned}$$

where $N(b,c,s)$ and $D(b,c,s)$ correspond to the numerator and the denominator of the defining equation for $j(E_s)$, as given in Proposition 3.12. When we eliminate b,c,s from these equations, we are left with the classical modular polynomial of level 3 in J_1, J_2. This means that there is a 3-isogeny $\phi\colon E \to E_s$ over $\bar{k}$. Indeed, in the light of Proposition 3.5 we expect to find $(4,4)$-split surfaces of this type that are not Jacobians. A priori, the fact that the j-invariants satisfy a modular polynomial only tells us that E and E_s are 3-isogenous over $\bar{k}$. However, we know that only one twist of E_s has $E_s[4]$ anti-isometric to $E[4]$ and similarly, only one twist of E_s can be 3-isogenous to E. From Proposition 3.5 we know they must coincide.

Furthermore, in general there are only 2 anti-isometries between $E[4]$ and $E_s[4]$ for 3-isogenous curves (otherwise $E[4]$ would have extra automorphisms, requiring the Galois representation to be small). This implies that the anti-isometries induced by our parametrization of $X_E^-(4)$ must coincide with the ones from Proposition 3.5 generally and therefore also for any valid specialization of b,c,s. □

3.5 Proofs of Theorems 3.1 and 3.2

Proof of Theorem 3.1. In Section 3.1 we established that a $(4,4)$-splitting Φ_4 factors as

$$E_1 \times E_2 \xrightarrow{\Phi_2} A \xrightarrow{\Psi} J.$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\quad \underbrace{\qquad\qquad}_{\Phi_4}$$

Let $E_1\colon V^2 = U^3 + bU + C$ be a model for E_1. If A is a Jacobian then Lemma 3.15 provides a model for C_2 such that $A = \mathrm{Jac}(C_2)$ and if J is a Jacobian $\mathrm{Jac}(C_4)$ as well, then Section 3.4 shows that (B.2.1) provides a model for C_4.

More generally, Corollary 3.13 describes that b,c,s together parametrize all J with optimal $(4,4)$-splitting. Proposition 3.16 analyzes all the degeneracies of C_4 and identifies which correspond to the $(4,4)$-splittings described by Propositions 3.7 and 3.17. Together, these give the cases listed in Theorem 3.1. □

Proof of Theorem 3.2. Recall that the moduli space of genus 2 curves is birational to $\mathbb{A}^3$ and that (i_1, i_2, i_3) as given in (3.0.1), give coordinates on that space.

Let $\mathcal{X}$ denote the surface inside $\mathbb{A}^3$ describing genus 2 curves with $(4,4)$-split Jacobians. This surface is the Humbert surface of discriminant 16 and it is irreducible (see [26, Corollaries 1.6-1.8] and [36]).

Theorem 3.1 and Proposition 3.16 show that by specializing b, c, s we can generate points on a Zariski-open part of $\mathcal{X}$. In fact, if we set $b = 1$, the points we can generate still lie dense in $\mathcal{X}$. By computing the Igusa invariants of C_4 we obtain rational functions $i_1(c,s), i_2(c,s), i_3(c,s) \in \mathbb{Q}(c,s)$ such that the image of the rational map

$$\begin{array}{ccc} \mathbb{A}^2 & \dashrightarrow & \mathbb{A}^3 \\ (c,s) & \mapsto & (i_1(c,s), i_2(c,s), i_3(c,s)) \end{array}$$

lies dense in $\mathcal{X}$. The defining equations are too large to compute the image using Gröbner bases or resultants. Instead, we compute the image by interpolation. Our strategy consists of three steps.

1. Determine a candidate equation $\mathcal{L}(i_1, i_2, i_3) = 0$ to describe $\mathcal{X}$,
2. prove that $\mathcal{X}$ is contained in $\mathcal{L}(i_1, i_2, i_3) = 0$,
3. observe that if the Zariski-closure of $\mathcal{X}$ is a proper subset of $\mathcal{L}(i_1, i_2, i_3) = 0$ then $\mathcal{X}$ must lie on a surface of lower degree and derive a contradiction from that.

For (1), we guessed degree bounds with which to interpolate $\mathcal{L}$ and computed a tentative version $\mathcal{L}_{p_i}(i_1, i_2, i_3) \pmod{p_i}$ via interpolation, for 93 consecutive 6-digit primes p_i. For future reference, note that we found a unique solution to the system for each prime p_i.

We then used rational reconstruction to compute a tentative equation $\mathcal{L}(i_1, i_2, i_3) = 0$ over $\mathbb{Q}$. The equation of the surface is too large to reproduce here: $\mathcal{L}$ contains 4574 monomials with coefficients of up to 138 digits. Note that the information we computed should allow us to construct $\mathcal{L} \pmod{N}$, where $N = \prod_{i=1}^{93} p_i \approx 10^{600}$, so the coefficients we found in $\mathcal{L}$ are relatively tiny. This is a strong indicator that we have computed something that indeed has intrinsic meaning over $\mathbb{Q}$ (at this point, basically what could go wrong is that our degree bound is too low and that we have very unluckily picked interpolation points that happen to map to points satisfying some lower degree equation as well).

For (2), we show that $\mathcal{L}(i_1(c,s), i_2(c,s), i_3(c,s))$ is identically zero in $\mathbb{Q}(c,s)$. The expression $\mathcal{L}(i_1(c,s), i_2(c,s), i_3(c,s)) = 0$ gives rise, after clearing denominators, to a polynomial $p(c,s)$ of degrees at most 1800 and 4050 in c and s respectively. We need to establish that $p(c,s) = 0$ as a bivariate polynomial. Expanding $p(c,s)$ explicitly is computationally infeasible, so instead, we evaluate $p(c,s)$ over a large number of distinct values for c and s. For a fixed value $s = s_0$, if we show that $p(c, s_0) = 0$ at 1801 distinct values for c, then $p(c, s_0)$

is the zero polynomial on the line $s = s_0$. If we repeat this process on 4501 distinct lines $s = s_i$ then $p(c, s)$ is in fact the zero polynomial. This calculation was performed in parallel on multiple computers over the course of several weeks.

For (3), note that we have now established that the Zariski-closure of $\mathcal{X}$ is indeed contained in $\mathcal{L}(i_1, i_2, i_3) = 0$. Since $\mathcal{X}$ is irreducible (see [26, Corollary 1.8]), proper containment implies that $\mathcal{X}$ must be described by an equation of strictly lower degree. But then we would have found this lower degree equation in step (1) as well. However, we found there that $\mathcal{L}_{p_i}$ was the unique equation below the guessed degree bounds that interpolated the computed images. So $\mathcal{X}$ does not lie in a lower degree surface. □

Chapter 4

On the visibility of $Ш(E/k)[4]$ in abelian surfaces

4.1 Introduction

In this chapter, we consider an approach to using the $(4,4)$-isogeny $\mathrm{Jac}(C) \to E_1 \times E_2$ to make elements of order 4 of the *Shafarevich-Tate group* of E_1 visible. We begin in this section with an brief introduction to the problem. In Section 4.2, we review Galois cohomology and in Section 4.3, we define the Selmer and Shafarevich-Tate groups. Sections 4.4 and 4.5 cover the general technique we will use to make elements of order m of the Shafarevich-Tate group visible, and review the case $m = 2$. We finally apply the technique to the elements of order 4 in Section 4.6. A sample procedure is presented, along with some specific examples to round out the chapter in Section 4.7.

Let E be an elliptic curve over a number field k. The Mordell-Weil theorem states that the group $E(k)$ is finitely generated. Hence, we can write

$$E(k) = E_{\mathrm{tors}}(k) \times \mathbb{Z}^r$$

where $E_{\mathrm{tors}}(k)$ is finite and r is a non-negative integer, called the *rank* of E.

For any given elliptic curve, one can determine the torsion subgroup, $E_{\mathrm{tors}}(k)$, in the following way. Let $\mathfrak{p}$ be a prime of good reduction for E, unramified in $k/\mathbb{Q}$ and of odd residue characteristic. Then $\#E_{\mathrm{tors}}(k) \mid \#E(k \bmod \mathfrak{p})$. By computing $N_{\mathfrak{p}} = \#E(k \bmod \mathfrak{p})$ for a variety of appropriate $\mathfrak{p}$ (i.e. such that $\#E(k \bmod \mathfrak{p})$ is nonsingular), then $E_{\mathrm{tors}}(k)$ will divide the greatest common divisor of all the $N_{\mathfrak{p}}$. In practice, one does not need to

evaluate $N_{\mathfrak{p}}$ for very many $\mathfrak{p}$ before one gets a modest bound on $\#E_{\text{tors}}(k)$. The actual determination of the torsion points on E is then a matter of determining the rational points on E with x-coordinates that are roots of the relevant division polynomials. See Silverman [45, Section VII.3] for a more detailed discussion on determining $E_{\text{tors}}(k)$.

The rank, on the other hand, is difficult to effectively compute. In this chapter, we deal with a question related to the problem of determining the rank of an elliptic curve E over a number field k.

One approach to computing the rank of E is to try and compute the group $E(k)/mE(k)$ for some positive integer m. Since the torsion subgroup can be determined, we would then be able to determine the rank of $E(k)$ from the order of $E(k)/mE(k)$. We find that the order of $E(k)/mE(k)$ is not easy to determine. We can, however, approximate $E(k)/mE(k)$ by an effectively computable object called the *m-Selmer group*, $S^{(m)}(E/k)$. Since $\#E(k)/mE(k) \leq \#S^{(m)}(E/k)$, the Selmer group can provide an upper bound on the rank of $E(k)$.

Unfortunately, the failure of the local-to-global principle may prevent the bound obtained from the m-Selmer group from being sharp. The m-torsion of the *Shafarevich-Tate group*, Ш$(E/k)[m]$ measures the discrepancy, and can be defined by the exact sequence

$$0 \longrightarrow E(k)/mE(k) \longrightarrow S^{(m)}(E/k) \longrightarrow Ш(E/k)[m] \longrightarrow 0. \tag{4.1.1}$$

See Section 4.3 for a review of the Selmer and Shafarevich-Tate groups, including full definitions of each group.

Let $\delta \in S^{(m)}(E/k)$. If δ comes from an element in $E(k)/mE(k)$ then one can demonstrate this by finding a point $P \in E(k)$ which maps to δ. Since P is of finite height, this process can be completed in finite time. However, as there is no bound on the lowest height of a point $P \in E(k)$ which maps to such a $\delta \in S^{(m)}(E/k)$, the failure to find P does not show that δ represents a non-trivial element of Ш$(E/k)[m]$.

One can use isogenies between elliptic curves to try to refine the bounds on $\#E(k)/mE(k)$ and possibly decide whether a given $\delta \in S^{(m)}(E/k)$ represents a non-trivial element of Ш$(E/k)[m]$. If E_1 and E_2 are isogenous elliptic curves, then $\text{rk}(E_1(k)) = \text{rk}(E_2(k))$ where $\text{rk}(E_i)$ denotes the rank of E_i for $i = 1, 2$. It may happen that $\#Ш(E_1/k)[m] \neq \#Ш(E_2/k)[m]$, in which case $\text{rk}(E_1(k))$ would have distinct bounds from $S^{(m)}(E_1/k)$ and $S^{(m)}(E_2/k)$ respectively. In particular, one has the usual rank bound on E_1 given by

$$m^{\text{rk}(E_1(k))} \#\big(E_{1,\text{tors}}(k)/mE_{1,\text{tors}}(k)\big) \leq \#S^{(m)}(E_1/k).$$

Now suppose that $\#Ш(E_1/k)[m] < \#Ш(E_2/k)[m]$. Then

$$\frac{\#S^{(m)}(E_1/k)}{\#\big(E_{1,\mathrm{tors}}(k)/mE_{1,\mathrm{tors}}(k)\big)} < \frac{\#S^{(m)}(E_2)}{\#\big(E_{2,\mathrm{tors}}(k)/mE_{2,\mathrm{tors}}(k)\big)}.$$

These quantities provide upper bounds on $m^{\mathrm{rk}(E_1(k))}$ (respectively $m^{\mathrm{rk}(E_2(k))}$) which may be better rank bounds than the bound obtained by the usual approach mentioned above.

We can adapt the above technique to isogenies between abelian varieties. Let A and B be two abelian varieties such that the product $A \times B$ has a isogeny to an abelian variety J. Then

$$\mathrm{rk}\, J(k) = \mathrm{rk}\,(A \times B)(k) = \mathrm{rk}\, A(k) + \mathrm{rk}\, B(k). \tag{4.1.2}$$

We may be able to conclude that $Ш((A \times B)/k)[m] = Ш(A/k)[m] \times Ш(B/k)[m]$ is non-trivial. If an additional argument allows us to exhibit that $\#Ш(B/k)[m] = 1$, we can conclude that $Ш(A/k)[m]$ is non-trivial.

This last technique for finding non-trivial elements of $Ш(A/k)[m]$ is called *visualization* and originates from Mazur [16]. It refers to the fact that the homogenous spaces representing the visible elements of $S^{(m)}(A/k)$ occur as fibres of the map $J \to B$.

