Descent methods and torsion on Jacobians of higher genus curves

Chris Nicholls

Balliol College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity Term 2018

Abstract

In this thesis we accomplish four main results related to Jacobians of curves.

Firstly, we find a large number of hyperelliptic curves of genus 2, 3 and 4 whose Jacobians have torsion points of large order. The genus 2 case is particularly well-studied in the literature, and we provide a new example of a geometrically simple Jacobian of a genus 2 curve with a point of order 25, an order which was not previously known. For geometrically simple Jacobians of curves of genus 3 and 4, we extend the known orders of points, increasing the largest known order in both cases to 91 and 88, respectively.

Secondly, we find an explicit embedding of the Kummer variety of a genus 3 superelliptic curve into projective space. This is a natural extension of the embeddings that are already known for the Kummer varieties of hyperelliptic curves of genus 2 and 3.

Thirdly, we classify the genus 2 curves whose Jacobians admit a $(4, 4)$-isogeny. We find an infinite family of genus 2 curves for which the elements of the kernel of the $(4, 4)$-isogeny are defined over the ground field, and make partial progress on classifying the genus 2 curves with this property. We also extend Flynn's example of a genus 2 curve whose Jacobian admits a $(5, 5)$-isogeny to infinitely many geometrically nonisomorphic curves.

Finally, we extend Schaefer's algorithm for computing the Selmer group of a Jacobian to carry out a $(4, 4)$-descent on Jacobians of curves that admit a $(4, 4)$-isogeny.

Acknowledgements

I would like to thank my supervisor Victor Flynn for his support and encouragement during the last four years. I have learned a lot from him during many very interesting and useful conversations.

I have benefitted greatly from discussions and reading groups with my fellow students in the Mathematics Department at Oxford. I would like to thank Joshua Jackson, Jamie Beacom and Alex Betts for spending countless hours discussing Mathematics with me. I would also like to thank Minhyong Kim, Alan Lauder and Jennifer Balakrishnan for insightful conversations during my DPhil, my college advisor Frances Kirwan for her invaluable advice on many occasions, and my undergraduate tutors Nick Woodhouse and Andrew Hodges for encouraging me to pursue my love of Mathematics. I am very grateful to my examiners for their helpful comments and advice.

I would especially like to thank my parents, who inspired me to study Mathematics at university and have been incredibly supportive in all aspects of my life, my sister for being an amazing source of support throughout my DPhil, and Ellie, who has always been there to support and encourage me.

I am very grateful to the Engineering and Physical Sciences Research Council (EPSRC) and MathWorks for funding my DPhil.

Contents

List of Tables

Chapter 1

Introduction

A major aim of arithmetic geometry is to study rational solutions to diophantine equations. In more modern language, we consider solutions to algebraic varieties over number fields. This is hard in general, so it's helpful to impose more structure on the varieties. There are two situations in which finding rational points on varieties is easier. The first is when the dimension of the variety is small. The second is when there is more structure on the variety; for example, when the set of points forms a group. The first condition leads us to consider curves, which are 1-dimensional varieties, and the second condition leads us to consider abelian varieties.

The space of curves is partitioned by an isomorphism invariant called the genus. Genus 0 curves are well understood. These are the conics, and whenever there is a single rational point on a conic, the space of all rational points is birationally equivalent to the projective line. Moreover, there is an effective procedure to decide whether or not a rational point exists.

Genus 1 curves (with a rational point) are elliptic curves. Elliptic curves are also abelian varieties, and are very important objects in arithmetic geometry. If the elliptic curve is given in the form $y^2 = f(x)$ where $f(x)$ is a monic cubic, then the group law can be described by an elementary *chord and tangent process*: this defines three points P, Q, R on the curve as adding to zero precisely when they are the intersection of the curve with a line (counting multiplicities).

Curves of genus at least 2 are somewhat understood. Faltings' theorem implies that a curve of genus at least 2 over a number field has only finitely many rational points. The theorem is ineffective, meaning that it doesn't identify the points, or even how many points there are.

To any curve $\mathcal{C}$, we can associate an abelian variety called the *Jacobian* of the curve. This can be used to study the curve, but is also interesting in its own right, and is our main object of study in this thesis.

Abelian varieties Let A be an abelian variety over a number field K, and let $A(K)$ denote the group of K-rational points. The Mordell–Weil theorem states that $A(K) = A(K)_{\text{tors}} \times \mathbb{Z}^r$, where $A(K)_{\text{tors}}$ is a finite group, called the *torsion subgroup*, and r is a nonnegative integer, called the *rank*. Mordell proved the case when A is an elliptic curve over the rational numbers ([Mor22]) and Weil generalised this to abelian varieties over number fields ([Wei29]).

In this thesis we focus on the situation when the abelian variety is the Jacobian $\mathcal{J}$ of a curve $\mathcal{C}$. We are interested in the torsion subgroups that can occur and methods to determine the rank of Jacobians. A well-known method for bounding the rank is called *descent*, which aims to find an upper bound for the size of $\mathcal{J}(K)/m\mathcal{J}(K)$ for some integer $m \geq 2$. This method always theoretically gives an upper bound on the rank, but it need not be sharp. In fact, there is an exact sequence of groups

$$0 \to \mathcal{J}(K)/m\mathcal{J}(K) \to \mathrm{Sel}^m(\mathcal{J}/K) \to Ш(\mathcal{J}/K)[m] \to 0, \tag{1.1}$$

where $\mathrm{Sel}^m(\mathcal{J}/K)$ is the upper bound computed by descent, called the *Selmer group*, and $Ш(\mathcal{J}/K)[m]$ is the m-part of the *Tate-Shafarevich group*. Thus $Ш(\mathcal{J}/K)[m]$ measures the sharpness of the bound computed by descent.

It is of interest to compute examples of nontrivial elements of $Ш(\mathcal{J}/K)[m]$. One method of doing this is to play off different descents; for example, showing that the bound from a 2-descent is sharp but that the bound from a 3-descent is not. Unfortunately, it is currently computationally infeasible to do descents on Jacobians of genus 2 curves for m large. We can reduce the size of the computation by doing a descent via isogeny, instead of a complete m-descent. This can be done by finding isogenies $\varphi\colon \mathcal{J} \to \mathcal{J}'$ and $\varphi'\colon \mathcal{J}' \to \mathcal{J}$ such that the multiplication-by-m map factors as $[m] = \varphi' \circ \varphi$. For such isogenies to exist over the ground field, it is necessary that the m-torsion group $\mathcal{J}[m](\overline{K})$ has a subgroup of size m^g that is K-rational as a set. We address this problem in Chapter 5. Given a Jacobian $\mathcal{J}$ of a curve with a suitable subgroup Σ, we can often use an embedding of the Kummer variety to compute the curve $\mathcal{C}'$ such that $\mathcal{J}/\Sigma$ is isomorphic to the Jacobian of $\mathcal{C}'$. Computing the curve $\mathcal{C}'$ is interesting in its own right, but is also useful for applying the descent theory in [Sch98], as we later explain.

Torsion We are also interested in the problem of torsion on abelian varieties. This is completely understood in genus 1 using Mazur's theorem ([Maz77]), which provides an explicit list of the possible torsion subgroups of elliptic curves over $\mathbb{Q}$, as well as

examples for each torsion subgroup. It is also well-studied on Jacobians of hyperelliptic curves of genus at least 2, for which there are many examples of large order torsion points in the literature. The ultimate goal is, for each genus g, to compute the set of positive integers N for which there is a point of order N defined over $\mathbb{Q}$ on the Jacobian of a genus g curve. In genus $g \geq 2$, we can so far only find examples of such N, rather than prove bounds on the sets, or show that a certain order can't exist.

The problem naturally has two cases: split Jacobians and geometrically simple Jacobians. If the Jacobian of a curve is split, isogenous to a product of lower dimension abelian varieties, then its torsion is made up of the torsion of the varieties in the splitting. In the split case, many examples of torsion orders are known in genus 2 and 3. The main contributions are due to Howe et al. ([HLP00]) and Howe ([How14]). Of particular note is Howe's example of a split Jacobian of a genus 2 curve with a 70-torsion point ([How14]). In contrast, if the Jacobian is geometrically simple, then the torsion doesn't come from abelian varieties of lower dimension. We provide a new criterion for the Jacobian of a curve to be geometrically simple, that is easy to apply and has a simple proof.

Most of the examples of large torsion orders on Jacobians of genus 2 curves are produced by forcing the curve to have some rational non-Weierstrass points and then imposing relations between them. This produced many examples in dimension 2, and has also been used to generate families of curves whose torsion orders grow with the genus. One hopes to find larger torsion orders outside of such families, but the method has been difficult to generalise to Jacobians of higher genus curves. In fact, not many torsion orders are known for geometrically simple Jacobians of curves of genus $g \geq 3$. One main contribution is due to Kronberg, who finds a Jacobian of a genus 3 curve with a point of order 41 and a Jacobian of a genus 4 curve with a point of order 71 ([Kro15]). Kronberg doesn't show the Jacobians are geometrically simple, but we can show this using our method.

In Chapter 3, we generalise several methods for finding Jacobians with torsion points of large order so that they are practical for Jacobians of hyperelliptic genus 3 and 4 curves. We find the first example of a point of order 25 on a geometrically simple Jacobian of a genus 2 curve, and recover all known orders of torsion points on geometrically simple Jacobians of genus 2 curves. In addition, we find (conjecturally) two new curves with points of order 48, whose Jacobians are split, and one new (again, conjecturally) genus 2 curve with a point of order 32, whose Jacobian is geometrically simple. We also find a genus 2 curve with geometrically simple Jacobian defined

over $\mathbb{Q}$ with a point of order 35 defined over a quadratic extension, and a genus 2 curve with geometrically simple Jacobian defined over a degree 4 number field with a point of order 42. In genus 3 and 4 we find many new examples of torsion orders on geometrically simple Jacobians of hyperelliptic curves, contributing significantly to the known orders of points. We improve the largest known orders in both cases, to 91 and 88, respectively. Tables 3.1, 3.2 and 3.3 summarise our results, as well as the known torsion orders.

Kummer embeddings The Kummer variety is a variety associated to an abelian variety given by the quotient by negation. Like Jacobians of curves, in general Kummer varieties are usually described abstractly, without an explicit embedding into projective space. But an explicit embedding of the Kummer variety is a useful tool. Recently, Bruin et al. used the explicit embedding of the Kummer variety of a family of genus 2 curves to do explicit descent ([BFT14]). They considered the family of genus 2 curves admitting a rational copy of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ in $\mathcal{J}(\mathcal{C})[3]$. Denoting this subgroup by Σ, there is an isogeny $\varphi\colon \mathcal{J} \to \mathcal{J}/\Sigma$. The quotient $\mathcal{J}' \coloneqq \mathcal{J}/\Sigma$ is the Jacobian of another genus 2 curve, and in the paper they find the explicit equation of the curve for which $\mathcal{J}'$ is the Jacobian. To do this, they descend the isogeny φ to the Kummer varieties $\mathcal{K}$ of $\mathcal{J}$ and $\mathcal{K}'$ of $\mathcal{J}'$. The explicit embedding of the Kummer variety encodes the equation of the curve, and they were able to find the equation of the curve for $\mathcal{K}'$, and thus for $\mathcal{J}'$. They then used an algorithm due to Schaefer ([Sch98]) to compute the Selmer groups of specific Jacobians in the family, and exhibit examples of Jacobians of genus 2 curves with nontrivial 3-part of Ш.