Definition 4.1. Let $0 \to A \to J \to B \to 0$ be a short exact sequence of abelian varieties. The *visible subgroup* of $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), A)$ is obtained by taking Galois cohomology, and is defined as $\mathrm{Vis}_k(A \to J)$ in the induced long exact sequence

$$0 \longrightarrow \mathrm{Vis}_k(A \to J) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k})) \xrightarrow{\phi} \mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), J(\bar{k})) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), B(\bar{k})).$$

See Section 4.2 for a review of Galois cohomology. Note that elements of $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), A)$ are actually equivalence classes of elements. For $\delta \in S^{(m)}(A/k)$, one can only prove that the class $\bar{\delta}$ of δ in $Ш(A/k)[m]$ is nontrivial via comparison with $S^{(m)}(J/k)$ if $\bar{\delta} \in \mathrm{Vis}_k(A \to J)$. In that case, we will say that δ is *visible* in J.

In this chapter, we consider the case where A and B are elliptic curves, J is the Jacobian of a genus 2 curve and where $m = 4$. A number of other papers have considered this problem for different m; see [6, 7] for $m = 2$ and [5, 31] for $m = 3$.

4.2 Review of Galois cohomology

For full texts on Galois cohomology, see Serre [41], or Ribes [38]. We follow a more abbreviated introduction as given in Silverman [45, Appendix B].

Definition 4.2. A *(discrete)* $\mathrm{Gal}(\bar{k}/k)$*-module* is an abelian group M on which $\mathrm{Gal}(\bar{k}/k)$ acts such that for all $m \in M$, the stabilizer of m is a subgroup of finite index.

An example of a Galois module has already played a prominent role throughout the thesis. Consider the Jacobian $\mathrm{Jac}(C/k)$ of a curve C over a field k. Then $\mathrm{Jac}(C)$ is certainly an abelian group on which $\mathrm{Gal}(\bar{k}/k)$ acts. We need only show that any point $P \in \mathrm{Jac}(C)$ is rational in some finite extension of k. Consider a projective model of $\mathrm{Jac}(C)$ and fix a representative of the divisor class P. Then that representative is a linear combination of a finite set of points $P_0, \ldots P_j \in C$. But for any $x \in \bar{k}$, the extension $k(x)/k$ is finite. Therefore, in particular, one can find a finite extension L of k over which the coordinates of each of $P_0, \ldots, P_j$ are rational, and hence a Jacobian can be viewed as a $\mathrm{Gal}(\bar{k}/k)$-module.

More generally, the above argument shows that any principally polarized abelian variety is in fact a $\mathrm{Gal}(\bar{k}/k)$-module over its base field k.

Definition 4.3. The 0^{th}*-cohomology group* of the $\mathrm{Gal}(\bar{k}/k)$-module M is the group of $\mathrm{Gal}(\bar{k}/k)$-invariant elements of M and is written $\mathrm{H}^0(\mathrm{Gal}(\bar{k}/k), M)$.

Let M be a $\mathrm{Gal}(\bar{k}/k)$-module. We say that a map $\xi : \mathrm{Gal}(\bar{k}/k) \to M$ is *continuous* if for every $m \in M$, $\xi^{-1}(m)$ contains a subgroup of finite index of $\mathrm{Gal}(\bar{k}/k)$ (that is to say, it is continuous with respect to the discrete topology on M and the profinite topology on $\mathrm{Gal}(\bar{k}/k)$).

Definition 4.4. Let M be a $\mathrm{Gal}(\bar{k}/k)$-module. The group of *continuous* 1*-cocycles* from $\mathrm{Gal}(\bar{k}/k)$ to M is the group of continuous maps $\xi : \mathrm{Gal}(\bar{k}/k) \to M$ satisfying the cocycle condition

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau.$$

We write $Z^1(\mathrm{Gal}(\bar{k}/k), M)$ for the group of continuous 1-cocycles from $\mathrm{Gal}(\bar{k}/k)$ to M. The group of 1*-coboundaries* from $\mathrm{Gal}(\bar{k}/k)$ to M is the group of continuous maps ξ for which there exists an $m \in M$ such that

$$\xi_\sigma = m^\sigma - m \text{ for all } \sigma \in \mathrm{Gal}(\bar{k}/k).$$

We write $B^1(\mathrm{Gal}(\bar{k}/k)$ for the group of continuous 1-coboundaries from $\mathrm{Gal}(\bar{k}/k)$ to M.

Notice that every 1-coboundary is a 1-cocycle. Note also that the restriction to continuous maps in the definition of coboundaries is superfluous as a map $\sigma \to m^\sigma - m$ will automatically be continuous when M is viewed as having the discrete topology.

Definition 4.5. The 1^{st}*-cohomology group* of the $\mathrm{Gal}(\bar{k}/k)$-module M is defined by

$$\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), M) := \mathrm{Z}^1(\mathrm{Gal}(\bar{k}/k), M)/\,\mathrm{B}^1(\mathrm{Gal}(\bar{k}/k), M).$$

So an element of the 1-cohomology group of the $\mathrm{Gal}(\bar{k}/k)$-module M is actually a class of cocycles, modulo coboundaries. We will often write a cocycle ξ as a representative of a given class.

Notation. As we will be working exclusively with Galois cohomology, we will apply the usual abbreviated notation. For the remainder of the thesis, we write $\mathrm{H}^0(k, A)$ and $\mathrm{H}^1(k, A)$ for $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k}))$ and $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k}))$ respectively.

We conclude with a useful result in Galois cohomology (see Silverman [45, Proposition B.2.3]).

Proposition 4.6. *Let*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

be a short exact sequence of $\mathrm{Gal}(\bar{k}/k)$*-modules. Then there is a long exact sequence*

$$0 \longrightarrow \mathrm{H}^0(k, P) \longrightarrow \mathrm{H}^0(k, M) \longrightarrow \mathrm{H}^0(k, N) \xrightarrow{\alpha} \mathrm{H}^1(k, P) \longrightarrow \mathrm{H}^1(k, M) \longrightarrow \mathrm{H}^1(k, N),$$

where the connecting homomorphism α *is defined as follows.*

Let $n \in \mathrm{H}^0(k, N)$ *and let* $m \in M$ *such that* $\psi(m) = n$*. Define a map* $\xi : \mathrm{Gal}(\bar{k}/k) \to M$ *by*

$$\xi_\sigma = m^\sigma - m.$$

Then $\xi \in Z^1(k, P)$*, and* $\alpha(n)$ *is the cohomology class in* $\mathrm{H}^1(k, P)$ *of the* 1*-cocycle* ξ*.*

Now suppose M is a $\mathrm{Gal}(\bar{k}/k)$-module and let L/k be a finite Galois extension. Then $\mathrm{Gal}(\bar{k}/L) \subset \mathrm{Gal}(\bar{k}/k)$ is a subgroup of finite index and so M is naturally a $\mathrm{Gal}(\bar{k}/L)$-module. This leads to a *restriction map* $\mathrm{H}^1(k, M) \to \mathrm{H}^1(L, M)$.

4.3 Review of the Selmer and Shafarevich-Tate groups

In this section, we briefly review the Selmer and Shafarevich-Tate groups. See also Silverman [45, Section X.4].

Let E and E' be elliptic curves over a number field k and let $\phi : E \to E'$ be an isogeny defined over k. Then there is a short exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

where $E[\phi]$ denotes the kernel of ϕ. Using Proposition 4.6, we take Galois cohomology on this short exact sequence to obtain the long exact sequence

$$0 \longrightarrow E(k)[\phi] \longrightarrow E(k) \xrightarrow{\phi} E'(k) \longrightarrow \mathrm{H}^1(k, E[\phi]) \longrightarrow \mathrm{H}^1(k, E) \xrightarrow{\phi} \mathrm{H}^1(k, E') \longrightarrow \dots$$

from which we get the fundamental exact sequence

$$0 \longrightarrow E(k)/\phi E(k) \longrightarrow \mathrm{H}^1(k, E[\phi]) \longrightarrow \mathrm{H}^1(k, E)[\phi] \longrightarrow 0. \tag{4.3.1}$$

Our goal is to compute $E(k)/mE(k)$. To this end, we can take ϕ to be the multiplication by m isogeny $[m] : E \to E$, in which case (4.3.1) becomes

$$0 \longrightarrow E(k)/mE(k) \longrightarrow \mathrm{H}^1(k, E[m]) \longrightarrow \mathrm{H}^1(k, E)[m] \longrightarrow 0. \tag{4.3.2}$$

By the Mordell-Weil theorem, we have

$$\#E(k)/mE(k) = m^r \cdot \#(E_{\mathrm{tors}}(k)/mE_{\mathrm{tors}}(k)).$$

The torsion subgroup is effectively and often practically computable, so if we are able to compute the kernel of $\mathrm{H}^1(k, E[m]) \to \mathrm{H}^1(k, E)[m]$ then we would be able to determine the rank of E directly from $E(k)/mE(k)$. Unfortunately, there is no known method to compute this kernel.

We can, however, obtain an approximation of the kernel by using local considerations. Let p be a (finite or infinite) prime of k and fix an extension of the p-adic absolute value $|\cdot|_p$ to $\bar{k}$. This gives us an embedding $\bar{k} \to \bar{k}_p$ which in turn gives us a decomposition group $\mathrm{Gal}(\bar{k}_p/k_p) \subset \mathrm{Gal}(\bar{k}/k)$ (see Neukirch [37, Section II.9] for a discussion on Galois theory of valuations). By using the natural inclusion maps $\mathrm{Gal}(\bar{k}_p/k_p) \hookrightarrow \mathrm{Gal}(\bar{k}/k)$ and $E(\bar{k}) \hookrightarrow E(\bar{k}_p)$, we can obtain a restriction map $\mathrm{H}^1(k, E) \to \mathrm{H}^1(k_p, E)$.

Definition 4.7. The *m-Selmer group* of E/k is the subgroup of $\mathrm{H}^1(k, E)$ defined by

$$S^{(m)}(E/k) = \ker\left(\mathrm{H}^1(k, E[m]) \to \prod_p \mathrm{H}^1(k_p, E)\right)$$

where the product is taken over all primes p of k (taken over the finite and the infinite places). The *Shafarevich-Tate group* of E/k is defined by

$$Ш(E/k) = \ker\left(\mathrm{H}^1(k, E) \to \prod_p \mathrm{H}^1(k_p, E) \right)$$

where the product is taken over all primes p of k (both finite and infinite).

The Selmer group is in principle effectively computable and $E(k)/mE(k)$ injects into $S^{(m)}(E/k)$, giving us an effective upper bound for the rank of E. The obstruction to this bound being sharp is due to the 1-cocycles which restrict to coboundaries everywhere locally. This obstruction is the Shafarevich-Tate group. Both groups fit in the exact sequence (4.1.1) which is the local analogue of the exact sequence given in (4.3.2).

4.4 Visibility of $Ш(E/k)[m]$ in abelian surfaces

In this section, we review a technique to construct abelian surfaces J in which $\delta \in Ш(E/k)[m]$ is visible. See also [5, Section 3], [6], [7], [16], and [31].

Let $m > 1$ be an integer and k be a number field. Let E_1 and E_2 be elliptic curves over k and let $\lambda : (E_1/k)[m] \to (E_2/k)[m]$ be an isomorphism of k-group schemes. Let $\Delta \subset E_1 \times E_2$ be the graph of $-\lambda$ so that

$$\Delta(\bar{k}) = \left\{ (P, -\lambda(P) \mid P \in E_1[m](\bar{k}) \right\} \tag{4.4.1}$$

and let $A := (E_1 \times E_2)/\Delta$. Then A is a non-simple Abelian surface over k and fits in the exact sequence

$$0 \longrightarrow \Delta \longrightarrow E_1 \times E_2 \longrightarrow A \longrightarrow 0.$$

Now suppose $\xi \in Ш(E_1/k)[m] \subset \mathrm{H}^1(k, E_1)$. Then ξ is the class of an element $\delta \in \mathrm{H}^1(k, E_1[m])$. If $\lambda(\delta) \in \mathrm{H}^1(k, E_2[m])$ maps to zero in $\mathrm{H}^1(k, E_2)$ under the homomorphism induced from the inclusion $E_2[m] \hookrightarrow E_2$, then ξ is visible in E_2. Cremona and Mazur [31] first made this observation (in their paper, combine Remark 3 and subsequent proposition with the discussion on page 19 of their paper). Mazur also cites this result at the beginning of Section 2 in [31]. We summarize it here in the form that it appeared in Bruin [7, Corollary 3.4]

Proposition 4.8 (Cremona-Mazur)**.** *A class $\delta \in \mathrm{H}^1(k, E_1)$ vanishes in $\mathrm{H}^1(k, A)$ precisely if δ is in the image of $\varphi : E_2(k) \to \mathrm{H}^1(k, \Delta)$.*

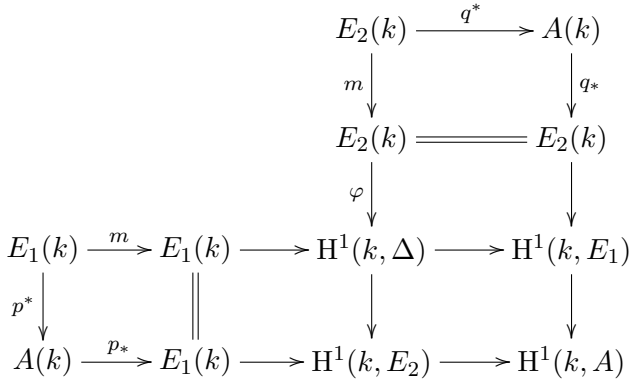


Figure 4.1: Commutative diagram with exact rows and columns. See Bruin [7, p. 1468].