An explicit embedding of the Kummer variety can also be used to give a theory of heights for Jacobians of curves ([Fly95], [FS97], [Sto17]). This is required to compute the full Mordell–Weil group given a full rank sublattice.

The Kummer embedding has been computed for genus 2 curves ([Fly90b]) and for genus 3 hyperelliptic curves ([Mül14], [Sto17]). In fact, in genus 2, an embedding of the Jacobian is known ([Fly90b]). The class of genus 3 curves is divided into hyperelliptic curves and smooth plane quartics. A subclass of smooth plane quartic curves is superelliptic curves of genus 3. Assuming the characteristic is not 2 or 3, such curves can be written in the form $y^3z = f(x, z)$, where f is a degree 4 homogeneous form. In Chapter 4, we find an explicit embedding of the Kummer variety of genus 3 superelliptic curves.

Descent Complete 2-descents on Jacobians of hyperelliptic curves are now routine. Recently, Bruin et al. computed a descent via $(3,3)$-isogeny [BFT14] and Flynn computed a descent via $(5,5)$-isogeny ([Fly15]). These exhibited nontrivial 2-part, 3-part and 5-part of Ш, respectively, on Jacobians of genus 2 curves. In Section 5.8, we generalise Flynn's example of Jacobians of curves with a $(5,5)$-subgroup and derive their isogenous curves.

We also find a family of genus 2 curves whose Jacobians admit a $(4,4)$-isogeny. We explicitly compute the isogeny on Kummer surfaces and find a subfamily such that the kernel of the $(4,4)$-isogeny is defined elementwise over $\mathbb{Q}$, rather than just as a subgroup. We then develop the theory required to do a descent via $(4,4)$-isogeny on the Jacobians of curves in the family. This allows us to compare the Richelot descent (also called the $(2,2)$-descent) against the $(4,4)$-descent, which gives the potential to exhibit nontrivial 2-part of Ш. We have implemented this in MAGMA but have yet to find such an example.

As a byproduct of the work on $(4,4)$-isogenies, we find an algorithm to compute $\mathcal{J}[4](\overline{K})$ for the Jacobian of a genus 2 curve.

Future work Chapter 7 contains ideas to build on the work presented in this thesis.

A note on computations All the computations in this thesis are written in the MAGMA programming language ([BCP97]). We provide the code in [Nic18]. See the `README.txt` file in that directory for instructions.

Notation We list some important notation here, though some concepts are only explained in Chapter 2. Throughout this thesis, K denotes a field and $\mathcal{C}$ denotes a curve. We write $\mathcal{J}$ for the Jacobian of a curve, and we write $\mathcal{K}$ for the Kummer variety of a curve. We usually use φ to denote an isogeny of abelian varieties. We write $[m]$ for the translation-by-m map on an abelian variety. If $f\colon A \to B$ is a homomorphism of groups, then we write $A[f]$ for the kernel of f.

For a hyperelliptic or superelliptic curve $\mathcal{C}$, we write $\pi\colon \mathcal{C} \to \mathbb{P}^1$ for the map $(x,y) \mapsto x$. For a hyperelliptic curve $\mathcal{C}\colon y^2 = f(x)$, we write $\iota\colon \mathcal{C} \to \mathcal{C}$ for the hyperelliptic involution: $(x,y) \mapsto (x,-y)$. We write $\kappa\colon \mathcal{J} \to \mathcal{K}$ for the map that sends a point on the Jacobian of a curve to its image on the Kummer variety.

Chapter 2

Background

2.1 Curves and Jacobians

2.1.1 Curves

Let K be a field. An *elliptic curve* E/K is a genus 1 curve with a K-rational point. Assuming the characteristic of K is not equal to 2 or 3, an elliptic curve is birational to $y^2 = x^3 + ax + b$ for some $a, b \in K$. Explicitly, we consider this as the projective curve in $\mathbb{P}^2$ defined by $y^2z = x^3 + axz^2 + bz^3$.

Hyperelliptic curves generalise elliptic curves to higher genus. A hyperelliptic curve is one of the form $\mathcal{C}\colon y^2 = f(x)$ for a square-free polynomial $f(x)$ of degree at least 3. When $\deg f > 3$, the projective closure of $\mathcal{C}$ in $\mathbb{P}^2$ is singular. To get around this, we define two affine coordinate charts for $\mathcal{C}$, and glue them together. Let $g = \lceil \frac{\deg f}{2} \rceil$ (we will see in Lemma 2.1.11 that this is the genus of $\mathcal{C}$). Explicitly, one coordinate chart is $y^2 = f(x)$ in $\mathbb{A}^2$ (which we refer to as the affine coordinate chart), and the other coordinate chart is $v^2 = \tilde{f}(u) = u^{2g+2}f(1/u)$. The charts are glued together via $(u, v) = \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$. We sometimes refer to this coordinate change as the *flip map*, since the coefficients of $\tilde{f}(u) = u^{2g+2}f(1/u)$ are in reverse order to the coefficients of $f(x)$.

Hyperelliptic curves naturally divide into two classes, depending on whether $\deg f$ is even or odd. If $\deg f$ is odd, then the curve always has a rational point: the (u, v)-coordinate chart has equation $v^2 = \tilde{f}(u) = u^{2g+2}f(1/u)$ and u divides $\tilde{f}(u)$, since $\deg f = 2g + 1$; thus $(u, v) = (0, 0)$ always lies on the curve. We denote this point by ∞. If $\deg f$ is even, then $\mathcal{C}$ need not have a rational point. The other coordinate chart in this case is $v^2 = \tilde{f}(u)$, where $\tilde{f}(0) = f_{2g+2} \neq 0$. There are two points at infinity: $(0, +\sqrt{f_{2g+2}})$ and $(0, -\sqrt{f_{2g+2}})$, which we denote by ∞^+ and ∞^-, respectively. We refer to ∞ and ∞^+, ∞^- as the *points at infinity*.

An odd degree hyperelliptic curve can always be transformed to an even degree hyperelliptic curve by first transforming to $(x, y) = (X + \delta, Y)$, giving the equation

$Y^2 = f(X+\delta) = g(X)$, where δ is chosen so that $g(0) \neq 0$. The flip map then gives an even degree hyperelliptic curve. To see which curves admit an odd degree form, we need to introduce Weierstrass points.

Given a hyperelliptic curve $\mathcal{C}\colon y^2 = f(x)$, we can define the hyperelliptic map $\pi\colon \mathcal{C} \to \mathbb{P}^1$ by $(x, y) \mapsto [x\colon 1]$ (in the affine coordinate chart) and $(u, v) \mapsto [1\colon u]$ in the other coordinate chart. The points at which this map is ramified are called *Weierstrass points*. If $\deg f$ is even, then these points are just $(\alpha, 0)$, where α is a root of $f(x)$. If $\deg f$ is odd, then we still get the points $(\alpha, 0)$ where α is a root of $f(x)$, but the point at infinity, ∞, is also a Weierstrass point.

A hyperelliptic curve $\mathcal{C}\colon y^2 = f(x)$ is K-birational to one of odd degree if and only if it has a K-rational Weierstrass point. Indeed, if the curve has a K-rational Weierstrass point, we can linearly transform so that $y^2 = xg(x)$, and then the flip map takes the curve to an odd degree form. Conversely, if $\mathcal{C}$ is K-birational to one of odd degree, then this odd degree curve has the K-rational Weierstrass point ∞.

A superelliptic curve is a curve of the form $y^m = f(x)$, where $m \geq 2$ and $f(x) \in K[x]$ has degree $d \geq 1$, and $f(x)$ is m-power free. If $\gcd(m, d) = 1$, then the normalisation of this affine curve is nonsingular and has a single point at infinity, denoted ∞.

If $\mathcal{C}$ is a curve over the field K, then we write $K(\mathcal{C})$ for the function field of $\mathcal{C}$.

2.1.2 Divisors and Jacobians

If X is a variety over a field K and if F/K is a field extension, then write X_F for the base extension $X \times_{\operatorname{Spec} K} \operatorname{Spec} F$.

Definition 2.1.1. *Let $\mathcal{C}$ be a smooth curve over a field K. A* divisor *on $\mathcal{C}$ is a finite linear combination of points in $\mathcal{C}(K)$. Explicitly, if $P_1, \ldots, P_r \in \mathcal{C}(K)$ and $n_1, \ldots, n_r \in \mathbb{Z}$, then $\sum_{i=1}^r n_i P_i$ is a divisor on $\mathcal{C}$. If $F \subseteq \overline{K}$ is a perfect field extension of K, then the Galois group $\operatorname{Gal}(\overline{K}/F)$ acts on $\operatorname{Div} \mathcal{C}_{\overline{K}}$ by extension of the action on $\mathcal{C}(\overline{K})$. We define $(\operatorname{Div} \mathcal{C})(F) = (\operatorname{Div} \mathcal{C}_{\overline{K}})^{\operatorname{Gal}(\overline{K}/F)}$. The set of all divisors on $\mathcal{C}$ forms an abelian group. The* degree *of the divisor $\sum_{i=1}^r n_i P_i$ is $\sum_{i=1}^r n_i$. The group of degree-0 divisors forms a subgroup of $\operatorname{Div} \mathcal{C}$, denoted $\operatorname{Div}^0 \mathcal{C}$.*

Given a function f on a smooth irreducible curve $\mathcal{C}$, we can associate a divisor $\operatorname{div} f$ as the divisor of zeroes and poles of f. Formally, for each point $P \in \mathcal{C}$, the local ring $K[\mathcal{C}]_P$ is a discrete valuation ring, with valuation $v_P\colon K(\mathcal{C}) \to \mathbb{Z}$. We define the

divisor of f as

$$\operatorname{div} f = \sum_{P \in \mathcal{C}} v_P(f) \cdot P. \tag{2.1}$$

This is a finite sum ([Sil09, Chapter II.3]).

Proposition 2.1.2 ([Har77])**.** *Let $\mathcal{C}$ be a smooth curve and let $f \in K(\mathcal{C})$ be a function on the curve. Then the degree of* $\operatorname{div} f$ *is zero.*

Example 2.1.3. *Consider the hyperelliptic curve $\mathcal{C}\colon y^2 = x^5 + 1$. This has the point $P = (0, 1)$. The function $t = x$ is a uniformiser at P since $t = 0$ intersects $\mathcal{C}$ at $y^2 = 1$, which gives $y = \pm 1$, each with multiplicity 1. We have $v_P(y) = 0$ and $v_P(x) = 1$. Note that the tangent to $\mathcal{C}$ at P is $y = 1$, and that $v_P(y-1) = v_P((y-1)(y+1)) = v_P(x^5) = 5$; we know that $v_P(y + 1) = 0$ since $t = x$ doesn't divide $y + 1$. So in fact the function $y - 1$ has a zero of multiplicity 5 at P. We reduce to finitely many calculations of $v_P(g)$ since g only meets the curve at finitely many points.*

Definition 2.1.4. *Let $\mathcal{C}$ be a curve over a field K. We say that divisors D and E in* $\operatorname{Div}\mathcal{C}$ *are* linearly equivalent *if there exists a function $g \in K(\mathcal{C})^*$ such that* $\operatorname{div} g = D - E$*. In this case, we write $D \sim E$. We define* $\operatorname{Princ}\mathcal{C}$ *as the group of divisors that are linearly equivalent to zero.*

By Proposition 2.1.2, we have $\operatorname{Princ}\mathcal{C} \subset \operatorname{Div}^0\mathcal{C}$*. We define the* Picard group *as* $\operatorname{Pic}\mathcal{C} = \operatorname{Div}\mathcal{C}/\operatorname{Princ}\mathcal{C}$*, and the degree-zero part of the Picard group as* $\operatorname{Pic}^0\mathcal{C} = \operatorname{Div}^0\mathcal{C}/\operatorname{Princ}\mathcal{C}$*.*

Let $\overline{K}$ be an algebraic closure of K and let $F \subseteq \overline{K}$ be a perfect field extension of K. The Galois group $\operatorname{Gal}(\overline{K}/F)$ naturally acts on $\operatorname{Div}^0\mathcal{C}_{\overline{K}}$, preserving the subgroup $\operatorname{Princ}\mathcal{C}_{\overline{K}}$.