If we further assume that A is a principally polarized abelian surface, then we can put all the information into a concise commutative diagram. We have injections $p^* : E_1 \to A$ and $q^* : E_2 \to A$ induced by $P \mapsto (P, O_{E_2}) \in E_1 \times E_2$ and $Q \mapsto (O_{E_1}, Q) \in E_1 \times E_2$ respectively. Since $\Delta \subset (E_1 \times E_2)[m]$, the multiplication-by-$m$ map on $E_1 \times E_2$ factors through A. This factorization map induces the maps $p_* : A \to E_1 \times E_2 \to E_1$ and $q_* : A \to E_1 \times E_2 \to E_2$. Note that $p_* \circ p^* = m|_{E_1}$ and $q_* \circ q^* = m|_{E_2}$.

We will consider when the Selmer group $S^{(m)}(A/k)$ leads to a sharper rank bound on E_1 than the bound found by taking an m-descent on E_1. In particular, the question arises as to when we might expect this improvement to occur. Suppose $\delta \in \mathrm{H}^1(k, \Delta)$ has a nontrivial image under $\mathrm{H}^1(k, \Delta) \to \mathrm{H}^1(k, E_1)$, but which is trivial in $\mathrm{H}^1(k_p, E_1)$ for any place p of k. We can combine Galois cohomology of the short exact sequences

$$0 \to E_1 \xrightarrow{p^*} A \xrightarrow{q_*} E_2 \to 0,$$
$$0 \to E_2 \xrightarrow{q^*} A \xrightarrow{p_*} E_1 \to 0, \text{ and}$$
$$0 \to E_i[m] \to E_i \xrightarrow{m} E_i \to 0 \text{ for } i = 1, 2$$

to obtain the commutative diagram in Figure 4.1. Note that $\mathrm{H}^1(k, \Delta) \cong \mathrm{H}^1(k, E_1[m]) \cong \mathrm{H}^1(k, E_2[m])$. If δ does not vanish in $\mathrm{H}^1(k, A)$, then it leads to a nontrivial element in

$$Ш(A/k)[p_* \times q_*] \subset Ш(A/k)[m].$$

This suggests that if we do ensure that δ vanishes in $\mathrm{H}^1(k, A)$, then we remove a reason for $Ш(A/k)[m]$ to be non-trivial. This opens the possibility for $S^{(m)}(A/k)$ providing a sharper bound on $\mathrm{rk}(A(k))$ than the one we obtain from an m-descent on $E_1 \times E_2$.

4.4.1 Unramified coverings of E

In light of the general visibility technique which we just outlined, it would be useful to have some means of interpreting elements of the group $\mathrm{H}^1(k, E_1[m])$. Cremona et al [14] collect several such interpretations for that group. One of these interpretations will be particularly useful for our construction.

Definition 4.9. Let C be a smooth projective curve and let $\pi : C \to E_1$ be an unramified covering over k that is Galois and irreducible over $\bar{k}$. Then (C, π) is a *covering* of E_1 and we say that C is a *cover* of E_1.

We also write $\pi : C \to E$ for the covering (C, π). An isomorphism of coverings $(C_1, \pi_1) \cong (C_2, \pi_2)$ is an isomorphism of curves $\phi : C_1 \to C_2$ over k with $\pi_1 = \pi_2 \circ \phi$.

Definition 4.10. An *m-covering* (C, π) is a covering that is isomorphic to $(E, [m])$ over $\bar{k}$.

A *twist* D of a curve C is a curve which is isomorphic to C over $\bar{k}$. So an m-covering (C, π) is a twist of $(E, [m])$. The m-covering $[m] : E \to E$ is called the *trivial m-covering* of E.

Proposition 4.11 ([14, Proposition 1.14])**.** *The m-covers are in bijective correspondence to classes in* $\mathrm{H}^1(k, E[m])$.

Proof. To show the m-coverings of E are parametrized up to isomorphism by $\mathrm{H}^1(k, E[m])$, see [14, Proposition 1.14]. For the converse, consider an elliptic curve E/k and an m-cover $\pi : C \to E$. We know that $\pi : C \to E$ is a twist of the trivial m-covering $[m] : E \to E$, so there exists an isomorphism $\phi : C \to E$ over $\bar{k}$ such that $\pi = [m]\,\phi$.

Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Then σ will act on ϕ such that $\phi^\sigma \phi^{-1}$ is an automorphism of E satisfying

$$[m] = [m]\,\phi^\sigma\,\phi^{-1}. \tag{4.4.2}$$

Therefore $\phi^\sigma \phi^{-1}$ is a translation by an m-torsion point. Let $\mathcal{T}$ denote the group of translation maps on E and define the map $\xi : \mathrm{Gal}(\bar{k}/k) \to \mathcal{T}$ by

$$\begin{aligned} \xi_\sigma &= \phi^\sigma \phi^{-1}(O_E) \\ &= (O_E \mapsto O_E + T_\sigma = T_\sigma) \qquad \text{for some } T_\sigma \in E[m]. \end{aligned}$$

Let $\sigma, \tau \in \mathrm{Gal}(\bar{k}/k)$. Then we have

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1}(O_E) = \phi^{\sigma\tau}\left(\phi^{-1}\right)^\tau \phi^\tau \phi^{-1}(O_E) = \left(\phi^\sigma \psi^{-1}\right)^\tau \phi^\tau \phi^{-1}(O_E) = \xi_\sigma^\tau \xi_\tau$$

and so ξ is a continuous 1-cocycle by Definition 4.4. Now suppose $\pi_2 : D \to E$ is another cover of E that is isomorphic to $\pi : C \to E$. Then there exists an isomorphism $\psi : D \to E$ over $\bar{k}$ satisfying $\pi_2 = [m]\,\phi$. We can trace through (4.4.2) again to conclude that the map $\zeta : \mathrm{Gal}(\bar{k}/k) \to \mathcal{T}$ given by

$$\zeta_\sigma = \psi^\sigma \psi^{-1}(O_E)$$

is also a translation by an m-torsion point map. Thus isomorphic m-covers may differ by a composition with a translation-by-m-map. In fact, this is only a change by a coboundary. To see this, recall that (D, π_2) and (C, π) being isomorphic implies that there exists a k-rational isomorphism $\theta : C \to D$. Consider the element $m = \psi\,\theta\,\phi^{-1} \in \mathcal{T}$. Then for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, we have

$$\begin{aligned} m^\sigma \xi_\sigma = m^\sigma \left(\phi^\sigma \phi^{-1}\right) &= (\psi\,\theta\,\phi^{-1})^\sigma \phi^\sigma \phi^{-1} \\ &= \psi^\sigma \theta^\sigma \left(\phi^{-1}\right)^\sigma \phi^\sigma \phi^{-1} \\ &= \psi^\sigma \theta \phi^{-1} \\ &= \psi^\sigma \left(\psi^{-1}\psi\right) \theta \phi^{-1} \\ &= \left(\psi^\sigma \psi^{-1}\right)\left(\psi\,\theta\,\phi^{-1}\right) = \zeta^\sigma m \end{aligned}$$

Therefore ζ and ξ differ by a coboundary. We conclude that an m-cover determines a class in $\mathrm{H}^1(k, E[m])$. Therefore m-covers are in bijective correspondence to classes in $\mathrm{H}^1(k, E[m])$. □

Lemma 4.12. *Suppose E_1 and E_2 are two elliptic curves over k with a k-group scheme isomorphism $\lambda : E_1[m] \to E_2[m]$. Suppose two m-covers*

$$\pi_1 : C_1 \to E_1 \qquad \text{and} \qquad \pi_2 : C_2 \to E_2$$

represent the same class in $\mathrm{H}^1(k, E_1[m]) \cong \mathrm{H}^1(k, E_2[m])$. Then $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ are isomorphic as k-schemes.

Proof. For $i = 1$ or 2, we know that C_i is trivial if $\pi_1^{-1}(O_{E_i})$ has a rational point. Therefore, if C_1 and C_2 represent the same class, then $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ must acquire points over the same extensions of k. However, note that the coordinate ring of $\pi_1^{-1}(O_{E_1})$ is an étale k-algebra and that the constituent fields are exactly the extensions of k over which $\pi_1^{-1}(O_{E_1})$ acquires a point. This shows that the coordinate rings of $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ have the same constituents and hence are isomorphic. □

The converse of Lemma 4.12, is not true. Over a trivializing extension L/k, we know that $\pi_1^{-1}(O_{E_1})$ is isomorphic to $E_1[m]$. As a finite étale algebra, $E_1[m]$ can have extra automorphisms, that is to say, automorphisms other than the translation-by-T maps used in the proof of Proposition 4.11. These extra automorphisms can change the cocycle class ξ (they no longer differ by a coboundary) without changing the extensions over which ξ trivializes. For example, for $\xi \in \mathrm{H}^1(k, E[3])$, we have that ξ and 2ξ are different cohomology classes, but of course both trivialize over exactly the same extensions. So the 0-fibers of their corresponding covers are isomorphic.

We can however, prove a weaker lemma by adding in an extra assumption on the number of automorphisms of $E_1[m]$. This lemma will suffice for our needs.

Lemma 4.13. *Suppose E_1 and E_2 are two elliptic curves over k with a k-group scheme isomorphism $\lambda : E_1[m] \to E_2[m]$. Let*

$$\pi_1 : C_1 \to E_1 \qquad \text{and} \qquad \pi_2 : C_2 \to E_2$$

be two m-covers such that $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ are isomorphic as k-schemes. Let ξ_1 and ξ_2 be the two cocycle classes in $\mathrm{H}^1(k, E_1[m]) \cong \mathrm{H}^1(k, E_2[m])$ corresponding to (C_1, π_1) and (C_2, π_2) respectively. Let L be a field extension of k such that $\pi_1^{-1}(O_{E_1})(L)$ is non-empty. Suppose

$$\#\operatorname{Aut}_k(\pi_1^{-1}(O_{E_1})) = 1 \qquad \text{and} \qquad \#\operatorname{Aut}_L(E_1[m]) = \#(\mathbb{Z}/m\mathbb{Z})^* \cdot \#E_1[m](L).$$

Then $\xi_1 = n\xi_2$ for some $n \in \mathbb{N}$ with $\gcd(n, m) = 1$.

Proof. Since (C_1, π_1) and (C_2, π_2) are twists of $(E_1, [m])$ and $(E_2, [m])$ respectively, there exist isomorphisms $\phi_1 : C_1 \to E_1$ and $\phi_2 : C_2 \to E_2$ such that $\pi_1 = [m]\,\phi_1$ and $\pi_2 = [m]\,\phi_2$ respectively.

We know that C_1 is trivial if $\pi_1^{-1}(O_{E_1})$ has a rational point. Since $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ are isomorphic as k-schemes, they will trivialize over the same extensions. Let L be an extension over which both trivialize (a factor of the coordinate ring of $\pi_1^{-1}(O_{E_1})$ would do). Then over L, we have that $\pi_1^{-1}(O_{E_1})$ is isomorphic to $E_1[m]$.

In the proof of Lemma 4.11, we first showed that if an automorphism satisfies the cocycle condition, then it is a translation map. We then proved that different translation maps will cause the corresponding cocycles to differ by a coboundary, and hence will represent the same class. Following the same argument here, we conclude that a k-rational isomorphism

$$\alpha : \pi_1^{-1}(O_{E_1}) \to \pi_2^{-1}(O_{E_2}).$$

will be evidence of C and D being isomorphic (i.e. representing the same cocycle class) if and only if the composition

$$\lambda^{-1}\,\phi_2\,\alpha\,\phi_1^{-1} \tag{4.4.3}$$

is a translation map. Note that we can assume ϕ_1 and ϕ_2 are defined over L.

Tracing through the compositions, we see that (4.4.3) denotes an L-rational automorphism of $E_1[m]$ (as a finite étale L-scheme). There are at most $(m^2)!$ automorphisms on $E_1[m]$ defined over L (if $E_1[m]$ splits over L, then any permutation of the m^2 points would be an automorphism defined over L). For each element $a \in E_1[m](L)$, there is an L-rational automorphism corresponding to the translation map, T_a, by the element a. That means there are $\#\operatorname{Aut}_L(E_1[m])/\#E_1[m](L)$ automorphisms which do not correspond to a translation map on $E_1[m](L)$, and hence which will affect the corresponding cocycles.

Since $\#\operatorname{Aut}_L(E_1[m]) = \#(\mathbb{Z}/m\mathbb{Z})^* \cdot \#E_1[m](L)$, we are restricting to the case where the automorphisms on $E_1[m]$ defined over L are compositions of a multiplication-by-m map by a translation-by-a map. This means that the automorphism in (4.4.3) is a multiplication map composed with translation and hence $\xi_1 = n\xi_2$ for some n with $\gcd(n, m) = 1$. □

Over $\bar{k}$, all m-coverings are isomorphic to the trivial m-covering, the multiplication-by-m map $[m] : E \to E$. For $\delta \in \mathrm{H}^1(k, E_1[m])$, we let C_δ denote the m-cover corresponding to δ. Combining Propositions 4.8 and 4.11, we see $\delta \in \mathrm{H}^1(k, E_1[m])$ is visible in A when there is some automorphism such that $C_{\lambda(\delta)}$ corresponding to $\lambda(\delta) \in \mathrm{H}^1(k, E_2[m])$ has a rational point. By our work proving of Lemma 4.13, we know that different automorphisms α_1 and α_2 on the m-torsion of E_1 may lead to different covers $C_{1,\lambda(\delta)}$ and $C_{2,\lambda(\delta)}$ of E_2. For visibility to occur, it suffices that one of those covers have a rational point.