Definition 2.1.5. *We define the* Jacobian *of $\mathcal{C}$ as the K-variety with F-points*

$$\mathcal{J}(F) = \left(\operatorname{Pic}^0\mathcal{C}_{\overline{K}}\right)^{\operatorname{Gal}(\overline{K}/F)}. \tag{2.2}$$

Milne shows the Jacobian exists ([Mil]). If $\mathcal{C}(K) \neq \emptyset$, then Proposition 2.1.7 shows that this definition of $\mathcal{J}(F)$ is equivalent to $\operatorname{Pic}^0\mathcal{C}_F$.

Remark 2.1.6. *Proposition 2.1.7 deals with the more general definition of the Picard group; if X is a variety over a field K, then* $\operatorname{Pic} X$ *is the group of isomorphism classes of invertible sheaves on X with multiplication being the tensor product. In this case,* $\operatorname{Pic}^0 X$ *is defined as the connected component of* $\operatorname{Pic} X$ *that contains the identity.*

Proposition 2.1.7 ([CM96])**.** *Let X be a variety over a field K. If $X(K) \neq \emptyset$, then* $\operatorname{Pic} X = (\operatorname{Pic} X_{\overline{K}})^{\mathrm{Gal}(\overline{K}/K)}$.

Proof. Suppose F/K is a finite Galois extension with Galois group G. Then we have an exact sequence

$$0 \to \operatorname{Pic} X \to (\operatorname{Pic} X_F)^G \to H^2(G, F^*) \to \ker(\operatorname{Br} X \to \operatorname{Br} X_F), \tag{2.3}$$

coming from the Hochschild-Serre spectral sequence (see Section 3.4 of [VA]). Taking the direct limit over all finite Galois extensions gives

$$0 \to \operatorname{Pic} X \xrightarrow{f} (\operatorname{Pic} X_{\overline{K}})^{G_K} \xrightarrow{g} \operatorname{Br} K \xrightarrow{h} \ker(\operatorname{Br} X \to \operatorname{Br} X_{\overline{K}}). \tag{2.4}$$

The map f is surjective if and only if $\operatorname{im} g = 0$, which holds if and only if $\ker h = 0$. Thus f is surjective if and only if h is injective. The map $g\colon \operatorname{Br} K \to \operatorname{Br} X$ comes from the structure map $\pi\colon X \to \operatorname{Spec} K$. If X has a K-point, then there is a morphism $s\colon \operatorname{Spec} K \to X$ that is a section of the structure map, meaning $\pi \circ s = \mathrm{id}$. Consider the map induced by $\pi \circ s$ on Brauer groups; this is $\operatorname{Br} K \xrightarrow{\psi} \operatorname{Br} X \xrightarrow{s} \operatorname{Br} K$ and the composition is the identity. Hence ψ is injective, so f is surjective. See [CM96] for more details. □

2.1.3 Differentials

Definition 2.1.8 (Differentials on a curve)**.** *Let $\mathcal{C}$ be a smooth irreducible curve over a field K and let $\overline{K}$ denote the algebraic closure of K. The space of* differentials *on $\mathcal{C}$ is denoted $\Omega_{\mathcal{C}}$; it is a 1-dimensional $\overline{K}(\mathcal{C})$-vector space. There is a nontrivial $\overline{K}$-linear derivation $d\colon \overline{K}(\mathcal{C}) \to \Omega_{\mathcal{C}}$; it satisfies $d(fg) = f\,dg + g\,df$ and $d(f+g) = df + dg$. There is some $f \in \overline{K}(\mathcal{C})$ such that $d(f) \neq 0$. The space $\Omega_{\mathcal{C}}$ is generated as a $\overline{K}(C)$-vector space by elements dg, where $g \in \overline{K}(\mathcal{C})$.*

If $\omega \in \Omega_{\mathcal{C}}$ is a differential on a curve $\mathcal{C}$, then, fixing $g \in \overline{K}(\mathcal{C})$, there is a unique $f \in \overline{K}(\mathcal{C})$ such that $\omega/dg = f$. We can also define divisors of differentials. If $P \in \mathcal{C}$ is a point on $\mathcal{C}$, and if $t \in \overline{K}(\mathcal{C})$ is a uniformiser at P, then we define

$$v_P(\omega) = v_P(\omega/dt). \tag{2.5}$$

Note that ω/dt is just a function on $\mathcal{C}$, so that v_P is well-defined. This valuation is nonzero for only finitely many points $P \in \mathcal{C}(\overline{K})$, and we define

$$\operatorname{div} \omega = \sum_{P \in \mathcal{C}(\overline{K})} v_P(\omega) \cdot P \tag{2.6}$$

as the divisor of ω.

The quotient of any two nonzero differentials is a function, and hence the divisors of any two differentials on a curve differ by the divisor of a function, and are thus linearly equivalent. The divisor of a differential is thus well-defined up to linear equivalence, and we call it the *canonical divisor*.

Given two divisors $D = \sum_P n_P \cdot P, E = \sum_P m_P \cdot P$ on a curve, we write $D \geq E$ if $n_P \geq m_P$ for all $P \in \mathcal{C}$. We say the divisor D is *effective* if $D \geq 0$. This leads to the definition of the Riemann-Roch space of a divisor. Let $\mathcal{C}$ be a smooth irreducible curve and let $\kappa_\mathcal{C}$ be the canonical divisor. Let D be a divisor on $\mathcal{C}$. Then let $L(D) = \{f \in \overline{K}(\mathcal{C})^* \colon \operatorname{div} f + D \geq 0\} \cup \{0\}$. This is the space of all functions on $\mathcal{C}$ that have zeroes at least where D has zeroes and poles at most where D has poles. The space $L(D)$ is a finite-dimensional $\overline{K}$-vector space. We write $\ell(D)$ for the dimension of $L(D)$.

Theorem 2.1.9 (Riemann-Roch)**.** *Let $\mathcal{C}$ be a smooth irreducible curve over an algebraically closed field K, and let $\kappa_\mathcal{C}$ be its canonical divisor. Further, let g be the genus of $\mathcal{C}$. Then*

$$\ell(D) - \ell(\kappa_\mathcal{C} - D) = \deg D + 1 - g. \tag{2.7}$$

Remark 2.1.10. *In particular, putting $D = \kappa_\mathcal{C}$ and $D = 0$ gives $\deg \kappa_\mathcal{C} = 2g - 2$.*

Using the Riemann-Roch theorem, and explicitly computing the canonical divisor on a hyperelliptic curve, we can compute the genus of hyperelliptic curves, as in the following Lemma. The proof of the lemma also serves as an example for how to compute the divisor of a function on a curve.

Lemma 2.1.11. *Let $\mathcal{C}/K$ be the hyperelliptic curve $\mathcal{C} \colon y^2 = f(x)$. Let $g = \lceil \frac{\deg f}{2} \rceil$. The canonical divisor on $\mathcal{C}$ is*

$$\kappa_\mathcal{C} = \begin{cases} (2g-2)\infty, & \text{if } \deg f \text{ odd} \\ (g-1)(\infty^+ + \infty^-), & \text{if } \deg f \text{ even}, \end{cases} \tag{2.8}$$

where ∞ and ∞^+, ∞^- are the points at infinity. Thus the genus of $\mathcal{C}$ is g.

Proof. To compute the canonical divisor it suffices to compute the divisor of any differential on $\mathcal{C}$. We use $\omega = dx$ for this. In the affine coordinate chart the curve is defined by $y^2 = f(x)$. At any non-Weierstrass affine point $P = (x_0, y_0)$ we have $y \neq 0$, and so $x - x_0$ is a uniformiser for P. Thus $v_P(dx) = v_P(dx/d(x-x_0)) = v_P(dx/dx) = 0$.

At a Weierstrass affine point, we have $P = (x_0, 0)$, and y is a uniformiser for P. We have $v_P(dx) = v_P(dx/dy)$. Since $2ydy = f'(x)dx$, we have $v_P(dx/dy) = v_P(2y/f'(x))$. Since $f(x)$ has no repeated roots, we have $f'(x) \neq 0$ at the point P. Thus $v_P(dx/dy) = 1$ at an affine Weierstrass point.

We now consider the points at infinity. In the other coordinate chart, the curve is defined by $v^2 = \tilde{f}(u) = u^{2g+2}f(1/u)$. If $\deg f$ is odd, then there is a single point at infinity, denoted ∞, and v is a uniformiser. If $\deg f$ is even, then there are two points at infinity, denoted ∞^+, ∞^-; they are the solutions to $u = 0, v^2 = \tilde{f}(0)$. In either case, we have $dx = d(1/u) = -\frac{1}{u^2}du$. The order of u at ∞ is 2 and the order of u at each of ∞^+, ∞^- is 1.

If $\deg f$ is odd, we have v is a uniformiser at ∞, and so $v_\infty(dx) = v_\infty(-\frac{1}{u^2}\frac{du}{dv})$. Using $2vdv = \tilde{f}'(u)du$, we find $v_\infty(dx) = -2v_\infty(u) + v_\infty(v) = -3$. Indeed, $\tilde{f}'(u)$ is invertible at ∞, and $v^2 = ug(u)$ where $g(0) \neq 0$ gives $u = v^2/g(u)$ in a neighbourhood of ∞.

If $\deg f$ is even, then u is a uniformiser at ∞^+, ∞^-, and so

$$v_{\infty^\pm}(dx) = v_{\infty^\pm}(-\frac{1}{u^2}du/du) = -2. \tag{2.9}$$

We can simplify by subtracting the divisor of y, which is the divisor of a function. Let W denote the set of Weierstrass points on $\mathcal{C}$. We can compute the divisor of y as

$$\operatorname{div} y = \begin{cases} \sum_{P\in W} P - (2g+2)\infty, & \text{if } \deg f \text{ odd} \\ \sum_{P\in W} P - (g+1)(\infty^+ + \infty^-), & \text{if } \deg f \text{ even}. \end{cases} \tag{2.10}$$

By subtracting the divisor of y from $\operatorname{div} dx$, we get exactly the statement in the Lemma. □

2.1.4 Mumford representation of divisors

We sometimes use the Mumford representation to represent divisors on the Jacobian of a hyperelliptic curve. This is the way MAGMA represents points on the Jacobian, and the MAGMA handbook has a good description (see [BCP97] for more details). The representation is originally due to Mumford ([Mum07], and see also [Can87]), but they only deal with the odd degree case.

Let $D \in \operatorname{Div}^0 \mathcal{C}$ be a divisor representing a point on the Jacobian $\mathcal{J}$ of a $\mathcal{C}$ of genus g. Let B be a degree g divisor on $\mathcal{C}$. The Riemann–Roch theorem (Theorem 2.1.9) implies that there is an effective degree g divisor E such that $D \sim E - B$; indeed,

$$\ell(D + B) = \ell(\kappa - D - B) + \deg(D + B) + 1 - g; \tag{2.11}$$

the right hand side is at least 1, since ℓ is the dimension of a vector space, and is thus nonnegative, and since $\deg(D+B) = g$. But $\ell(D+B)$ is the dimension of the space of functions $g \in K(\mathcal{C})$ such that $\operatorname{div} g + D + B \geq 0$. Since $\ell(D+B) \geq 1$, there exists a nonzero g, and we can then let $E = \operatorname{div} g + D + B$.

Now let $f(x)$ be a polynomial of degree 5 or 6; let $\mathcal{C}\colon y^2 = f(x)$ be the corresponding hyperelliptic curve of genus 2. We define

$$\mathfrak{m}_\infty = \begin{cases} 2\infty, & \text{if } \deg f = 5, \\ \infty^+ + \infty^-, & \text{if } \deg f = 6, \end{cases} \tag{2.12}$$

which will play the role of B in the above. Let $D \in \operatorname{Div}^0 \mathcal{C}$ be a divisor; let E be the effective divisor such that $D \sim E - \mathfrak{m}_\infty$, as above. The Mumford representation of the divisor D expresses $E - \mathfrak{m}_\infty$ as a triple $\langle a(x), b(x), d\rangle$ as follows. First write $E = P_1 + P_2$ for two points $P_1, P_2 \in \mathcal{C}$.

If $\deg f = 5$, then we first reduce the P_1, P_2 to remove any occurrences of ∞ among the P_i; after possibly relabelling, we may assume we have points $P_1, \ldots, P_d$ in the affine chart such that $E - g\infty = \sum_{i=1}^d P_i - d\infty$. Let $P_i = (x_i, y_i)$ be the coordinates of the points. Let $a(x) = \prod_{i=1}^d (x - x_i)$ be the unique monic polynomial whose roots are $x_1, \ldots, x_d$, with multiplicity. Let $b(x)$ be the unique degree $d-1$ polynomial such that $b(x_i) = y_i$ for each $i = 1, \ldots, d$. The Mumford representation of D is $\langle a(x), b(x), d\rangle$. If $d = 0$, then the representation is $\langle 1, 0, 0\rangle$, which represents the identity point on the Jacobian.

Now suppose $\deg f = 6$. If $P_1 = \iota(P_2)$, where ι denotes the hyperelliptic involution, then $P_1 + P_2 - \infty^+ - \infty^-$ is the divisor of the function $x - x(P_1)$, so represents the identity point on the Jacobian; in this case, the Mumford representation is $\langle 1, 0, 0\rangle$. This includes the case when $\{P_1, P_2\} = \{\infty^+, \infty^-\}$. If both P_1, P_2 are affine points, then we let $a(x) = (x - x_1)(x - x_2)$ and let $b(x)$ be the unique degree 1 polynomial such that $b(x_i) = y_i$ for each $i = 1, 2$. Next consider the case when precisely one of the P_i is affine, say $P_1 = (x_1, y_1)$, and $P_2 \in \{\infty^+, \infty^-\}$, with (u, v)-coordinates (u_2, v_2). In this case, we take $a(x) = x - x_1$, and define $b(x)$ of degree 2 such that $b(x_1) = y_1$ and $u_2^3 b(1/u_2) = v_2$. The remaining case is when both P_1, P_2 are at infinity and $P_1 \neq \iota(P_2)$. This corresponds to $P_1 = P_2$, with $P_1 \in \{\infty^+, \infty^-\}$. Let (u_1, v_1) be the (u, v)-coordinates of P_1. In this case, we let $a(x) = 1$ and define $b(x)$ such that $u_1^3 b(1/u_1) = v_1$. In all cases, $\deg a(x)$ is even when $\deg f = 6$.

Remark 2.1.12. *The conditions of the form $u^3 b(1/u) = v$ are due to the change of coordinates $(x, y) = (1/u, v/u^3)$ between the two coordinate charts of the hyperelliptic curve $y^2 = f(x)$.*

Remark 2.1.13. *This is unfortunately complicated to define properly, but not too difficult to work with.*

2.1.5 Igusa invariants

The Igusa invariants are geometric isomorphism invariants for hyperelliptic curves of genus 2 over a field K ([Igu60]). Two hyperelliptic curves of genus 2 over K are isomorphic over $\overline{K}$ if and only if their Igusa invariants are equal. Let $\mathcal{C}\colon y^2 = f(x)$ be a hyperelliptic curve. The Igusa invariants of $\mathcal{C}$ are defined as explicit polynomials $(I_2 \colon I_4 \colon I_6 \colon I_{10})$ in the coefficients of $f(x)$ in the weighted projective space $\mathbb{P}(2,4,6,10)$.

It suffices to define the Igusa invariants in the case $\deg f = 6$, since any hyperelliptic curve is birational to one in this form. We thus give the Igusa invariants in the case that $\deg f = 6$. See Igusa's original paper for his more general definition ([Igu60]).

Let $x_1, \ldots, x_6$ be the roots of $f(x)$ in $\overline{K}$. The symmetric group S_6 acts on the polynomial ring $K[t_1, \ldots, t_6]$ by permuting the t_i. We now define a map

$$\begin{aligned} h\colon K[t_1,\ldots,t_6] &\to K[t_1,\ldots,t_6] \\ g &\mapsto \frac{1}{\#\operatorname{Stab}_{S_6}(g)} \sum_{\sigma\in S_6} \sigma(g), \end{aligned} \tag{2.13}$$

where $\operatorname{Stab}_{S_6}(g)$ denotes the stabiliser subgroup of g. Let e be the map that sends $t_i \mapsto x_i$ for $i = 1, \ldots, 6$. We now also the notation t_{ij} to denote $t_i - t_j$.

With this notation, we define the Igusa invariants as

$$\begin{aligned} I_2 &= f_6^2 e(h(t_{12}^2 t_{34}^2 t_{56}^2)), \\ I_4 &= f_6^4 e(h(t_{12}^2 t_{23}^2 t_{31}^2 t_{45}^2 t_{56}^2 t_{64}^2)), \\ I_6 &= f_6^6 e(h(t_{12}^2 t_{23}^2 t_{31}^2 t_{45}^2 t_{56}^2 t_{64}^2 t_{14}^2 t_{25}^2 t_{36}^2)), \\ I_{10} &= f_6^{10} e(\prod_{i<j} t_{ij}^2), \end{aligned} \tag{2.14}$$

where f_6 is the leading coefficient of $f(x)$. In particular, $I_{10} = \operatorname{disc}(f)$.

Remark 2.1.14. *We will use the Igusa invariants to check whether the curves we find in Chapter 3 are geometrically isomorphic to known curves in the literature, and also in Chapter 5 to show that the curves we find that admit a $(5,5)$-isogeny are geometrically nonisomorphic.*

Example 2.1.15. *Let $\mathcal{C}_1\colon y^2 = x^6+x+1$ and $\mathcal{C}_2\colon y^2 = 2(x^6+x+1)$ be two hyperelliptic curves over $\mathbb{Q}$. The* MAGMA *function* `IgusaClebschInvariants` *computes their Igusa*

invariants as

$$(-240 : 1620 : -119880 : -43531), \tag{2.15}$$

$$(-960 : 25920 : -7672320 : -44575744), \tag{2.16}$$

respectively. These are equal in the projective space $\mathbb{P}(2,4,6,10)$*, since* (2.16) *equals* (2.15) *scaled by* 2*. This reflects that* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are isomorphic over* $\overline{\mathbb{Q}}$*. On the other hand, let* $\mathcal{C}_3\colon y^2 = x^6 + 2x + 1$*.* MAGMA *computes the Igusa invariants of* $\mathcal{C}_3$ *as*

$$(-240 : 1620 : -119880 : 153344). \tag{2.17}$$

There is no $d \in \overline{\mathbb{Q}}^*$ *such that* $(d^2 I_2 \colon d^4 I_4 \colon d^6 I_6 \colon d^{10} I_{10})$ *is equal to both* (2.15) *and* (2.17)*, and thus the Igusa invariants of* $\mathcal{C}_1$ *and of* $\mathcal{C}_3$ *are not equal. Consequently,* $\mathcal{C}_1$ *and* $\mathcal{C}_3$ *are not geometrically isomorphic.*

2.2 Abelian varieties

Definition 2.2.1. *Let* K *be a field. An* abelian variety A/K *is a proper variety* A *with a distinguished point* $0 \in A(K)$ *and morphisms* $m\colon A \times A \to A$ *and* $[-1]\colon A \to A$ *such that* m *(the group law) and* $[-1]$ *(the inverse map) satisfy the axioms of a group.*

If A is an abelian variety over a field K, then the set of rational points $A(K)$ is a group. Jacobians of curves are group varieties, with the group law inherited from the divisor group of the curve.

Theorem 2.2.2 (Mordell–Weil ([Wei29]))**.** *Let* A *be an abelian variety over a number field* K*. Then the group of rational points is finitely generated. Thus, there is a finite abelian group* $A_{\mathrm{tors}}(K)$ *and a nonnegative integer* r *such that* $A(K) \cong A_{\mathrm{tors}}(K) \times \mathbb{Z}^r$*.*

Definition 2.2.3. *Let* A *and* B *be abelian varieties over a field* K*. An* isogeny *is a surjective map* $\varphi\colon A \to B$ *with finite kernel.*

An important example of an isogeny is the multiplication-by-m map, defined for each nonzero $m \in \mathbb{Z}$. We denote the isogeny by $[m]\colon A \to A$.

For all $a \in A$, we let t_a denote the translation-by-a map $A \to A$. Given a line bundle L on an abelian variety A we can define the map

$$\varphi_L\colon A \to \mathrm{Pic}(A) \tag{2.18}$$

$$a \mapsto t_a^* L \otimes L^{-1}. \tag{2.19}$$

Theorem 2.2.4 (Riemann-Roch for abelian varieties ([Mum70]))**.** *Let L be a line bundle on an abelian variety A. Then $L = \mathcal{O}(D)$ for some divisor D on X. We have*

(i) $\chi(L) = (D^g)/g!$,

(ii) $\chi(L)^2 = \deg \varphi_L$,

where (D^g) is the gth self-intersection of D.

2.2.1 The dual abelian variety

We give a brief description of the dual abelian variety, following Milne in [Mil], and refer there for further background. We first introduce some notation. Let A be an abelian variety. Suppose T is a K-variety, with $t\colon \operatorname{Spec} K(t) \to T$ a given $K(t)$-point; then we write A_t for the product $A \times_K \operatorname{Spec} K(t)$.

We define the *Picard variety* of an abelian variety A as the group of invertible sheaves on A. We define $\operatorname{Pic}^0 A$ as the subgroup of invertible sheaves $\mathcal{L} \in \operatorname{Pic} A$ that satisfy $t_a^*\mathcal{L} \cong \mathcal{L}$ for all $a \in A(\overline{K})$. Let T be a K-variety. We define a *family of degree-0 invertible sheaves parametrised by* T as an invertible sheaf $\mathcal{L}$ on $A \times T$ satisfying

(i) $\mathcal{L}|_{A\times\{t\}} \in \operatorname{Pic}^0(A_t)$ for all $t \in T$, and

(ii) $\mathcal{L}|_{\{0\}\times T}$ is trivial.