In the case where $m = 4$, there is one possible non-translation automorphism on the 4-torsion, so we see $\delta \in \mathrm{H}^1(k, E_1[4])$ is visible in A when one of $C_{\lambda(\delta)}$ or $C_{-\lambda(\delta)}$ has a rational point.

So given an elliptic curve E_1 over k, let $\delta \in \mathrm{H}^1(k, E_1[m])$ be a cocycle class which we suspect may map to a nontrivial element of $Ш(E/k)[m]$. Search through all elliptic curves E_2 for which we can find a k-group scheme isomorphism $\lambda : E_1[m] \to E_2[m]$. If the m-cover $C_{\lambda(\delta)}$ has a rational point in one of these cases, then δ is visible in $A = (E_1 \times E_1)/\Delta$.

4.4.2 Polarization of A

Note that $E_1 \times E_2$ is principally polarized via the product polarization. As already noted, $E_1 \times E_2$ inherits a Weil pairing, corresponding to the product pairing. By Proposition 1.71, we know that our choice of E_2 and λ can influence the resulting Weil pairing on $E_1 \times E_2$ and hence on the restriction $A \cong (E_1 \times E_2)/\Delta$.

One may be interested in insisting that A be principally polarized over $\bar{k}$. One way for this to happen is for the isogeny $p^* + q^* : E_1 \times E_2 \to A$ to give rise to a principal polarization. This would be the case if the kernel Δ is a maximal isotropic subgroup of $E_1[m] \times E_2[m]$ with respect to the Weil pairing. This will occur when

$$(\lambda(P), \lambda(Q))_{E_2} = (P, Q)_{E_1}^{-1},$$

that is to say, when $\lambda : E_1[m] \to E_2[m]$ is an anti-isometry. By Proposition 1.71, we know that if $(P, Q)_{E_1}$ is a primitive n-th root of unity, then $(\lambda(P), \lambda(Q))_{E_2}$ will be as well.

In the case $m = 2$, there is only one primitive 2nd root of unity, ζ_2, and as such, there will be a unique way for λ to act on the Weil pairing. In particular, since $\zeta_2 = \zeta_2^{-1}$, the isomorphism $\lambda : E_1[m] \to E_2[m]$ will simultaneously be an isometry and an anti-isometry, and so the surface A will always be principally polarized over $\bar{k}$.

For larger m, the group $\mathbb{Z}/m\mathbb{Z}$ will have more than one primitive root of unity. If $(P, Q)_{E_1}$ is a primitive m-th root of unity, then $(\lambda(P), \lambda(Q))_{E_2}$ could conceivable be any of the primitive m-th roots of unity. Only in the case where $(\lambda(P), \lambda(Q))_{E_2} = (P, Q)_{E_1}^{-1}$ would we obtain a principally polarized abelian variety.

For the case $m = 4$, there are two primitive 4-th roots of unity. Therefore, there are two options: either λ is an isometry (i.e. $\zeta_4 \mapsto \zeta_4$) or it is an anti-isometry (i.e. $\zeta_4 \mapsto \zeta_4^{-1}$). Only the anti-isometric case gives rise to A being principally polarized. Nevertheless, we analyze both cases in Section 4.6.

4.5 A review of visibility in the case $m = 2$

When we analyze the case $m = 4$ in Section 4.6, we find that it will be closely related to the $m = 2$ case. To this end, we briefly review the visibility argument for $m = 2$. The details can be found in [7].

Let E be an elliptic curve over a number field k and let $v_1^2 = f(u)$ be a model for E. Let E_2 be an elliptic curve with 2-torsion isomorphic to the 2-torsion of E. By Lemma 1.75,

there exist parameters $a \in k \cup \{\infty\}$ with $f(a) \neq 0$ and $d \in k^\times$ such that E_2 has a model

$$E_2 : \begin{cases} v_2^2 = -df(u) & \text{if } a = \infty \\ v_2^2 = d(u-a)f(u) & \text{otherwise.} \end{cases}$$

Let $L = k(\theta) = k[t]/(f(t))$ and let $N_{L/k}$ denote the norm map on L over k; by abuse of notation, we also write $N_{L/k}$ as the norm map of $L[u]$ over $k[u]$ as the presence of u would make it clear in each instance.

Now let $\delta \in \mathrm{H}^1(k, E)$. For a given $P \in E(k)$, we have

$$f(u) = N_{A/k}(u(P) - \theta).$$

If $N_{L/k}(P) = \delta$, then we can find $u_0, u_1, u_2 \in k$ such that

$$\begin{aligned} u(P) - \theta &= \delta(u_0 + u_1\theta + u_2\theta^2)^2 \\ &= Q_{0,\delta}(\mathbf{u}) + Q_{1,\delta}(\mathbf{u})\theta + Q_{2,\delta}(\mathbf{u})\theta^2 \end{aligned} \tag{4.5.1}$$

where $N_{L/k}(\delta) = \square$ and $Q_{i,\delta}$ are quadratic forms in $\mathbf{u} = (u_0, u_1, u_2)$.

Regardless of whether we can find $P \in E(k)$ such that $N_{L/k}(P) = \delta$, we can use the quadratic forms in (4.5.1) to define a projective variety over k. Let C_δ be given by

$$C_\delta : \begin{cases} Q_{2,\delta}(\mathbf{u}) = 0 \\ Q_{1,\delta}(\mathbf{u}) = -y_1^2. \end{cases}$$

Then C_δ is a 2-cover of E_1 and can be obtained by taking the fibre product over the u-line of E_1 with a projective variety given by $Q_{2,\delta}(\mathbf{u}) = 0$. If the latter variety has no k-rational point, then C_δ will have no k-rational points. Similarly, if we try to construct a 2-cover $C_{2,\delta}$ of E_2 by taking the fibre product over the u-line of E_2 with $Q_{2,\delta}(\mathbf{u}) = 0$, again we find that $C_{2,\delta}$ will have no k-rational points and we need not proceed further.

Otherwise, the projective variety $Q_{2,\delta}(\mathbf{u}) = 0$ has a rational point, and so it is a $\mathbb{P}^1$. In this case, we can fix a parametrization $x \mapsto \mathbf{u}(x)$ and write $\mathbb{P}^1_x$ for this variety. With this parametrization

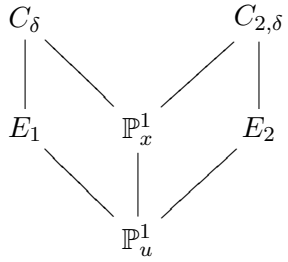
$$C_\delta : y_1^2 = -Q_{1,\delta}(\mathbf{u}(x)) = g(x)$$

where $g(x)$ is a quartic in x.

In an identical manner, we can find a 2-cover $C_{2,\delta}$ of E_2 by taking the fibre product of E_2 with a $\mathbb{P}^1$. If we insist that the fibre product is taken with $\mathbb{P}^1_x$, then we find

$$C_{2,\delta} : y_2^2 = d\left(Q_{0,\delta}(\mathbf{u}(x)) + aQ_{1,\delta}(\mathbf{u}(x))\right)$$

and all the curves fit into the following diagram:



Proposition 4.14 ([7, Theorem 1.1])**.** *Let E_1 be an elliptic curve over a number field k and let $\delta \in \mathrm{H}^1(k, E_1[2])$ map to a non-trivial element $\xi \in Ш(E_1/k)[2]$. Then there are infinitely many elliptic curves E_2 for which ξ is made visible in $A := (E_1 \times E_2)/\Delta$, where Δ is defined in* (4.4.1)*.*

Bruin [7] proves Proposition 4.14 by showing that for any $a \in k$ where $f(a) \neq 0$, one can find an appropriate $d \in k$ for which the 2-cover $C_{2,\delta}$ of the elliptic curve $E_2 : v_2^2 = d(u-a)f(u)$ will have a rational point.

4.6 On the visibility of $Ш(E/k)[4]$

As mentioned at the beginning of Section 4.5, visibility of elements in $Ш(E/k)[4]$ can be related to the construction used to make elements of $Ш(E/k)[2]$ visible. Suppose E_1 and E_2 are elliptic curves over a number field k and let $\lambda : E_1[4] \to E_2[4]$ be a k-group scheme isomorphism. Let λ_2 be the restriction of λ to $E_1[2]$. Then λ_2 is a k-group scheme isomorphism between $E_1[2]$ and $E_2[2]$. The added condition of having isomorphic 4-torsion can be seen as restrictions of our choices of the parameters a and d in Theorem 1.76 to a one-parameter family, as given by Proposition 3.12 (see also (3.3.4), (3.3.5), and (3.3.6) for the explicit parameterizations of a and d).

Let E be an elliptic curve over a number field k and let $v_1^2 = f(u)$ be a model for E. By Proposition 3.12, an elliptic curve E_s which has isomorphic 4-torsion to E has a model of the form

$$E_s : v_2^2 = d(s) \cdot (u - a(s))f(u) \tag{4.6.1}$$

where $a(s)$ and $d(s)$ are rational functions in one parameter, $s \in k$. The parametrization for $a(s)$ is given by (3.3.4); the parametrization for $d(s)$ is given by (3.3.5) in the case where E

and E_s have isometric 4-torsion and by (3.3.6) in the case where E and E_s have anti-isometric 4-torsion. For a given pair (E, E_s), fix a k-group scheme isomorphism $\lambda_s : E[4] \to E_s[4]$.

Let $\xi \in \mathrm{H}^1(k, E_1[4])$. Then $2\xi \in \mathrm{H}^1(k, E_1[2])$, so we can follow the approach in Section 4.5 to construct the 2-covers C_δ over E and $C_{s,\delta}$ over E_s which correspond to 2ξ and $\lambda_s(2\xi)$ respectively. We obtain

$$\begin{aligned} C_\delta &: y_1^2 = g(x) \\ C_{s,\delta} &: y_2^2 = d(s)\big(Q_{0,\delta}(\mathbf{u}(x)) + a(s)Q_{1,\delta}(\mathbf{u}(x))\big) \\ &\quad = h(x,s) \end{aligned} \tag{4.6.2}$$

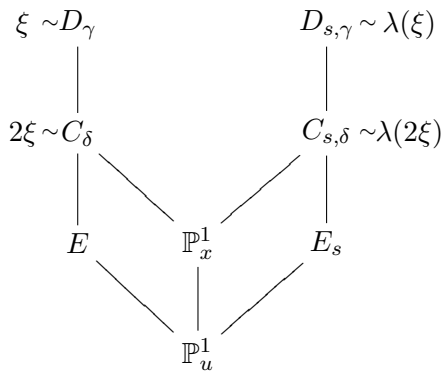
where $g(x)$ is a quartic in x and $h(x,s)$ is a *biquartic* in x and s (it has bidegree $(4,4)$ in (x,s)).

Our next step is to construct the 4-covers D_γ of E and $D_{s,\gamma}$ of E_s which will correspond to ξ and $\lambda_s(\xi)$ respectively.

Lemma 4.15. *The 4-covers D_γ and $D_{s,\gamma}$ are 2-covers of C_δ and $C_{s,\delta}$ respectively.*

Proof. This result follows immediately from the fact that C_δ and $C_{s,\delta}$ were constructed to correspond to 2ξ and $\lambda_s(2\xi) = 2\lambda_s(\xi)$ respectively. □

By Lemma 4.15, all the relevant curves fit into the following concise diagram



where $E : v_1^2 = f(u)$ is an elliptic curve and E_s is an elliptic curve with isomorphic 4-torsion to E; C_δ and $C_{s,\delta}$ are 2-covers of E and E_s respectively, and D_γ and $D_{s,\gamma}$ are 4-covers of E and E_s respectively. See (4.6.1) for a model of E_s and (4.6.2) for models of C_δ and $C_{s,\delta}$. It remains to construct D_γ and $D_{s,\gamma}$.