We temporarily refer to such a pair $(T, \mathcal{L})$ as a K-pair for A. We define the *dual abelian variety* as a K-pair $(A^\vee, \mathcal{P})$ for A satisfying the following universal property: for any K-pair $(T, \mathcal{L})$ for A there exists a unique regular map $f\colon T \to A^\vee$ such that $\mathcal{L} \cong (1 \times f)^*\mathcal{P}$.

Letting T be a field extension K' of K, the points $A^\vee(K')$ are in bijection with $\operatorname{Pic}^0 A_{K'}$. Thus we can represent points of $A^\vee(K')$ by divisors on $A_{K'}$.

A *polarisation* of an abelian variety A is an isogeny $\lambda\colon A \to A^\vee$ such that over $\overline{K}$ there is an ample invertible sheaf $\mathcal{L}$ such that λ is the map

$$\begin{aligned} A(\overline{K}) &\to \operatorname{Pic}(A_{\overline{K}}) \\ a &\mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}. \end{aligned} \tag{2.20}$$

Given an isogeny $\varphi\colon A \to B$ of polarised abelian varieties, Milne defines the *dual isogeny* $\varphi^\vee\colon B^\vee \to A^\vee$ in [Mil]. If A is principally polarised, with polarisation $\lambda_A\colon A \to A^\vee$, and B is polarised, with polarisation $\lambda_B\colon B \to B^\vee$, we can define the composition

$$B \xrightarrow{\lambda_B} B^\vee \xrightarrow{\varphi^\vee} A^\vee \xrightarrow{\lambda_A^{-1}} A, \tag{2.21}$$

which we also refer to as the dual isogeny when it is clear from context.

Remark 2.2.5. *In the case that $\varphi\colon A \to A$ is an endomorphism of abelian varieties, and $\lambda\colon A \to A^\vee$ is a principal polarisation, then $\varphi \mapsto \lambda^{-1} \circ \varphi^\vee \circ \lambda$ is the Rosati involution (see [CS86] for more about the Rosati involution).*

2.2.2 The Weil pairing

We first give the general definition of the Weil pairing on an abelian variety, which generalises better to the Weil pairing e_φ of an isogeny, and then give a definition more suitable for computations.

We follow Milne for this section ([Mil]). Let A be an abelian variety over a field K. For an integer $n \geq 2$, we define the Weil pairing

$$e_n\colon A[n] \times A^\vee[n] \to \mu_n \tag{2.22}$$

as follows. Let $a \in A[n](\overline{K})$ and let $a' \in A^\vee[n](\overline{K})$. As in Section 2.2.1, we can represent a' by a divisor D on A. Let $\mathcal{L}$ be the invertible sheaf corresponding to the divisor D; since $\mathcal{L} \in \operatorname{Pic}^0 A$, we have $[n]^*\mathcal{L} \cong \mathcal{L}^n$ (see [Mil, Remark 8.5]). The equivalent statement in divisors is that $[n]^*D$ is linearly equivalent to nD, and since $a' \in A^\vee[n]$ we have $nD \sim 0$. In particular, there are functions f, g on A such that $\operatorname{div} f = nD$ and $\operatorname{div} g = [n]^*D$. Following Milne (and compare with [Sil09, Section III.8] for the elliptic curves case), we have

$$\operatorname{div}(f \circ [n]) = [n]^* \operatorname{div} f = [n]^*(nD) = n([n]^*D) = n \operatorname{div} g = \operatorname{div} g^n. \tag{2.23}$$

Hence $g^n/(f \circ [n])$ is a rational function on A without zeroes or poles and is therefore constant, say $g^n = c(f \circ [n])$ for some $c \in K^*$. Let $x \in A$; then

$$g^n(x + a) = cf([n](x + a)) = cf([n](x)) = g^n(x), \tag{2.24}$$

which implies $x \mapsto g^n(x + a)/g^n(x)$ is the constant map 1, wherever it is defined. The image of the map $x \mapsto g(x + a)/g(x)$ is thus contained inside μ_n. A map from a complete variety to an affine variety is constant, and so we identify the map with $g(x + a)/g(x) \in \mu_n$ for any $x \in A$ at which the map is defined. Thus we define

$$e_n(a, a') = \frac{g(x + a)}{g(x)} \in \mu_n \tag{2.25}$$

for any $x \in A$ at which the right hand side is defined.

Given a polarisation $\lambda\colon A \to A^\vee$, we can then define the pairing

$$\begin{aligned} e_n^\lambda\colon A[n] \times A[n] &\to \mu_n \\ e_n^\lambda(a, b) &= e_n(a, \lambda b). \end{aligned} \tag{2.26}$$

An alternative definition of e_n Let $f \in K(\mathcal{C})$ be a function defined on a curve. If $D = \sum_P n_P \cdot P \in \operatorname{Div} \mathcal{C}$ is a divisor and if D and $\operatorname{div} f$ have disjoint support, then we define

$$f(D) = \prod_P f(P)^{n_P}. \tag{2.27}$$

If $c \in K^*$, then

$$(c \cdot f)(D) = \prod_P (c \cdot f)(P)^{n_P} = c^{\deg D} f(D). \tag{2.28}$$

Hence if $\deg D = 0$, then $f(D)$ is independent of scaling f by a constant.

Remark 2.2.6. *Note the difference between $(c \cdot f)(D)$ and $c \cdot (f(D))$. The former is the function $c \cdot f$ evaluated at the divisor D, and the latter is $f(D)$ multiplied by the constant c.*

Then we can define the Weil pairing on degree zero divisors as follows.

Proposition 2.2.7 ([How96])**.** *Let $D_1, D_2 \in \operatorname{Div}^0 \mathcal{C}$ be divisors representing n-torsion points in $\mathcal{J}(\mathcal{C})$. Then there are functions $h_i \in \overline{K}(\mathcal{C})^\times$ such that $\operatorname{div} h_i = nD_i$, for $i = 1, 2$. The Weil pairing satisfies*

$$\begin{aligned} e_n &\colon \mathcal{J}[n] \times \mathcal{J}[n] \to \mu_n \\ e_n(D_1, D_2) &= \frac{h_2(D_1)}{h_1(D_2)}. \end{aligned} \tag{2.29}$$

The following well-known lemma shows explicitly that the Weil pairing is well-defined on the Jacobian. There are many proofs for the elliptic curve case, but I couldn't find an exact reference for the more general case. We give the proof as it is instructive for computing the Weil pairing.

Lemma 2.2.8. *The Weil pairing e_n is well-defined on the Jacobian. That is, if $D_1 \sim D_1'$, then $e_n(D_1, D_2) = e_n(D_1', D_2)$.*

Proof. Suppose we replace D_1 with D_1' where $\operatorname{div} g = D_1 - D_1'$ and h_1 with h_1', where $\operatorname{div} h_1' = nD_1'$. Then we want to show the Weil pairing is invariant; that is,

$$\frac{h_2(D_1)}{h_1(D_2)} = \frac{h_2(D_1')}{h_1'(D_2)}. \tag{2.30}$$

We start with the right hand side and rearrange:

$$\frac{h_2(D_1')}{h_1'(D_2)} = \frac{h_2(D_1 - \operatorname{div} g)}{h_1(D_2)(h_1'/h_1)(D_2)} \tag{2.31}$$

$$= \frac{h_2(D_1)}{h_1(D_2)} \cdot \frac{1}{h_2(\operatorname{div} g)(h_1'/h_1)(D_2)}. \tag{2.32}$$

To show the result it is equivalent to show that $h_2(\operatorname{div} g) = (h_1/h_1')(D_2)$. Using Weil reciprocity, this is equivalent to

$$g(\operatorname{div} h_2) = (h_1/h_1')(D_2). \tag{2.33}$$

But $\operatorname{div} h_2 = nD_2$, so that $g(\operatorname{div} h_2) = g^n(D_2)$. Moreover, $\operatorname{div} g^n = nD_1 - nD_1' = \operatorname{div}(h_1/h_1')$. Hence g^n and h_1/h_1' differ by a constant, and so are equal when evaluated on divisors.

We can show similarly that we can replace D_2 by a linearly equivalent D_2'. Hence the Weil pairing is invariant on replacing divisors with linearly equivalent divisors. □

Remark 2.2.9. *Note that if we just replace D_1 by $D_1' = D_1 + \operatorname{div} g$, and don't replace h_1 by h_1', then we find*

$$\frac{h_2(D_1')}{h_1(D_2)} = \frac{h_2(D_1 + \operatorname{div} g)}{h_1(D_2)} = \frac{h_2(D_1)}{h_1(D_2)} \cdot h_2(\operatorname{div} g) \tag{2.34}$$

$$= e_n(D_1, D_2) \cdot g(\operatorname{div} h_2) = e_n(D_1, D_2) \cdot g(D_2)^n, \tag{2.35}$$

so that $e_n(D_1, D_2)$ is well-defined modulo $K(g, D_2)^{*n}$, where $K(g, D_2)$ is the field of definition of g and D_2. In particular, if D_1, D_1', D_2 are defined over K, then we can compute $e_n(D_1, D_2) \equiv$ modulo K^{*n} by just computing $h_2(D_1')/h_1(D_2)$. This can be useful when the supports of D_1 and D_2 are not disjoint, as then one of h_1 or h_2 can have a zero or pole along D_2 or D_1.

The Weil pairing for an isogeny We now define the Weil pairing for an isogeny of abelian varieties. This is the definition given in [Sch98].

Definition 2.2.10. *Let $\varphi\colon A \to B$ be a degree n isogeny of abelian varieties, and let $\varphi^\vee\colon B^\vee \to A^\vee$ be the dual isogeny. Let $D \in A[\varphi]$ and let $E \in B^\vee[\varphi^\vee]$. Let D' be a divisor on $A^\vee$ representing D and let g be a function on $B^\vee$ with divisor $\varphi^{\vee -1}D'$. Then define*

$$e_\varphi(D, E) = g(E + X)/g(X) \tag{2.36}$$

for any $X \in B^\vee$ for which the right hand side is defined.

Suppose $\varphi\colon \mathcal{J} \to \mathcal{J}'$ is an isogeny of Jacobians, and let $\lambda\colon \mathcal{J} \to \mathcal{J}^\vee$ and $\lambda'\colon \mathcal{J}' \to \mathcal{J}'^\vee$ be the canonical principal polarisations. Let $\varphi' = \lambda^{-1}\varphi^\vee\lambda'$, as in Section 2.2.1. Then we can define the φ-Weil pairing with respect to λ' as

$$\begin{aligned} e_\varphi^{\lambda'}\colon \mathcal{J}[\varphi] \times \mathcal{J}'[\varphi'] &\to \mu_m \\ (P, Q) &\mapsto e_\varphi(P, \lambda'(Q)). \end{aligned} \tag{2.37}$$

Where it is clear from context, we drop the superscript for the polarisation.