Constructing D_γ

To construct D_γ, we perform a second descent, this time on C_δ. Let $A = k[\beta] = k[x]/(g(x))$. Then A is an étale algebra over k. Let $\mathrm{N}_{A/k}$ denote the norm function of A over k. We can use this norm to write

$$y_1^2 = \mathrm{N}_{A[x]/k[x]}(\epsilon(x-\beta))$$

for some $\epsilon \in A^*$ where $N(\epsilon)$ equals the leading coefficient of g modulo squares. Note that since ϵ is defined through a norm equation and since the extension has degree 4, it will only be unique up to squares and scalars. As before, we can find $u_0, u_1, u_2, u_3 \in k$ and $\gamma \in A^*/A^{*2}k^*$ where $\mathrm{N}_{A/k}(\gamma)$ is a square such that

$$\begin{aligned} x - \beta &= \gamma\epsilon\left(u_0 + u_1\beta + u_2\beta^2 + u_3\beta^3\right)^2 \\ &= B_{0,\gamma}(\mathbf{u}) + B_{1,\gamma}(\mathbf{u})\beta + B_{2,\gamma}(\mathbf{u})\beta^2 + B_{3,\gamma}(\mathbf{u})\beta^3 \end{aligned} \tag{4.6.3}$$

where $\mathbf{u} = (u_0 : u_1 : u_2 : u_3) \in \mathbb{P}^3(k)$. By comparing the left and right sides of (4.6.3), we get a model of a curve

$$B_{2,\gamma}(\mathbf{u}) = B_{3,\gamma}(\mathbf{u}) = 0. \tag{4.6.4}$$

Observe that this is the intersection of two quadrics, so it is has genus 1. Working with homogeneous coordinates, this curve covers the x-line and the cover is given by

$$\mathbf{u} \longmapsto x(\mathbf{u}) = -\frac{B_{0,\gamma}(\mathbf{u})}{B_{1,\gamma}(\mathbf{u})}. \tag{4.6.5}$$

Theorem 4.16. *The pair (δ, γ) determine a 4-cover of E up to a sign choice.*

Proof. The above construction gives us a 2-cover of C_δ which in turn is a 2-cover of E. We therefore end up with D_γ being a 4-cover of E. In particular, we have the genus 1 curve in (4.6.4) covering the x-line, as given in (4.6.5). From this, it is easy to construct the cover $\psi : D_\gamma \to C_\delta$; it is given by

$$\mathbf{u} \longmapsto \left(-\frac{B_{0,\gamma}(\mathbf{u})}{B_{1,\gamma}(\mathbf{u})}, y_1(\mathbf{u})\right)$$

where

$$y_1(\mathbf{u}) = \pm\sqrt{N_{A/k}\big(\epsilon(B_{0,\gamma}(\mathbf{u}) + B_{1,\gamma}(\mathbf{u})\beta + B_{2,\gamma}(\mathbf{u})\beta^2 + B_{3,\gamma}(\mathbf{u})\beta^3)\big)}.$$

Notice that we are left with some ambiguity regarding the appropriate sign choice for $y_1(\mathbf{u})$. Recall that the $B_{i,\gamma}$ terms were found such that the above norm is a square and that these

terms are dependent on choice of γ. The $B_{i,\gamma}$'s are quadratic forms in w, so this cover is a double cover.

Similarly, we know C_δ is a 2-cover of E. Denote the cover $\phi_\delta : C_\delta \to E$ by

$$(x, y) \longmapsto (u(x, y_1), v_1(x, y_1)) .$$

Then we can construct the 4-cover $\phi_\epsilon : D_\gamma \to E$ by

$$(w, z_1) \longmapsto (\phi_\delta \circ \psi)(\mathbf{u}) = \left(u\left(-\frac{B_{0,\gamma}(\mathbf{u})}{B_{1,\gamma}(\mathbf{u})}, y_1(\mathbf{u}) \right), v_1\left(-\frac{B_{0,\gamma}(\mathbf{u})}{B_{1,\gamma}(\mathbf{u})}, y_1(\mathbf{u}) \right) \right) .$$

The forms $B_{i,\gamma}$ for $i = 0, \ldots, 3$ in (4.6.3) are dependent on our choice of γ and on the 2-cover C_δ. The 2-cover C_δ is in turn determined by the choice of δ. □

The challenge of constructing $D_{s,\lambda_s(\gamma)}$

The natural approach to constructing $D_{s,\lambda_s(\gamma)}$ is to follow the above process, but to do so by constructing the double cover over $C_{s,\lambda_s(\delta)}$, rather than over C_δ. We know that we can construct $C_{s,\lambda_s(\delta)}$ as it only requires us to follow the steps in laid out in Section 4.5, except that now the constants a and d are actually functions in a parameter s. Following through this construction in (4.6.2), we obtained

$$C_\delta : y_1^2 = g(x) \qquad \text{and} \qquad C_{s,\delta} : y_2^2 = h(x, s)$$

where g is a quartic in x and h is biquartic in x and s. We see that the dependence of a and d on s leads to a dependence of h on s. This dependence on s may pose problems in the construction of $D_{s,\lambda_s(\gamma)}$; see Remark 4.18.

As in the construction of D_γ, we begin by stepping up to an étale algebra where $h(x)$ factors. By the following Proposition, we see that we step up to the same étale algebra as before.

Proposition 4.17. *Let $A = k[\beta] = k[x]/(g(x))$. Then there exist $\alpha_1, \ldots, \alpha_4 \in A$ and $h'(x, s) \in A[x, s]$ such that*

$$h(x, s) = (\alpha_1 + \alpha_2 x + \alpha_3 s + \alpha_4 x s)h'(x, s).$$

Proof. Suppose that $\pi_s : D_{s,\lambda_s(\gamma)} \to E_s$ is a 4-cover of E_s which represents the same class as $\pi : D_\gamma \to E$. Then by Lemma 4.15, the 4-covers D_γ and $D_{s,\lambda_s(\gamma)}$ are both 2-covers of C_δ

and $C_{s,\delta}$ respectively. Both C_δ and $C_{s,\delta}$ are 2-covers which represent the same element of $\mathrm{H}^1(k, \Delta_2)$ where $\Delta_2 = E_1[2] = E_s[2]$.

By our construction, the points on C_δ which map to the identity element of E are exactly those points $P_0 = (x, 0)$, and hence have x-coordinates which satisfy $g(x) = 0$. Therefore, the points in D_γ which map to O_E are exactly the points which map to $(x, 0)$ on C_δ. By an identical argument, the points in $D_{s,\lambda_s(\gamma)}$ which lie in the zero-fibre of O_{E_s} are exactly those points (y_2, x) for which $h(x, s) = 0$. Therefore for any valid parameter s (that is to say, for any s which avoids the exceptions in Proposition 3.16) the coordinate rings of the respective zero fibres are given by $k[\beta] = k[x]/(g(x))$ and $k[\beta_s] = k[x, s]/(h(x, s))$ respectively.

By Lemma 4.12, the zero-fibres $\pi^{-1}(O_E)$ and $\pi^{-1}(O_{E_s})$ are isomorphic as 0-dimensional k-group schemes. Therefore, the coordinate rings $k[\beta]$ and $k[\beta_s]$ of the zero fibres must be isomorphic, and in so, $h(x, s)$ will acquire a bilinear factor over $A = k[\beta]$. □

To find $D_{s,\lambda_s(\gamma)}$, write $y_2^2 = h(x, s)$ as a norm equation of the bilinear factor from Proposition 4.17

$$y_2^2 = N_{A/k}(\epsilon_s(\alpha_1 + \alpha_2 x + \alpha_3 s + \alpha_4 xs)), \tag{4.6.6}$$

where $\epsilon_s \in A^*$ has norm equal to the leading coefficient of h. Once again, we can find $v_0, \ldots, v_4 \in k$ such that

$$\begin{aligned}\alpha_1 + \alpha_2 x + \alpha_3 s + \alpha_4 xs &= \epsilon_s \lambda_s(\gamma)\big(v_0 + v_1\beta + v_2\beta^2 + v_3\beta^3\big)^2 \\ &= Q_{0,\gamma}(\mathbf{v}) + Q_{1,\gamma}(\mathbf{v})\beta + Q_{2,\gamma}(\mathbf{v})\beta^2 + Q_{0,\gamma}(\mathbf{v})\beta^3\end{aligned}$$

for $\gamma \in k[\beta]^*/A^{*2}k^*$ such that $N_{A/k}(\lambda_s(\gamma))$ is square. Each $Q_{i,\gamma}$ is a quadratic form in $\mathbf{v} = (v_0, v_1, v_2, v_3)$. Note that each $\alpha_i \in A$, so write $\alpha_i = \alpha_{i,0} + \alpha_{i,1}\beta + \alpha_{i,2}\beta^2 + \alpha_{i,3}\beta^3$ for $i = 1, \ldots, 4$.

Remark 4.18. Notice that $\lambda_s(\gamma)$ may be dependent on the choice of s. If $\lambda_s(\gamma)$ has a dependence on s, then different choices of s may lead to different 4-covers $D_{s,\lambda_s(\gamma)}$. Experimental evidence obtained by checking the zero fibres of $D_{s,\lambda_s(\gamma)}$ for different s-values have shown this to be the case. Therefore, by Lemma 4.12, they cannot represent the same class in $\mathrm{H}^1(k, E[4])$. This approach will therefore not allow us to build a general model of $D_{s,\lambda_s(\gamma)}$ which takes s as a parameter to construct the appropriate 4-cover of E_s for which $\mathrm{Aut}_{\bar{k}}(C_\delta/E) \cong \mathrm{Aut}_{\bar{k}}(C_{s,\delta}/E_s)$.

In view of Remark 4.18, we will continue the discussion for a fixed value of s. Our goal in this section is to demonstrate that the visibility argument for $Ш(E/k)[m]$ is less tractable

in the $m = 4$ case than it is in the $m = 2$ or $m = 3$ cases addressed in earlier literature. To that end, we make the (generous) assumption that our choice of s in the visibility argument is not an impediment to attempting to construct the appropriate 4-cover $D_{s,\lambda_s(\gamma)}$ of E_s. We will end up demonstrating that even if one can construct $D_{s,\lambda_s(\gamma)}$, the visibility question is by no means solved.

Fisher published a paper [18] on the Hessian of a genus one curve where (in our terminology) he writes the family of 4-covers of genus one curves as the intersection of two quadrics. In particular, paraphrasing Proposition 4.1, we obtain

Proposition 4.19 (Fisher)**.** *Let $s = (a : b) \in \mathbb{P}^1$. The non-singular model $\phi_s \in X_4$ of the base 4-cover $\pi_s : E_s \to E_s$ is given by $u_4 : k^2 \to X_4$ where*

$$u_4(a, b) = \begin{cases} a(x_1^2 + x_3^2) - bx_2x_4 \\ a(x_2^2 + x_4^2) - bx_1x_3. \end{cases}$$

Proposition 4.19 provides a model for the universal elliptic curve over one particular twist of $X(4)$. Substituting back $s = (a : b)$ in the equations in Proposition 4.19 yields

$$\begin{aligned} &s(x_1^2 + x_3^2) - x_2x_4 \\ &s(x_2^2 + x_4^2) - x_1x_3. \end{aligned}$$

We can eliminate s from this to obtain

$$(x_1^2 + x_3^2)x_1x_3 = (x_2^2 + x_4^2)x_2x_4. \tag{4.6.7}$$

This surface is a smooth quartic surface in $\mathbb{P}^3$, so it is a *K*3*-surface*. For a study of *K*3-surfaces, see for example [30] and [39]. We only require the following result which was proved classically by Noether (see [30, p. 1]); using modern terminology, it reads.

Theorem 4.20 (Noether)**.** *A nonsingular quartic surface over $\mathbb{P}^3$ is a K*3*-surface.*

In fact, if we allow $i = \sqrt{-1}$, then Equation (4.6.7) factors as

$$(x_1 - ix_3)(x_1 + ix_3)x_1x_3 = (x_2 - ix_4)(x_2 + ix_4)x_2x_4. \tag{4.6.8}$$

If we make the substitution

$$(x_1 : x_2 : x_3 : x_4 :) \longmapsto (X_1 : X_2 : X_3 : X_4) = (x_1 + x_3 : x_2 + x_4 : x_1 - x_3 : x_2 - x_4)$$

then (4.6.8) becomes

$$X_1^4 - X_3^4 = X_2^4 - X_4^4. \tag{4.6.9}$$

This surface is a *diagonal quartic surface*. By Theorem 4.20, we know that it is a $K3$-surface.

To construct the surface of 4-covers $D_{s,\lambda_s(\gamma)}$, where $\gamma \in \mathrm{H}^1(k, E[4])$ is fixed and s is some parameter, we construct a surface which becomes isomorphic to $X(4)$ over $\bar{k}$. So our surface in (4.6.7) is a twist of a diagonal quartic surface. Since all twists are isomorphic over $\bar{k}$ and since being a $K3$-surface is a geometric property, the surface we are interested in constructing is indeed a $K3$-surface.

A known issue with $K3$-surfaces is that it is possible to have points everywhere locally and not be guaranteed any rational points (see for example [13, Section 5]). So even if we find a $\lambda_s(\gamma)$ such that $D_{s,\lambda_s(\gamma)}$ represents the same cocycle as D_γ (and we have no systematic way of doing this, as observed in Remark 4.18), then we still would need to search for rational points on a $K3$-surface, which is a nontrivial task on its own right.

4.7 Examples

In the previous section, we showed the difficulties that we encounter if we try to construct a general $D_{s,\gamma}$ to be a 4-cover of the family of elliptic curves E_s which have isometric (resp. anti-isometric) 4-torsion. We can, however, take our elliptic curve, E, together with a 2-cover C_δ and construct the surface $y^2 = h(x, s)$. If we find a rational point (x_0, s_0, y_0) on this surface, then we know that C_δ is visible in $(E \times E_{s_0})/\Delta_2$, where $\Delta_2 \cong E[2] \cong E_{s_0}[2]$.

Since we know that a 4-cover $D_{\delta,\gamma}$ factors through a 2-cover

$$D_{\delta,\gamma} \longrightarrow C_\delta \longrightarrow E,$$

then in order to have visibility of $D_{\delta,\gamma}$ in $(E \times E_{s_0})/\Delta_4$, we must also have that $D_{\delta,\gamma}$ is visible in $(E \times E_{s_0})/\Delta_2$. So we can carry through the first step of the construction (to check for visibility in $(E \times E_{s_0})/\Delta_2$) and then hope that the second step occurs as well. In this way, it is possible to look to make Ш[4] visible on a case by case basis.

Using our results from Chapter 3, or by using pairs of elliptic curves from Cremona and Mazur's list [16, Table 2], it is easy to construct pairs of elliptic curves with isomorphic 4-torsion. Using modern computer algebra software (we used Magma [3]), it is possible to construct 2-descents and 4-descents of our elliptic curves and to see if their fibres over O_{E_1} match up. The following would be an outline of one such procedure.

`Input:` An elliptic curve E_1, together with an everywhere locally trivial class $\gamma \in \mathrm{H}^1(k, E[4])$.

1. Find a likely candidate elliptic curve, E_2 (we can skip this step if we already have a pari of elliptic curves, as in the Cremona-Mazur list).

   (a) Using the general model of elliptic curves, E_s, which have isometric (respectively anti-isometric) 4-torsion to E_1, construct the surface $y^2 = h(x, s)$ in (4.6.2).

   (b) Search for a rational point (x_0, s_0, y_0) on the surface $y^2 = h(x, s)$. This is not easy as we are trying to find a rational point on a $K3$-surface. If a rational point (x_0, s_0, y_0) is found, then the elliptic curve E_{s_0} is a likely candidate for 4-visibility. Set $E_2 := E_{s_0}$.

2. Calculate the everywhere locally solvable 2-coverings $\mathcal{C}_1$ and $\mathcal{C}_2$ of the two elliptic curves E_1 and E_2 respectively (the Magma command `TwoDescent` would do this).

3. Verify that the two 2-coverings match up as isomorphic fibres over 0 as sets with Galois action. That is to say, for each element $C_{1,\delta} \in \mathcal{C}_1$, check that there is a unique element $C_{2,\delta} \in \mathcal{C}_2$ such that their zero fibres represent the same class in $\mathrm{H}^1(k, \Delta_2)$ (where $\Delta_2 := E_1[2] = E_2[2]$). This step gives us a means of matching each $C_{1,\delta} \in \mathcal{C}_1$ with an appropriate $C_{2,\delta} \in \mathcal{C}_2$.

4. Verify that $C_{2,\delta} \in \mathcal{C}_2$ has a rational point. If E_2 was found in step 1, then the point (x_0, s_0, y_0) should work. If, on the other hand, we began with two elliptic curves E_1, E_2 as part of our input (as is the case when using two elliptic curves off the Cremona-Mazur list) then we still need to find a rational point in this step. A rational point on $C_{s,\delta}$ indicates visibility of

$$\delta \in \ker\big(\mathrm{H}^1(k, E_1) \to \mathrm{H}^1(k, J)\big)\,,$$

   where $J = (E_1 \times E_2)/\Delta_2$. At this point, we do not know if $\delta = 0 \in \mathrm{H}^1(k, E_1)$ or if $\delta \in$ Ш$(E/k)[2]$.

5. For each matched pair $(C_{1,\delta}, C_{2,\delta})$ with $C_{i,\delta} \in \mathcal{C}_i$, perform the following loop:

   (a) Perform second descents on $C_{1,\delta}$ and $C_{2,\delta}$ to obtain the 2-coverings $\mathcal{D}_{1,\delta}$ and $\mathcal{D}_{2,\delta}$ of $C_{1,\delta}$ and $C_{2,\delta}$ respectively.

(b) Construct the zero fibres of each $D_{i,\delta,\gamma} \in \mathcal{D}_{i,\delta}$ and determine whether one can pair up each $D_{1,\delta,\gamma} \in \mathcal{D}_{1,\delta}$ with a unique $D_{2,\delta,\gamma} \in \mathcal{D}_{2,\delta}$ such that their zero fibres correspond to the same element in $\mathrm{H}^1(k, \Delta_4)$ where $\Delta_4 := E_1[4] = E_2[4]$.

6. Verify that $D_{i,\delta,\gamma} \in \mathcal{D}_4$ has a rational point. As in step 4 above, this only indicates visibility of

$$\gamma \in \ker\big(\mathrm{H}^1(k, E_1) \to \mathrm{H}^1(k, A)\big)\,,$$

where $A = (E_1 \times E_2)/\Delta_4$.

`Output:` (if positive results are obtained in step 5 and 6) Pairs of 4-covers

$$\pi_1 : D_{1,\delta,\gamma} \to E_1 \qquad \text{and} \qquad \pi_2 : D_{2,\delta,\gamma} \to E_2$$

such that $\pi_1^{-1}(O_{E_1})$ and $\pi_2^{-1}(O_{E_2})$ are isomorphic as finite sets with an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on them (i.e. they are isomorphic as 0-dimensional schemes over $\bar{k}$), and such that the element $\gamma \in \mathrm{H}^1(k, E_1)$ which is represented by $D_{1,\delta,\gamma}$ is visible in $\mathrm{H}^1(k, E_1) \to \mathrm{H}^1(k, A)$.

Suppose we find a matched pair $D_{1,\delta,\gamma}$ and $D_{2,\delta,\gamma}$ which correspond to the same element $\xi \in \mathrm{H}^1(k, \Delta_4)$, and suppose that we also find a rational point on $D_{2,\delta,\gamma}$. Then ξ vanishes in $\mathrm{H}^1(k, E_1) \to \mathrm{H}^1(k, A)$ where $A = (E_1 \times E_2)/\Delta_4$, as discussed in Section 4.4. In this case, ξ corresponds to a (possibly trivial) element of $Ш(E_1/k)[4]$. If we can also show that $\mathrm{rk}(E_2)$ and $\mathrm{rk}(A)$ would not lead to a sharper rank bound on E_1, then this would in turn guarantee that the element we found in $Ш(E_1/k)[4]$ is not trivial.

If we do not find a matched pair $D_{1,\delta,\gamma}$ and $D_{2,\delta,\gamma}$ which correspond to the same element $\xi \in \mathrm{H}^1(k, \Delta_4)$, then we have not made any element of $Ш(E_1/k)[4]$ visible. This does not imply that $Ш(E_1/k)[4]$ is empty; it merely says that the isogeny $E_1 \times E_2 \to A$ does not make any element of $Ш(E_1/k)[4]$ visible in this case. Similarly, if we fail to find a rational point on $D_{2,\delta,\gamma}$, then we have failed to show visibility in that particular case.

Example 4.1. Using Cremona and Mazur's list [16, Table 2], we can select likely candidate elliptic curves for visibility. Let E_1 and E_2 be the elliptic curves 2045B and 4090B respectively (by which we mean the elliptic curves of conductor 2045 and 4090 respectively as listed in Cremona's elliptic curve database [15]). In short Weierstrass form (over a field k with

char(k) not 2 or 3)

$$\begin{aligned} E_1 &: v_1^2 = u^3 - 7089363u - 40312768338 = f(u) \quad \text{and} \\ E_2 &: v_2^2 = u^3 + 8397u^2 + 1596942. \end{aligned} \tag{4.7.1}$$

In comparing these elliptic curves to the work in Chapter 3, we find that E_1 and E_2 have isometric 4-torsion and E_2 is obtained from E_1 by setting $s = 261$ in the model

$$v_2^2 = d(s)\,(x - a(s))\,f(u)$$

where $a(s)$ and $d(s)$ are given by (3.3.4) and (3.3.5) respectively and $f(u)$ is given by (4.7.1).

We perform a 2 descent to find the locally solvable 2-coverings $\mathcal{C}_i$ of E_i. We obtain

$$\mathcal{C}_1 = \{C_{1,1}, C_{1,2}, C_{1,3}\} \qquad \text{and} \qquad \mathcal{C}_2 = \{C_{2,1}, C_{2,2}, C_{2,3}\}$$

where

$$\begin{aligned} C_{1,1} &: y_1^2 = -27x^4 + 134x^3 + 471x^2 + 562x - 823 \\ C_{1,2} &: y_1^2 = -67x^4 + 26x^3 - 579x^2 + 808x + 12 \\ C_{1,3} &: y_1^2 = -175x^4 - 190x^3 + 147x^2 + 618x + 53 \end{aligned}$$

and

$$\begin{aligned} C_{2,1} &: y_1^2 = x^4 + 6x^3 - x^2 + 34x + 25 \\ C_{2,2} &: y_1^2 = 4x^4 - 4x^3 + 5x^2 + 20x - 12 \\ C_{2,3} &: y_1^2 = x^4 - 18x^3 + 11x^2 - 10x + 9 \end{aligned}$$

and such that for $1 \leq i \leq 3$, the zero fibre of $C_{1,i}$ is isomorphic to the zero fibre of $C_{2,i}$ as finite sets with Galois action.

We see that $(0, 5) \in C_{2,1}$, $(-2, 8) \in C_{2,2}$, and $(0, 3) \in C_{2,3}$ and so all three 2-covers of E_2 have rational points. Therefore, in all three cases, the corresponding $\delta \in \mathrm{H}^1(k, E_1)$ is made visible in $Ш(E_1, k)[2]$ (although it may be the trivial element).

Performing a second descent on each curve in the matched pair $(C_{1,1}, C_{2,1})$ yields the locally solvable 4-coverings $\mathcal{D}_{1,1} = \{D_{1,1,1}, D_{1,1,2}\}$ and $\mathcal{D}_{2,1} = \{D_{2,1}, D_{2,2}\}$ where

$$D_{1,1,1} : \begin{cases} 2u_1u_2 + u_1u_4 + u_2^2 - u_2u_3 - u_2u_4 + u_3^2 + 2u_4^2 \\ 2u_1^2 - u_1u_2 + u_1u_3 + u_1u_4 + u_2^2 - 5u_2u_3 + 4u_2u_4 - 2u_3^2 - 2u_3u_4 + u_4^2, \end{cases}$$

$$D_{1,1,2} : \begin{cases} u_1u_2 + 2u_1u_4 - u_2u_3 - 4u_2u_4 + u_3^2 + u_3u_4 + u_4^2 \\ u_1^2 + 2u_1u_2 + u_1u_3 + 3u_1u_4 + 7u_2^2 - u_2u_3 + 2u_3^2 - 4u_3u_4 - 2u_4^2, \end{cases}$$

and

$$D_{2,1,1}: \begin{cases} u_1u_3 + u_1u_4 - u_2u_4 \\ u_1u_2 - 2u_1u_3 + 2u_1u_4 + u_2^2 - u_2u_3 + u_3^2 - u_3u_4 - 2u_4^2, \end{cases}$$

$$D_{2,1,2}: \begin{cases} u_1u_4 + u_2u_3 + u_2u_4 + u_3^2 - u_3u_4 + 2u_4^2 \\ u_1u_3 + u_1u_4 + u_2^2 + u_2u_3 + u_3^2 - 7u_3u_4 - 4u_4^2. \end{cases}$$

We find with this labelling that the curves $D_{i,1,1}$ and $D_{i,1,2}$ do indeed have isomorphic zero fibres as finite sets with Galois action. If we check for automorphisms on the zero fibres, we find that each zero fibre only has the identity automorphism defined on it. Therefore, by Lemma 4.13, the covers $D_{i,1,1}$ and $D_{i,1,2}$ do indeed represent the same element in $\mathrm{H}^1(k, E_1[4]) \cong \mathrm{H}^1(k, E_2[4])$ up to multiplication by -1. We also see that the point $(u_1 : u_2 : u_3 : u_4) = (1 : 0 : 0 : 0)$ is a point on both $D_{2,1,1}$ and $D_{2,1,2}$, and therefore the classes of $D_{1,1,1}$ and $D_{1,1,2}$ both lie in the kernel of

$$\mathrm{H}^1(k, E_1) \longrightarrow \mathrm{H}^1(k, A).$$

If we perform a search for rational points on $D_{1,1,1}$ or $D_{1,1,2}$ up to a reasonable height, we do not find any points. As such, we suspect that one or both of the classes of $D_{1,1,1}$ or $D_{1,1,2}$ may in fact correspond to a nontrivial element in $Ш(E_1/k)[4]$.

If we repeat this process with the matched pairs $(C_{1,2}, C_{2,2})$ and $(C_{1,3}, C_{2,3})$, we find that in each case, the 4-coverings can also be matched up to have pairwise isomorphic zero fibres and that in each case, the point $(1 : 0 : 0 : 0)$ is on the curve $D_{2,i,j}$. So once again, we have found $\xi \in \mathrm{H}^1(k, E_1)$ which map to the zero in $\mathrm{H}^1(k, A)$.

Unfortunately, without proving that these covers in fact have no rational points, we cannot conclude that we have found nontrivial elements in $Ш(E_1/k)[4]$. In this example, we know that E_1 and E_2 have isometric 4-torsion, and so we cannot follow our construction in Chapter 3 to build A. As such, we do not know how to do a descent on A and so we cannot get an independent rank bound for A. If we check the analytic rank of E_1, we find that it has analytic rank zero. By Coates-Wiles [12], we know that the Birch-Swinnerton-Dyer conjecture is true for rank 0 curves over $\mathbb{Q}$. Therefore $\mathrm{rk}(E_1) = 0$, and since $D_{1,1,1}$ and $D_{1,1,2}$ are non-isomorphic 4-covers of E_1, we conclude that we have visibility of a nontrivial element in $Ш(E_1/k)[4]$.

In the above example, we relied on Coates-Wiles to complete the argument. By doing so, we cannot claim that our calculations contributed to improving current approaches.