The Weil pairing is compatible Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be an isogeny, and let $\varphi'\colon \mathcal{J}' \to \mathcal{J}$ be its dual, so that $\varphi' \circ \varphi = [m]$ for some integer m. The Weil pairing is compatible, in the sense that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{J}[m] \times \mathcal{J}[\varphi] & & \\ \downarrow{\scriptstyle \varphi\times\mathrm{id}} & \searrow^{e_m} & \\ & & \mu_m \\ \mathcal{J}'[\varphi'] \times \mathcal{J}[\varphi] & \nearrow_{e_\varphi} & \end{array} \tag{2.38}$$

More generally, let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a sequence of isogenies, so φ_1 is an m_1-isogeny and φ_2 is an m_2-isogeny. Then the following diagram commutes

$$\begin{array}{ccc} \mathcal{J}_1[\varphi_2\varphi_1] \times \mathcal{J}_3[\varphi_2'] & & \\ \downarrow{\scriptstyle \varphi_1\times\mathrm{id}} & \searrow^{e_{\varphi_2\varphi_1}} & \\ & & \mu_{m_1m_2} \\ \mathcal{J}_2[\varphi_2] \times \mathcal{J}_3[\varphi_2'] & \nearrow_{e_{\varphi_2}} & \end{array} \tag{2.39}$$

Remark 2.2.11. *The first commutative diagram shows that on $\mathcal{J}[m] \times \mathcal{J}[\varphi]$ we have $e_m(D, E) = e_\varphi(\varphi(D), E)$. This shows that if we restrict to $\mathcal{J}[\varphi] \times \mathcal{J}[\varphi]$, then we have $e_m(D, E) = e_\varphi(\varphi(D), E) = e_\varphi(0, E) = 1$, since $D \in \mathcal{J}[\varphi]$.*

2.2.3 Principally polarised abelian surfaces

Let X be an abelian variety over an algebraically closed field K. Let $G = \sum_{i=1}^n \mathcal{C}_i$ be an effective 1-cycle on X, and let D be an ample divisor on X. Let $\mathcal{J}_i$ be the Jacobian of $\mathcal{C}_i$. The Albanese variety of a curve $\mathcal{C}$ is its Jacobian, $\mathcal{J}$. Thus, given a curve $\mathcal{C}$ contained in an abelian variety X, the inclusion $\iota\colon \mathcal{C} \hookrightarrow X$ and the Abel-Jacobi map $u\colon \mathcal{C} \to \mathcal{J}$ induce a map $f\colon \mathcal{J} \to X$. Now let f be the map $\mathcal{J}(\mathcal{C}_1) \times \cdots \times \mathcal{J}(\mathcal{C}_n) \to X$, with the ith component defined as in the previous sentence for $\mathcal{C}_i$.

We say (X, D, G) is a *Jacobian triple* if f is an isomorphism of abelian varieties and f^*D gives a principal polarisation for $\mathcal{J}(\mathcal{C}_1) \times \cdots \times \mathcal{J}(\mathcal{C}_n)$.

Theorem 2.2.12 (Matsusaka-Ran criterion ([Col84]))**.** *Let X be an abelian variety of dimension g over an algebraically closed field. Let G be an effective 1-cycle that generates X and let D be an ample divisor on X such that $\deg(G \cdot D) = g$. Then (X, D, G) is a Jacobian triple.*

Corollary 2.2.13 ([And17])**.** *Let X be a principally polarised abelian surface over an algebraically closed field. Then either $X \cong \mathcal{J}(\mathcal{C})$ for a genus 2 curve $\mathcal{C}$, or $X \cong E_1 \times E_2$ for elliptic curves E_1, E_2.*

Proof. Let $\mathcal{L} = \mathcal{O}(D)$ be the principal polarisation of X. By the Riemann-Roch theorem for abelian varieties (Theorem 2.2.4), we have $\chi(\mathcal{O}(D))^2 = \deg \mathcal{L} = 1$, since $\mathcal{L}$ is a principal polarisation. Since $\mathcal{O}(D)$ is ample, we conclude that $\chi(\mathcal{O}(D)) = 1$. Also by the Riemann-Roch theorem for abelian varieties, we have $\chi(\mathcal{O}(D)) = (D^g)/g! = (D \cdot D)/2$. Thus $(D \cdot D) = 2$.

We can now apply the Matsusaka-Ran criterion to the effective 1-cycle D. If D is irreducible, then D is a smooth curve and $X \cong \mathcal{J}(D)$. Also, $g(D) = \dim \mathcal{J}(D) = \dim X = 2$, so D has genus 2. If D is reducible, then $D = D_1 + D_2$ for two smooth curves D_1, D_2, and we have $X \cong \mathcal{J}(D_1) \times \mathcal{J}(D_2)$. Thus $\dim \mathcal{J}(D_1) + \dim \mathcal{J}(D_2) = \dim X = 2$, so $\dim \mathcal{J}(D_i) = 1$ for $i = 1, 2$. Consequently, the D_i are both elliptic curves, so $\mathcal{J}(D_i) \cong E_i$ for elliptic curves E_1, E_2. □

Remark 2.2.14. *The principally polarised abelian varieties that are isomorphic to a product of elliptic curves form a closed subset. Thus Jacobians of genus 2 curves are dense in the moduli space of principally polarised abelian surfaces.*

Proposition 2.2.15 ([CS86], Proposition 16.8)**.** *Let $f\colon A \to B$ be an isogeny of degree prime to* char k*, and let $\lambda\colon A \to A^\vee$ be a polarisation of A. Then $\lambda = f^*(\lambda')$ for some polarisation λ' on B if and only if $\ker f \subset \ker \lambda$ and e^λ is trivial on $\ker f \times \ker f$.*

This implies the following useful corollary.

Corollary 2.2.16. *Let A be a principally polarised abelian variety, and let $\Sigma \subseteq A[m]$. Then A/Σ is an abelian variety. If Σ is isotropic for the m-Weil pairing and $\#\Sigma = m^g$, then A/Σ is principally polarised.*

Proof. Let λ_A be a principal polarisation for A. Consider the polarisation $\eta = \lambda_A \circ [m]$ of A. If Σ is isotropic for the m-Weil pairing, then e_m^η is trivial on $\Sigma \times \Sigma$. Let $f\colon A \to A/\Sigma$ be the quotient map. We have $\ker f = \Sigma \subset A[m] = \ker \eta$ and thus by Proposition 2.2.15, there is a polarisation η' on A/Σ such that $\eta = f^*(\eta')$.

Comparing degrees, we have $\deg \eta = (\deg f)^2 \deg \eta'$. By assumption, $\#\ker f = \#\Sigma = m^g$. Also, $\deg \eta = \deg(\lambda_A \circ [m]) = \deg(\lambda_A)\deg([m]) = m^{2g}$, where $g = \dim A$. This implies $\deg \eta' = 1$, so that η' is a principal polarisation on A/Σ. □

2.3 Simplicity of Jacobians

Let A be an abelian variety over a field K. We say A is *simple* if the only abelian subvarieties of A are 0 and A. Otherwise we say that A is *split*. By Poincaré's complete reducibility theorem (see Theorem 1 in section 19 of [Mum70]), given an abelian variety A, there are pairwise non-isogenous abelian varieties $A_1, \ldots, A_r$ and positive integers n_i such that A is isogenous to $A_1^{n_1} \times \cdots \times A_r^{n_r}$. The A_i are unique up to isogeny and the n_i are unique.

We say that A is simple or split over an extension F of K if the base change A_F is simple or split, respectively. If A is split over F, then the abelian varieties $A_1, \ldots, A_r$ and the isogeny $A \to A_1^{n_1} \times \cdots \times A_r^{n_r}$ are defined over F. We say that A is *geometrically split* (or *absolutely split*) if A is split over the algebraic closure $\overline{K}$, and otherwise say that A is *geometrically simple* (or *absolutely simple*).

2.3.1 The characteristic polynomial of Frobenius

Let X be a scheme over the finite field $k = \mathbb{F}_q$, where char $k = p$. We define the Frobenius endomorphism F of X to be the identity on the topological space X and the homomorphism $f \mapsto f^q$ on structure sheaves. If A is an abelian variety over k and $\ell \neq p$ is prime, then the Frobenius endomorphism F of A induces an endomorphism of the Tate module $T_\ell A$. This endomorphism has an associated characteristic polynomial, which we denote by $P_A(t)$. The polynomial $P_A(t)$ is monic of degree $2\dim A$ and lies in $\mathbb{Z}[t]$ (see [Mum70], section 19, Theorem 4).

The following theorem of Tate relates abelian subvarieties of an abelian variety to factors of its characteristic polynomial.

Theorem 2.3.1 ([Tat66], Theorem 1)**.** *Let X and Y be abelian varieties defined over a finite field k. Let P_X and P_Y be the characteristic polynomials of their Frobenius endomorphisms over k, respectively. Then the following statements are equivalent:*

1. Y is isogenous over k to an abelian subvariety of X defined over k;

2. P_Y divides P_X.

Thus if P_A is irreducible, then A is simple over k.

Let $\mathcal{C}$ be a curve of genus g over a finite field $\mathbb{F}_q$, and let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. By the Weil conjectures, the characteristic polynomial of Frobenius of $\mathcal{J}$ over $\mathbb{F}_q$ factors as

$$P_{\mathcal{J}}/\mathbb{F}_q = \prod_{i=1}^{g}(t-\alpha_i)(t-\overline{\alpha_i}) \tag{2.40}$$

for some complex numbers α_i such that $\alpha_i\overline{\alpha_i} = q$. We can also do this over extensions of $\mathbb{F}_q$, and the Weil conjectures relate $P_{\mathcal{J}}/\mathbb{F}_q$ to $P_{\mathcal{J}}/\mathbb{F}_{q^n}$ for $n \geq 1$. In particular,

$$P_{\mathcal{J}}/\mathbb{F}_{q^n} = \prod_{i=1}^{g}(t-\alpha_i^n)(t-\overline{\alpha_i}^n). \tag{2.41}$$

That is, the α_i in each factor over $\mathbb{F}_q$ is replaced by α_i^n. Note that $P_{\mathcal{J}}/\mathbb{F}_{q^n}$ is always considered as a polynomial over $\mathbb{Z}[t]$.

If instead $\mathcal{C}$ and $\mathcal{J}$ are defined over a number field K, we can consider their reduction modulo a good prime $\mathfrak{p}$ of K. If $\mathcal{J}/K$ is split, then we can also reduce the isogeny that splits it, and see that $\mathcal{J}/\mathbb{F}_q$ is split. In particular, if the Jacobian is geometrically split, then it must split over a finite extension of the number field K, which corresponds to a finite extension of $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, given by $\mathbb{F}_{q^n}$ for some n. Thus, if for all $n \geq 1$ the polynomial $P_{\mathcal{J}}/\mathbb{F}_{q^n}$ is irreducible, then $\mathcal{J}/K$ is geometrically simple.

Computing the characteristic polynomial of Frobenius In the following proposition by a *nice* variety we mean a smooth, projective, geometrically integral variety. Then a *nice curve* is a nice variety of dimension one.

Proposition 2.3.2 ([MZ13])**.** *Let $\mathcal{C}$ be a nice curve of genus g over $\mathbb{F}_q$, and let $\mathcal{J}$ be its Jacobian. Then*

$$P_{\mathcal{J}}(t) = t^{2g} + \sum_{i=1}^{g} a_i t^{2g-i} + \sum_{i=1}^{g} a_{g-i}q^i t^{g-i} + q^g. \tag{2.42}$$

The numbers a_i are determined by the following congruence

$$1 + a_1 t + \cdots a_g t^g \equiv (1-t)(1-qt)Z(\mathcal{C},t) \tag{2.43}$$

$$\equiv (1-t)(1-qt)\exp\left(\sum_{n\geq 1}\#\mathcal{C}(\mathbb{F}_{q^n})\frac{t^n}{n}\right) \pmod{t^{g+1}}. \tag{2.44}$$

Thus the point counts $\#\mathcal{C}(\mathbb{F}_{q^n})$ for $n \leq g$ determine $P_{\mathcal{J}}(t)$ for $\mathcal{J}/\mathbb{F}_q$.