In the next example, we use a pair of elliptic curves which do not appear (as a pair) on the Cremona-Mazur list. In this case, the two elliptic curves have anti-isometric 4-torsion and we are able to use the construction in Chapter 3 to prove that we do make a nontrivial element of Ш$(E_1/k)[4]$ visible (we do not need to use Coates-Wiles).

Although in this upcoming example, we once again find that $\mathrm{rk}(E_1) = 0$, the approach we use generalizes to elliptic curves of higher rank. Thus the following example shows that our approach can be used to make nontrivial elements of Ш$(E_1/k)[4]$ visible in cases where Coates-Wiles cannot be used.

Example 4.2. We now consider an example of a pair of elliptic curves which does not appear in the Cremona Mazur list [16, Table 2]. Let E_1 be the elliptic curve 2738C and let E_2 be the elliptic curve with anti-isometric 4-torsion to E_1 obtained by setting $s = 291597/7$ in Proposition 3.12. Weierstrass forms for E_1 and E_2 are given by

$$E_1 : v_1^2 + uv_1 + v_1 = u^3 + u^2 - 39045u - 7319857$$
$$E_2 : v_2^2 + uv_2 = u^3 - 12475471532u + 547368340279696.$$

We find that the locally solvable 2-coverings $\mathcal{C}_1$ and $\mathcal{C}_2$ can be pairwise matched up so that their zero fibres are isomorphic as finite sets with Galois action. Upon performing the second descent, we find that in each case, the 4-covers $\mathcal{D}_1$ and $\mathcal{D}_2$ also match up so that their zero fibres are pairwise isomorphic. The locally-solvable 4-coverings in this case are given by $\mathcal{D}_1 = \{D_{1,1}, D_{1,2}\}$ and $\mathcal{D}_2 = \{D_{2,1}, D_{2,2}, D_{2,3}, D_{2,4}\}$ where

$$D_{1,1} : \begin{cases} u_1^2 + u_1u_2 + 2u_1u_3 + u_1u_4 + u_2^2 - 4u_2u_3 - 3u_2u_4 + u_3^2 - 3u_3u_4 + 4u_4^2, \\ 5u_1u_3 + u_1u_4 + u_2^2 + 2u_2u_3 + 2u_2u_4 - 2u_3^2 + 4u_3u_4 + 3u_4^2, \end{cases}$$
$$D_{1,2} : \begin{cases} u_1^2 + u_1u_2 + 3u_1u_3 + u_2^2 + 3u_2u_3 + u_2u_4 + u_3^2 - 5u_3u_4 + 2u_4^2, \\ u_1^2 - u_1u_3 + u_1u_4 + 3u_2^2 + 2u_2u_3 - 2u_2u_4 + 3u_3^2 + 3u_3u_4 - 4u_4^2 \end{cases}$$

and where

$$D_{2,1}: \begin{cases} u_1u_4 - u_2u_3 + 3u_4^2, \\ 52u_1^2 + 23u_1u_2 + 20u_1u_3 - 358u_1u_4 - 78u_2^2 + 381u_2u_3 \\ \qquad\qquad - 53u_2u_4 - 302u_3^2 + 284u_3u_4 + 246u_4^2 \end{cases}$$

$$D_{2,2}: \begin{cases} u_1u_2 + 2u_1u_4 + u_2u_3 + u_2u_4, \\ 4u_1^2 - 159u_1u_2 + 101u_1u_3 - 107u_1u_4 - 15u_2^2 + 283u_2u_3 \\ \qquad\qquad + 90u_2u_4 + 65u_3^2 - 55u_3u_4 - 82u_4^2. \end{cases}$$

We obtain similar descriptions for $D_{2,3}$ and $D_{2,4}$. With this labelling, $D_{1,1}$ and $D_{2,1}$ have isomorphic zero fibres as finite sets with Galois action and similarly with $D_{1,2}$ and $D_{2,2}$. Checking for automorphisms on the zero fibres, we only find the identity, and so by Lemma 4.13, $D_{1,1}$ and $D_{2,1}$ (respectively $D_{1,2}$ and $D_{2,2}$) represent the same element in $\mathrm{H}^1(k, E_1[4]) \cong \mathrm{H}^1(k, E_2[4])$ up to multiplication by -1. The 4-covers $D_{2,3}$ and $D_{2,4}$ of E_2 are not isomorphic with any of the 4-covers of E_1.

If we search for points on $D_{2,1}$ and $D_{2,2}$, we find the point $(u_1 : u_2 : u_3 : u_4) = (30 : -3 : -11 : 1)$ on $D_{2,1}$ and the point $(u_1 : u_2 : u_3 : u_4) = (1/2 : -1 : -1/2 : 1)$ on $D_{2,2}$. A similar point search up to a reasonable height on $D_{1,1}$ and $D_{1,2}$ turns up no points as expected. So at this point, we know that the classes of $D_{1,1}$ and $D_{1,2}$ both lie in the kernel of

$$\mathrm{H}^1(k, E_1) \longrightarrow \mathrm{H}^1(k, A).$$

By finding no rational points in our point search of $D_{1,1}$ and $D_{1,2}$, we suspect that at least one of these may in fact correspond to nontrivial elements in $Ш(E_1/k)[4]$. We can prove this by constructing the principally polarized abelian surface $A = (E_1 \times E_2)/\Delta_4$ and checking rank bounds.

Since E_1 and E_2 have anti-isometric 4-torsion, we can construct A by using the work done in Chapter 3. In this particular case, A is the $(4,4)$-split Jacobian of a genus 2 curve C_4, and the $(4,4)$-splitting $\Phi_4 : E_1 \times E_2 \to A = \mathrm{Jac}(C_4)$ factors as

$$E_1 \times E_2 \xrightarrow{\Phi_2} \mathrm{Jac}(C_2) \xrightarrow{\Psi} \mathrm{Jac}(C_4) = A, \qquad E_1 \times E_2 \xrightarrow[\Phi_4]{} A,$$

where

$$C_2 : Y^2 = 1917636X^6 - 5752908X^5 + 661675028301X^4 - 1323340468422X^3 \\ + 66920387664764529X^2 - 66919725995489136X + 1260076140320582793936$$

and

$$\begin{aligned} C_4 : Y^2 = {} & 23018470289976X^6 - 9055728401461344X^5 + 948594742867308537X^4 \\ & + 367608666853793691018X^3 + 9836138768216101563033X^2 \\ & - 46535808647214530640895 68X - 53646240804240419319293937 6. \end{aligned}$$

We now calculate the 2-Selmer group of E_2 (using either one of the Magma [3] commands `TwoSelmerGroup`, or `TwoSelmerGroupOld`). We find that it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We also find that E_2 has no nontrivial 2-torsion elements, and so we suspect that E_2 has rank 3. Using `MordellWeilShaInformation`, we find that the following three rational points of E_2 are independent generators of the Mordell-Weil group of E_2:

$$\begin{aligned} P_1 &= \left(\frac{-149203896}{1369}, \frac{-1250794647788}{50653} \right), \\ P_2 &= \left(\frac{865048669}{19600}, \frac{24898306504623}{2744000} \right), \\ P_3 &= \left(\frac{-13769342696}{267289}, \frac{4488474509944932}{138188413} \right) \end{aligned}$$

and therefore E_2 has rank 3 as we suspected.

We can similarly calculate the 2-Selmer group of A. We find that $S^{(2)}(A/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and therefore $\mathrm{rk}(A) \leq 3$. On the other hand, by (4.1.2), we have $\mathrm{rk}(A) \geq \mathrm{rk}(E_2) = 3$ and therefore $\mathrm{rk}(A) = 3$. The rank of E_1 can be calculated by

$$\mathrm{rk}(E_1) + \mathrm{rk}(E_2) = \mathrm{rk}(E_1 \times E_2) = \mathrm{rk}(A).$$

But $\mathrm{rk}(A) = \mathrm{rk}(E_2) = 3$ and so we obtain a sharp bound of $\mathrm{rk}(E_1) = 0$. Since the rank bound is sharp and we found distinct elements in the kernel of $\mathrm{H}^1(k, E_1) \longrightarrow \mathrm{H}^1(k, A)$, we conclude that they correspond to nontrivial elements in $Ш(E_1/k)[4]$.

Appendix A

On a classical result by Bolza

An 1887 paper by O. Bolza [1] discusses hyperelliptic integrals which can reduce into elliptic integrals by a fourth degree transformation. In the terminology used in this thesis, he computes a model of a genus 2 curve with a $(4,4)$-split Jacobian. In this section we relate his results to our Chapter 3 results. The formulas given here are available electronically from [8]. Bolza works over $\mathbb{C}$. He gives a 3-parameter family of curves $y^2 = R(x)$, with parameters λ, μ, ν, with a sign error in the equation (A.0.3) below. Corrected, Bolza's family is given by:

$$C_{(\lambda,\mu,\nu)} : y^2 = R(x) = \nu' x^6 - 6\lambda\nu' x^5 + 3\left(4\mu\nu' + \lambda\mu'\right) x^4 + 2\left(\lambda\lambda' + 5\nu\nu'\right) x^3 \\ + 3\left(4\mu'\nu + \lambda'\mu\right) x^2 - 6\lambda'\nu x + \nu,$$

where

$$\lambda' = -\frac{1}{3} \cdot \frac{2\lambda^2\nu - \lambda\mu^2 - \mu\nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \tag{A.0.1}$$

$$\mu' = \frac{1}{9} \cdot \frac{\lambda^2\mu + \lambda\nu - 2\mu^2}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \tag{A.0.2}$$

$$\nu' = -\frac{1}{27} \cdot \frac{2\lambda^3 - 3\lambda\mu + \nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}. \tag{A.0.3}$$

He also gives the variable substitutions that turn the hyperelliptic integrals into elliptic integrals. In the language of this thesis, he gives the degree 4 maps from the curve $C_{(\lambda,\mu,\nu)}$ to two elliptic curves. Since Bolza is only interested in curves over $\mathbb{C}$, he does not care to determine the appropriate twist, but this is easily adjusted. With

$$z_1 = \frac{\lambda x^4 + 4\lambda\nu x + 3\mu\nu}{\lambda x^2 + 2\lambda x + \frac{3\mu\lambda - 2\nu}{2}}, \quad z_2 = \frac{\lambda' + 4\lambda'\nu' x^3 + 3\mu'\nu' x^4}{x^2(\lambda' + 2\lambda' x + \frac{3\mu'\lambda' - 2\nu'}{2} x^2)}$$

we find that $C_{(\lambda,\mu,\nu)}$ covers the two curves

$$E_{1,(\lambda,\mu,\nu)} : w_1^2 = \lambda R_1(z_1) = \lambda(\lambda z_1 - 2\nu)(\nu' z_1^3 - 3(9\lambda^2\nu' - 6\mu\nu' - \lambda\mu')z_1^2 + 12(9\lambda\nu\nu' + 3\mu'\nu + \lambda'\mu)z_1 + 12\nu(3\mu\mu' - \lambda\lambda'))$$

and

$$E_{2,(\lambda,\mu,\nu)} : w_2^2 = \lambda' R_2(z_2) = \lambda'(\lambda' z_2 - 2\nu')(\nu z_2^3 - 3(9\lambda'^2\nu - 6\mu'\nu - \lambda'\mu)z_2^2 + 12(9\lambda'\nu'\nu + 3\mu\nu' + \lambda\mu')z_2 + 12\nu'(3\mu'\mu - \lambda'\lambda)).$$

Checking this is straightforward by verifying that $\lambda R_1(z_1)R(x)$ and $\lambda' R_2(z_2)R(x)$ are squares in $\mathbb{Q}(\lambda,\mu,\nu)(x)$.