Example 2.3.3. *Let $N_n = \#\mathcal{C}(\mathbb{F}_{q^n})$. For convenience we give the first few terms of $(1-t)(1-qt)\exp\left(\sum_{n\geq 1} N_n \frac{t^n}{n}\right)$:*

$$\begin{aligned} &1 + (-q + N_1 - 1)t + (-qN_1 + q + \frac{1}{2}N_1^2 - N_1 + \frac{1}{2}N_2)t^2 \\ &\quad + (-\frac{1}{2}qN_1^2 + qN_1 - \frac{1}{2}qN_2 + \frac{1}{6}N_1^3 - \frac{1}{2}N_1^2 + \frac{1}{2}N_1N_2 - \frac{1}{2}N_2 + \frac{1}{3}N_3)t^3 \\ &\quad + \cdots . \end{aligned} \tag{2.45}$$

This suffices to compute the characteristic polynomial of Frobenius for a genus 3 curve. The following curve is from the family of genus 3 hyperelliptic curves in [Mes09] with $v = 2, a_1 = 1, a_2 = 2, a_3 = 7$ (with a_i not to be confused with the a_i from zeta functions):

$$y^2 = 2x^8 - 5x^7 - 18x^6 + 50x^5 + 26x^4 - 115x^3 + 18x^2 + 70x - 28. \tag{2.46}$$

The point counts for $q = 11$ are $(N_1, N_2, N_3) = (14, 152, 1322)$. This gives $1 + a_1t + a_2t^2 + a_3t^3 \equiv 1 + 2t + 17t^2 + 28t^3 \pmod{t^4}$. Thus the characteristic polynomial of Frobenius of the Jacobian over $\mathbb{F}_{11}$ is

$$P_{\mathcal{J},11}(t) = t^6 + 2t^5 + 17t^4 + 28t^3 + 17 \cdot 11t^2 + 2 \cdot 11^2 t + 11^3 \tag{2.47}$$

$$= t^6 + 2t^5 + 17t^4 + 28t^3 + 187t^2 + 242t + 1331. \tag{2.48}$$

We implement this in `zeta_function.m` in [Nic18].

2.3.2 Leprévost's method

The following proposition of Leprévost uses this idea to provide a criterion for Jacobians of genus 2 curves to be geometrically simple.

Proposition 2.3.4 ([Lep95])**.** *Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{Q}$ and let $\mathcal{J}$ be its Jacobian. Let p be a prime of good reduction for $\mathcal{C}$ and let $\tilde{\mathcal{C}}$ and $\tilde{\mathcal{J}}$ denote the reductions of $\mathcal{C}$ and $\mathcal{J}$ over the finite field $\mathbb{F}_p$. Let $P_{\tilde{\mathcal{J}},p} \in \mathbb{Z}[x]$ denote the characteristic polynomial of Frobenius of $\tilde{\mathcal{J}}$. If the Galois group of $P_{\tilde{\mathcal{J}}}$ is isomorphic to D_8, the dihedral group on 8 elements, then $\mathcal{J}/\mathbb{Q}$ is geometrically simple.*

Proof. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $P_{\tilde{\mathcal{J}},p}$. Let $L/\mathbb{Q}$ be a Galois closure of K. By assumption $\mathrm{Gal}(L/\mathbb{Q}) = D_8$. If $P_{\tilde{\mathcal{J}},p}$ were reducible, then it would have an irreducible factor of degree at most 3, so the Galois group would have order dividing 6. Therefore $P_{\tilde{\mathcal{J}},p}$ is irreducible, and $[K\colon \mathbb{Q}] = 4$.

Suppose that $\mathcal{J}/\mathbb{Q}$ is geometrically split. Then it must be split over a finite extension $M/\mathbb{Q}$. If M has degree n, then $P_{\tilde{\mathcal{J}},p^n}$ factors into quadratic factors over the residue field $k_M = \mathcal{O}_M/\mathfrak{p}\mathcal{O}_M$, where $\mathfrak{p}$ is a prime of $\mathcal{O}_M$ lying above p. Thus α^n is a root of one of the quadratic factors of $P_{\tilde{\mathcal{J}},p}$, and so defines a degree 1 or 2 subfield of K.

Let $\beta, \bar{\beta}$ denote the other conjugate pair of roots of $P_{\tilde{\mathcal{J}}}$. Then $P_{\tilde{\mathcal{J}},p^n} = (x^2 - A_n x + p^n)(x^2 - B_n x + p^n)$, where $A_n = \alpha^n + \bar{\alpha}^n$ and $B_n = \beta^n + \bar{\beta}^n$. If the split happens over M, then $x^2 - A_n x + p^n \in \mathbb{Z}[x]$, and so $A_n \in \mathbb{Z}$. Note also that $A_1 \notin \mathbb{Q}$ (else the split happens over $\mathbb{Q}$).

We know that $A_1 \in K$ and that $\mathbb{Q}(A_1)$ is fixed under conjugation, while $\mathbb{Q}(\alpha)$ is not. Hence $\mathbb{Q}(A_1) \neq K$, and so must be a degree 2 subfield. Moreover, by the Galois group, K has a unique degree 2 subfield. Hence $\alpha^n \subset \mathbb{Q}(A_1)$. But then α^n is real, and so $p^n = \alpha^n \bar{\alpha}^n = \alpha^{2n}$. Finally, we get $\alpha = \zeta\sqrt{p}$ for some root of unity ζ.

But then $K \subseteq \mathbb{Q}(\zeta, \sqrt{p})$, which is an abelian field. Thus $K/\mathbb{Q}$ is Galois, so $L = K$. But this contradicts $\mathrm{Gal}(L/\mathbb{Q}) = D_8$, which has size 8, not 4. □

2.3.3 Stoll's method for absolute simplicity

Stoll also has a method for proving absolute simplicity of Jacobians of genus 2 curves.

Proposition 2.3.5 ([Sto95])**.** *Let $\mathcal{C}$ be a genus 2 hyperelliptic curve over $\mathbb{Q}$, and let $\mathcal{J}$ be its Jacobian. Let p be a prime of good reduction for $\mathcal{C}$ and let $\tilde{\mathcal{C}}$ and $\tilde{\mathcal{J}}$ be the reductions of $\mathcal{C}$ and $\mathcal{J}$ at p, respectively. Let a_1, a_2 be as in the characteristic polynomial of Frobenius of $\tilde{\mathcal{J}}$ over $\mathbb{F}_p$. Define*

$$\Psi_{\tilde{\mathcal{J}},p}(x) \coloneqq x^4 - \frac{a_2 - 2p}{p}x^3 + \frac{a_1^2 - 2a_2 - 2p}{p}x^2 - \frac{a_2 - 2p}{p}x + 1. \tag{2.49}$$

If $\Psi_{\tilde{\mathcal{J}},p}$ is coprime to the cyclotomic polynomial $\Phi_n(x)$ for $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$, and if $P_{\tilde{\mathcal{J}}}(t)$ is irreducible, then $\mathcal{J}$ is geometrically simple.

Proof. Let q be a power of a good prime p for $\mathcal{C}$. The characteristic polynomial of Frobenius of $\tilde{\mathcal{J}}$ over $\mathbb{F}_q$ is

$$t^4 + a_1 t^3 + a_2 t^2 + a_1 q t + q^2. \tag{2.50}$$

Let $N_r = \#\tilde{\mathcal{C}}(\mathbb{F}_{q^r})$ for $r = 1, 2$. Then

$$a_1 = N_1 - q - 1 \tag{2.51}$$

$$a_2 = \frac{1}{2}(N_2 + a_1^2 - q^2 - 1). \tag{2.52}$$

Suppose that $\mathcal{J}$ is isogenous over $\overline{\mathbb{Q}}$ to a product of elliptic curves E_1, E_2. Then we can replace $\overline{\mathbb{Q}}$ by a finite extension M of $\mathbb{Q}$ (the field of definition of the two elliptic curves and the isogeny). Then consider the characteristic polynomial of Frobenius at a place $\mathfrak{p}$ above a good prime p of $\mathcal{J}$. We find

$$P_{\tilde{\mathcal{J}}/\mathfrak{p}}(t) = P_{\tilde{E_1}/\mathfrak{p}}(t) P_{\tilde{E_2}/\mathfrak{p}}(t). \tag{2.53}$$

Let p^n be the norm of $\mathfrak{p}$, and write

$$\begin{aligned} P_{\tilde{jac}/p}(t) &= t^4 + a_1 t^3 + a_2 t^2 + a_1 p t + p^2 && (2.54)\\ &= (t-\alpha)(t-\bar{\alpha})(t-\beta)(t-\bar{\beta}) && (2.55)\\ &= (t^2 - At + p)(t^2 - Bt + p), && (2.56) \end{aligned}$$

where $A = \alpha + \bar{\alpha}$ and $B = \beta + \bar{\beta}$. The Weil conjectures imply $\alpha\bar{\alpha} = \beta\bar{\beta} = p$.

Also by the Weil conjectures, the characteristic polynomial of Frobenius for $\tilde{\mathcal{J}}/\mathfrak{p}$ satisfies

$$\begin{aligned} P_{\tilde{\mathcal{J}}/\mathfrak{p}}(t) &= (t-\alpha^n)(t-\bar{\alpha}^n)(t-\beta^n)(t-\bar{\beta}^n) && (2.57)\\ &= (t^2 - A_n t + p^n)(t^2 - B_n t + p^n), && (2.58) \end{aligned}$$

where $A_n = \alpha^n + \bar{\alpha}^n$ and $B_n = \beta^n + \bar{\beta}^n$.

Now, if $\mathcal{J}$ factors into a product of elliptic curves over M, then the characteristic polynomials of Frobenius of the elliptic curves must be the factors in the above. This is only possible if A_n and B_n are both rational. Now note that $A + B = a_1$ and $AB = a_2 - 2p$ (by multiplying out the expression above) are both rational. Hence, symmetric polynomials in A, B are also rational. In particular, $A_n + B_n$ is rational (for example $A_2 + B_2 = \alpha^2 + \bar{\alpha}^2 + \beta^2 + \bar{\beta}^2 = A^2 + B^2 - 4p$). Thus A_n and B_n are both rational if and only if $A_n - B_n$ is rational. Let $\Delta_n = (A_n - B_n)^2$. Then A_n and B_n are rational if and only if Δ_n is a square in $\mathbb{Q}$. Note that Δ_n is a symmetric polynomial in A, B, so is in $\mathbb{Q}$.

The result is that $P_{\tilde{\mathcal{J}},p}$ factors only if Δ_n is a square in $\mathbb{Q}$. We can also relate this to Δ_1 by defining $g_n = (A_n - B_n)/(A - B)$, which is a symmetric polynomial in A, B and thus lies in $\mathbb{Q}$. We have $\Delta_n = g_n^2 \Delta_1$. Hence Δ_n is a rational square if and only if Δ_1 is a square or if $\Delta_n = 0$. The first case gives Δ_1 is a square so $P_{\tilde{\mathcal{J}},p}$ is already reducible. The second case gives $A_n = B_n$. Hence the polynomials $x^2 - A_n x + p^n$ and $x^2 - B_n x + p^n$ are equal, so have the same roots. In particular, $\alpha^n = \beta^n$ or $\alpha^n = \bar{\beta}^n$. Hence $(\alpha/\beta)^n = 1$ or $(\alpha/\bar{\beta})^n = 1$. Thus an nth root of unity satisfies

$$(x - \alpha/\beta)(x - \bar{\alpha}/\beta)(x - \alpha/\bar{\beta})(x - \bar{\alpha}/\bar{\beta}), \tag{2.59}$$

which simplifies to $\Psi_{\tilde{J},p}(x)$. This is possible if and only if the nth cyclotomic polynomial $\Phi_n(x)$ divides the polynomial. For degree reasons, this implies n is in the set $\{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. □

2.3.4 Cassels and Flynn's criteria

In the other direction, Cassels and Flynn provide the following sufficient conditions for the Jacobian of a genus 2 curve to be split.