In order to find the relation between Bolza's family and the model (B.2.1), we put $E_{1,(\lambda,\mu,\nu)}$ in short Weierstrass form $V^2 = U^3 + bU + c$, where

$$\begin{aligned} b = {} & 3(\nu^2 - 3\nu\mu\lambda + 2\mu^3)^2(2\nu^4\mu - 5\nu^4\lambda^2 + 2\nu^3\mu\lambda^3 + 16\nu^3\lambda^5 - \nu^2\mu^4 + \\ & 10\nu^2\mu^3\lambda^2 - 45\nu^2\mu^2\lambda^4 - 6\nu\mu^5\lambda + 36\nu\mu^4\lambda^3 - 9\mu^6\lambda^2) \\ c = {} & (\nu^2 - 3\nu\mu\lambda + 2\mu^3)^3(\nu^7 - 3\nu^6\mu\lambda - 10\nu^6\lambda^3 - 10\nu^5\mu^3 + 84\nu^5\mu^2\lambda^2 - 138\nu^5\mu\lambda^4 + 160\nu^5\lambda^6 - \\ & 30\nu^4\mu^4\lambda + 68\nu^4\mu^3\lambda^3 - 78\nu^4\mu^2\lambda^5 - 288\nu^4\mu\lambda^7 - 2\nu^3\mu^6 + 30\nu^3\mu^5\lambda^2 - \\ & 189\nu^3\mu^4\lambda^4 + 738\nu^3\mu^3\lambda^6 - 18\nu^2\mu^7\lambda + 198\nu^2\mu^6\lambda^3 - 729\nu^2\mu^5\lambda^5 - \\ & 54\nu\mu^8\lambda^2 + 324\nu\mu^7\lambda^4 - 54\mu^9\lambda^3). \end{aligned}$$

We compute the linear transformation $U = \frac{t_1 z_2 + t_2}{t_3 z_2 + t_4}$ such that $\lambda' R_2(z_2) = d(U - a)(U^3 + bU + c)$, where d is specified up to squares, and find

$$\begin{aligned} a &= \frac{(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(2\nu^3\lambda - 3\nu^2\mu^2 - 4\nu^2\lambda^4 + 2\nu\mu^3\lambda + 6\nu\mu^2\lambda^3 - 3\mu^4\lambda^2)}{\mu\lambda - \nu} \\ d &= 3(\nu - \mu\lambda)(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(\nu^2 - 6\nu\mu\lambda + 4\nu\lambda^3 + 4\mu^3 - 3\mu^2\lambda^2). \end{aligned}$$

From $a = \frac{s^4 - 2bs^2 - 8cs + b^4}{4(s^3 + bs + c)}$ one finds one rational choice:

$$s = \frac{(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(\nu^3\lambda + 3\nu^2\mu^2 - 18\nu^2\mu\lambda^2 + 16\nu^2\lambda^4 + 10\nu\mu^3\lambda - 15\nu\mu^2\lambda^3 + 3\mu^4\lambda^2)}{\nu - \mu\lambda}.$$

This shows that outside $(\nu - \mu\lambda)(\nu^2 - 3\nu\mu\lambda + 2\mu^3) = 0$, Bolza's family covers the family (B.2.1). The relation turns out to be birational: both $(\lambda : \mu : \nu)$ and $(s : b : c)$ are naturally coordinates on weighted projective space $\mathbb{P}(1,2,3)$. The formulae above express $(b/s^2, c/s^3)$

as functions in $(\mu/\lambda^2, \nu/\lambda^3)$. Via the appropriate resultant computations and polynomial factorizations, we find

$$\begin{aligned}\psi(b,c,s) &= 2b^6 + 36b^5s^2 + 45b^4cs + 72b^4s^4 + 45b^3c^2 + 36b^3cs^3 - 36b^3s^6 + 297b^2c^2s^2 - 378b^2cs^5 \\ &\quad + 54b^2s^8 + 324bc^3s - 81bc^2s^4 + 324bcs^7 + 216c^4 - 324c^3s^3 + 891c^2s^6 - 27cs^9 \\ \frac{\mu}{\lambda^2} &= \frac{(2b^4 - 15b^2cs + 30b^2s^4 + 9bc^2 + 90bcs^3 + 135c^2s^2 - 27cs^5)\psi(b,c,s)}{3(bs + c + s^3)^2(b^2 - 6bs^2 - 12cs - 3s^4)^2(4b^3 + 27c^2)} \\ \frac{\nu}{\lambda^3} &= \frac{-\psi(b,c,s)^2}{(bs + c + s^3)^2(b^2 - 6bs^2 - 12cs - 3s^4)^3(4b^3 + 27c^2)}.\end{aligned}$$

This shows that outside some codimension one locus, the two families parametrize the same curves up to twist. Note, however, that the formulas for a, b, c, d are of weighted total degrees $13, 26, 39, 15$ in (λ, μ, ν). That means that with appropriate scaling, we can adjust the square class of d, so the two families really do parametrize essentially the same curves.

Appendix B

Long Equations

In this appendix, we have added the equations of some of the pertinent but lengthy curves found in Chapter 3. Section B.1 gives the factorization of the model of our bielliptic curve C_2 from Lemma 3.9 over a splitting field of its defining polynomial. Section B.2 gives a model of a genus 2 curve with $(4,4)$-split Jacobian, described in Theorem 3.1 and Proposition 3.16.

The equation for the Humbert surface $\mathcal{L}$ of genus 2 curves with $(4,4)$-split Jacobians (see Theorem 3.2) is too long to even include as an appendix. With this in mind, we have made it available for download over the internet [8].

B.1 The six roots of the defining polynomial for C_2

Let C_2 be a genus 2 curve over k which is $(2,2)$-isogenous to a genus 2 curve whose Jacobian is optimally $(4,4)$-split (see Lemma 3.9). Then C_2 is a degree 2 cover of an elliptic curve E_1 which admits a model $V^2 = f(U) = U^3 + bU + c$. A model for C_2 is given in (3.3.7).

$$f(U) = (U - r)\left(U^2 + rU + \left(r^2 + b\right)\right)$$

Over $k[r]/\left[U^2 - \left(-3r^2 - 4b\right)\right] = k[r, R]$, we have the factorisation

$$f(U) = (U - r)\left(U - \frac{R}{2} + \frac{r}{2}\right)\left(U + \frac{R}{2} + \frac{r}{2}\right).$$

Using our parametrization for a and d given in equations (3.3.4) and (3.3.6) respectively, we can write down the factorization for g over $k[r, R]$:

$$g(X) = f_6 \prod_{i=1}^{6} (X - w_i) \tag{B.1.1}$$

where

$$f_6 = \left(\frac{1}{-\operatorname{disc}(f)\cdot f(s)}\right)^3 = \frac{1}{\left(4b^3+27c^2\right)^3\left(s^3+bs+c\right)^3}$$

and:

$$\begin{aligned}
w_1 &= \frac{1}{2}\Big(\left(-3s^2-b\right)r^2+\left(-4bs-6c\right)r-bs^2-6cs+b^2\Big)R\\
w_2 &= \frac{1}{2}\Big(\left(3s^2+b\right)r^2+\left(4bs+6c\right)r+bs^2+6cs-b^2\Big)R\\
w_3 &= \frac{1}{2}\Big(\left(-3s^2-b\right)r^2+\left(2bs+3c\right)r-bs^2+3cs-b^2\Big)R\\
&\quad+\frac{1}{2}\Big(\left(-3bs-9c\right)r^2+\left(9cs-2b^2\right)r-4b^2s-6bc\Big)\\
w_4 &= \frac{1}{2}\Big(\left(3s^2+b\right)r^2+\left(-2bs-3c\right)r+bs^2-3cs+b^2\Big)R\\
&\quad+\frac{1}{2}\Big(\left(3bs+9c\right)r^2+\left(-9cs+2b^2\right)r+4b^2s+6bc\Big)\\
w_5 &= \frac{1}{2}\Big(\left(-3s^2-b\right)r^2+\left(2bs+3c\right)r-bs^2+3cs-b^2\Big)R\\
&\quad+\frac{1}{2}\Big(\left(3bs+9c\right)r^2+\left(-9cs+2b^2\right)r+4b^2s+6bc\Big)\\
w_6 &= \frac{1}{2}\Big(\left(3s^2+b\right)r^2+\left(-2bs-3c\right)r+bs^2-3cs+b^2\Big)R\\
&\quad+\frac{1}{2}\Big(\left(-3bs-9c\right)r^2+\left(9cs-2b^2\right)r-4b^2s-6bc\Big).
\end{aligned}$$

B.2 A representation for a $(4,4)$-split genus 2 curve

Let E_1 be an elliptic curve over k given by $V^2 = U^3 + bU + c$ for scalars b and c and let C_4 be a genus 2 curve which is a degree 4 cover of E_1. Then there exists a scalar s such that a representation for C_4 is given by $Y^2 = F(X)$ where:

$$
\begin{aligned}
F(X) = & \frac{\left(s^3+bs+c\right)\left(27cs^3-18b^2s^2-27bcs-2b^3-27c^2\right)}{\left(4b^3+27c^2\right)^3\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^6 \\
& + \frac{3\left(s^3+bs+c\right)^2\left(3s^2+b\right)}{\left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^5 \\
& + \frac{3\left(s^3+bs+c\right)E}{4\left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^4 \\
& + \frac{-\left(s^3+bs+c\right)^2 G}{2\left(4b^3+27c^2\right)\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^3 \\
& + \frac{-\left(s^3+bs+c\right)H}{16\left(4b^3+27c^2\right)\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^2 \\
& + \frac{3\left(s^3+bs+c\right)^2\left(3s^4+6bs^2+12cs-b^2\right)J}{16\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X \\
& + \frac{-\left(s^3+bs+c\right)JK}{64\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}
\end{aligned}
\tag{B.2.1}
$$

and where

$$
\begin{aligned}
E = & 9cs^7-26b^2s^6-171bcs^5+34b^3s^4-333c^2s^4+155b^2cs^3-6b^4s^2+126bc^2s^2 \\
& +7b^3cs+144c^3s-2b^5-17b^2c^2 \\
G = & 7s^6+23bs^4+68cs^3-11b^2s^2-4bcs-3b^3-20c^2 \\
H = & 27cs^{11}+6b^2s^{10}+585bcs^9-402b^3s^8+2349c^2s^8-3330b^2cs^7+460b^4s^6 \\
& -6156bc^2s^6+1410b^3cs^5-7776c^3s^5+140b^5s^4+4230b^2c^2s^4+23b^4cs^3 \\
& +3024bc^3s^3+46b^6s^2+516b^3c^2s^2+3024c^4s^2+5b^5cs-48b^2c^3s+6b^7 \\
& +85b^4c^2+288bc^4 \\
J = & s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2 \\
K = & 27cs^9-54b^2s^8-324bcs^7+36b^3s^6-891c^2s^6+378b^2cs^5-72b^4s^4 \\
& +81bc^2s^4-36b^3cs^3+324c^3s^3-36b^5s^2-297b^2c^2s^2-45b^4cs-324bc^3s \\
& -2b^6-45b^3c^2-216c^4.
\end{aligned}
$$

Bibliography

[1] Oskar Bolza, *Ueber die Reduction hyperelliptischer Integrale erster Ordnung und erster Gattung auf elliptische durch eine Transformation vierten Grade*, Math. Ann. **28** (1887), no. 3, 447–456.

[2] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR1484478

[4] Jean-Benoît Bost and Jean-François Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2, Gaz. Math. (1988), no. 38, 36–64. MR970659 (89k:14072)

[5] N. Bruin and S. R. Dahmen, *Visualizing elements of Sha[3] in genus 2 jacobians*, ArXiv e-prints (2010), `http://arxiv.org/abs/1001.5302`.

[6] N. Bruin and E. V. Flynn, *Exhibiting SHA[2] on hyperelliptic Jacobians*, J. Number Theory **118** (2006), no. 2, 266–291. MR2225283 (2006m:11091)

[7] Nils Bruin, *Visualising Sha[2] in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR2047096 (2005c:11067)

[8] Nils Bruin and Kevin Doerksen, *Electronic resources*, `http://www.cecm.sfu.ca/~nbruin/splitigusa`.

[9] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991. MR1144763 (92k:11058)

[10] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090 (97i:11071)

[11] Claude Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, No. VI, American Mathematical Society, Providence, R.I., 1963. MR0181641 (31 #5868)

[12] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251. MR0463176 (57 #3134)

[13] Daniel Coray and Constantin Manoil, *On large Picard groups and the Hasse principle for curves and $K3$ surfaces*, Acta Arith. **76** (1996), no. 2, 165–189. MR1393513 (97j:14038)

[14] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155. MR2384334 (2009g:11067)

[15] John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29. MR2282912 (2007k:11087)

[16] John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR1758797 (2001g:11083)

[17] Ron Donagi and Ron Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 2, 323–339. MR1736231 (2001a:14022)

[18] T. Fisher, *The Hessian of a genus one curve*, ArXiv Mathematics e-prints (2006), `http://arxiv.org/abs/math/0610403`.

[19] Gerhard Frey and Ernst Kani, *Curves of genus* 2 *covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. MR1085258 (91k:14014)

[20] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR1042981 (90k:14023)

[21] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 373–386. MR1913484 (2003e:14020)

[22] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[23] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction. MR1745599 (2001e:11058)

[24] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819 (22 #5637)

[25] ———, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR0141643 (25 #5040)

[26] Ernst Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), no. 2, 199–223. MR1285957 (95i:14042)

[27] Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR992075 (90i:12006)

[28] Robert M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. MR936803 (89f:14027)

[29] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800

[30] Alan L. Mayer, *Families of* $K-3$ *surfaces*, Nagoya Math. J. **48** (1972), 1–17. MR0330172 (48 #8510)

[31] B. Mazur, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232, Sir Michael Atiyah: a great mathematician of the twentieth century. MR1701928 (2000g:11048)

[32] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR861974

[33] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212. MR861976

[34] David Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34, Springer-Verlag, Berlin, 1965. MR0214602 (35 #5451)

[35] ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay, 2008, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037 (2010e:14040)

[36] Naoki Murabayashi, *The moduli space of curves of genus two covering elliptic curves*, Manuscripta Math. **84** (1994), no. 2, 125–133. MR1285952 (95f:14046)

[37] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859 (2000m:11104)

[38] Luis Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Applied Mathematics, vol. 24, Queen's University, Kingston, ON, 1999, Reprint of the 1970 original, with errata. MR1705274 (2000c:20047)

[39] B. Saint-Donat, *Projective models of $K-3$ surfaces*, Amer. J. Math. **96** (1974), 602–639. MR0364263 (51 #518)

[40] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French. MR918564 (88i:14041)

[41] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author. MR1867431 (2002i:12004)

[42] T. Shaska, *Curves of genus 2 with* (N, N) *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706 (2002m:14023)

[43] ———, *Genus 2 curves with* $(3, 3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218. MR2041085 (2005e:14048)

[44] Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461. MR1638488

[45] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR1329092 (95m:11054)

[46] Benjamin Smith, *Explicit endomorphisms and correspondences*, Ph.D. thesis, University of Sydney, 2005, `http://hdl.handle.net/2123/1066`.