Proposition 2.3.6 ([CF96, Theorem 14.1.1])**.** *Let $\mathcal{C}$ be a genus 2 curve. The following properties of $\mathcal{C}$ are equivalent:*

(i) the curve is birational to

$$y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0, \tag{2.60}$$

containing only even-degree terms in x;

(ii) the curve is birational to

$$y^2 = G_1(x)G_2(x)G_3(x), \tag{2.61}$$

where the quadratics $G_i(x)$ are linearly dependent;

(iii) the curve is birational to

$$y^2 = x(x-1)(x-a)(x-b)(x-ab), \tag{2.62}$$

for some a, b.

If one, and thus all, conditions is satisfied, then the Jacobian of $\mathcal{C}$ is split.

Remark 2.3.7. *Going from (ii) to (i) may require a quadratic extension. Going from (ii) to (iii) requires that we split two of the G_i. Going from (i) to (ii) may require a degree six extension, since we need $c(x^2)$ to split, where* $\deg c = 3$*. Going from (iii) to (ii) is rational.*

2.4 Criterion for simplicity of Jacobians

We are interested in finding torsion points on Jacobians of curves, and also in whether the Jacobians we find are geometrically simple or geometrically split. Given an N-torsion point on a Jacobian $\mathcal{J}_1$ and an M-torsion point on a Jacobian $\mathcal{J}_2$, we can

often glue $\mathcal{J}_1$ and $\mathcal{J}_2$ together to form the split abelian variety $\mathcal{J}_1 \times \mathcal{J}_2$ with an NM-torsion point. When we find an N-torsion point on the Jacobian of a genus g curve, therefore, we want to either rule this out (if it is geometrically simple), or understand the splitting.

Remark 2.4.1. *Note that even in the situation of $\mathcal{J}_1, \ldots, \mathcal{J}_r$ with $N_1, \ldots, N_r$ torsion points, respectively, it is not always possible to define $\mathcal{J}_1 \times \cdots \times \mathcal{J}_r$ as a Jacobian of a curve over the same field. The situation for genus 2 and 3 is well-described in [HLP00], and developed further in [How14]. For example, even though there is an elliptic curve with a 7-torsion point and an elliptic curve with an 8-torsion point, it is not yet known if there is a Jacobian of a genus 2 curve with a 56-torsion point (see [How14]).*

The papers [PP12a], [PZP13], [Pla14], [Kro15], [Kro17], [Mes09] [Lep95] all discuss the problem of showing that a Jacobian of a curve is simple. All except for [Mes09] deal with dimension 2 Jacobians.

The criteria from Section 2.3 apply to Jacobians of genus 2 curves only, while we are interested in Jacobians of higher genus curves. We now give a new criterion for a given Jacobian of a curve to be simple, using the characteristic polynomial of Frobenius of the Jacobian of a curve. Similar arguments appear in e.g. [HZ02] and [MZ13], but this criterion doesn't seem to be explicitly stated anywhere. Its main advantage is that it applies to curves of higher genus, so that we can show some of the genus 3 and genus 4 curves we find have geometrically simple Jacobians.

Proposition 2.4.2. *Let $\mathcal{C}/\mathbb{Q}$ be a curve of genus g and let $\mathcal{J}$ be its Jacobian. Let p be a prime of good reduction for $\mathcal{C}$ and let $\tilde{\mathcal{C}}$ and $\tilde{\mathcal{J}}$ denote the reduction of $\mathcal{C}$ and $\mathcal{J}$ modulo p, respectively. Let $P_{\tilde{\mathcal{J}}}(t)$ be the characteristic polynomial of Frobenius of $\tilde{\mathcal{J}}$. Suppose that $P_{\tilde{\mathcal{J}}}$ is irreducible; let α be a root of $P_{\tilde{\mathcal{J}}}$, and let $K = \mathbb{Q}(\alpha)$. Suppose all strict subfields of K are totally real. Suppose further that $t^{2n} - p^n$ and $P_{\tilde{\mathcal{J}}}(t)$ are coprime for all n with $\deg \Phi_n(t) \leq 2g$, where $\Phi_n(t)$ is the nth cyclotomic polynomial. Then $\mathcal{J}$ is geometrically simple.*

Proof. Let $P_{\tilde{\mathcal{J}},n}(t)$ be the characteristic polynomial of Frobenius for $\tilde{\mathcal{J}}$ over $\mathbb{F}_{p^n}$. It suffices to show that $P_{\tilde{\mathcal{J}},n}(t)$ is irreducible for each $n \geq 1$. For, if $\mathcal{J}$ splits into a product of two abelian varieties over $\bar{\mathbb{Q}}$, then it splits over a finite, say degree n, extension of $\mathbb{Q}$, and then $P_{\tilde{\mathcal{J}},n}$ is reducible.

Recall from the Weil conjectures that if the roots of $P_{\tilde{\mathcal{J}}}$ are $\alpha_1, \bar{\alpha}_1, \ldots, \alpha_g, \bar{\alpha}_g$, then the roots of $P_{\tilde{\mathcal{J}},n}(t)$ are $\alpha_1^n, \bar{\alpha}_1^n, \ldots, \alpha_g^n, \bar{\alpha}_g^n$. For a polynomial $f(t) \in \mathbb{Q}[t]$ with root

β, we have $[\mathbb{Q}(\beta)\colon \mathbb{Q}] = \deg f_1(t)$, where $f_1(t)$ is an irreducible factor of $f(t)$ such that $f_1(\beta) = 0$. It always holds that $\mathbb{Q}(\alpha^n) \subseteq \mathbb{Q}(\alpha)$, and equality holds if and only if $P_{\tilde{\mathcal{J}},n}(t)$ is irreducible.

Thus, for $\tilde{\mathcal{J}}/\mathbb{F}_{p^n}$ to be split, we must have $\mathbb{Q}(\alpha^n) \neq \mathbb{Q}(\alpha)$. Suppose this holds. By assumption, all strict subfields of $\mathbb{Q}(\alpha)$ are real, and hence α^n is real. By the Weil conjectures, $\alpha\bar{\alpha} = p$, and hence $p^n = \alpha^n\bar{\alpha}^n = \alpha^{2n}$. Thus α is a common root of $t^{2n} - p^n$ and $P_{\tilde{\mathcal{J}}}(t)$. Moreover, α^2/p is an nth root of unity lying in K. We can thus restrict to the values of n for which K could have an nth root of unity. Since K has degree $2g$, this is precisely $\{n\colon \deg \Phi_n \leq \deg P_{\tilde{\mathcal{J}}}\}$. This contradicts the assumption that $t^{2n} - p^n$ and $P_{\tilde{\mathcal{J}}}$ are coprime for all these n. □

Remark 2.4.3. *In practice, using the criterion at a range of small primes, we can often show that Jacobians of curves of genus 2, 3 or 4 are simple. Note that if the criterion does not hold, this does not imply that the Jacobian is split.*

We provide MAGMA code in the file `zeta_function.m` in [Nic18].

Chapter 3

Large rational torsion

3.1 Torsion on Jacobians of hyperelliptic curves

We now move on to finding large rational torsion points on Jacobians of curves of higher genus. Let $\mathcal{C}$ be a curve over a number field K and let $\mathcal{J}$ be its Jacobian. For a positive integer N, we say that a point $D \in \mathcal{J}(K)$ is an *N-torsion point* if $ND \sim 0$ and we say it has *order* N if N is the smallest positive integer with this property.

We introduce the notation $\mathcal{J}_{\text{simple}}(g, N), \mathcal{J}_{\text{split}}(g, N), \mathcal{J}_{\text{either}}(g, N)$ to denote the moduli spaces of Jacobians of genus g curves with a rational torsion point of order N that are, respectively, geometrically simple, geometrically split, or either geometrically simple or geometrically split.

Mazur's theorem ([Maz77]) gives a complete description of the orders that can occur for points on elliptic curves over $\mathbb{Q}$. The only possible orders are $2 \leq N \leq 10$ and $N = 12$. For each order, there is also a known family of elliptic curves that have a point of this order.

In higher genus this problem has only been studied from the direction of producing torsion points, as opposed to showing that a particular integer N cannot occur as the order of a point of a Jacobian of a curve of genus at least 2. The problem naturally divides into geometrically split Jacobians and geometrically simple Jacobians.

In the geometrically split case, one can try and find Jacobians of higher genus curves that have Jacobians of lower genus curves as factors. In genus 2 and 3 the main contribution is [HLP00], which contains many curves of genus 2 and 3 with torsion subgroups of large order.

We mainly study the geometrically simple case. In this chapter we study the values of N that can occur as the order of a rational divisor on a geometrically simple Jacobian of a hyperelliptic curve of genus at least 2. This is a well-studied problem, so we first summarise what is known.

3.1.1 What is known already

We first summarise which torsion orders are known to occur, and in which papers to find them. The following is intended only for reference, and the reader should not feel the need to read it all. Tables 3.1, 3.2 and 3.3 summarise the discussion.

Torsion points on curves of fixed genus Flynn studies genus 2 curves with torsion points in [Fly90a] and uses 'degenerate addition' to find families in $\mathcal{J}_{\text{either}}(2, N)$ for $N = 11, 13$. Leprévost finds 1-parameter families in $\mathcal{J}_{\text{either}}(2, N)$ for $N = 17, 19, 21$, though he does not discuss the simplicity of their Jacobians ([Lep92]). Ogawa finds a 1-parameter family in $\mathcal{J}_{\text{either}}(2, 23)$ ([Oga94]).

In [Lep95], Leprévost introduces his method for determining whether a Jacobian of a genus 2 curve is geometrically simple (Proposition 2.3.4), and finds points in $\mathcal{J}_{\text{simple}}(2, N)$ for $N = 22, 23, 24, 26, 29$. He also finds points in $\mathcal{J}_{\text{split}}(2, N)$ for $N = 21, 24, 25, 27$.

Remark 3.1.1. *Note that although Leprévost showed the Jacobian of the genus 2 curve with an order 25 point is simple over $\mathbb{Q}$, he did not show that the Jacobian was geometrically simple; subsequently, Platonov et al. showed the Jacobian was geometrically split [PZP13].*

Bernard et al. enlarged Flynn's 1-parameter family of Jacobians of genus 2 curves with an order 11 point to find 18 curves that are pairwise not isomorphic over $\overline{\mathbb{Q}}$ and also not $\overline{\mathbb{Q}}$-isomorphic to any curve in Flynn's family whose Jacobians have a point of order 11 ([BLP09]).

Platonov and Petrunin find points in $\mathcal{J}_{\text{simple}}(2, N)$ for $N = 14, 18, 28, 33$ and points in $\mathcal{J}_{\text{split}}(2, N)$ for $N = 28, 36, 48$ ([PZP13]).

Elkies has a website [Elk18] with some genus 2 curves whose Jacobians have torsion points of large order. He finds points in $\mathcal{J}_{\text{simple}}(2, N)$ for $N = 34, 39, 40$ and a family of solutions in $\mathcal{J}_{\text{simple}}(2, 32)$, though he doesn't write down the family.

Remark 3.1.2. *Elkies mentions an unpublished preprint by Leprévost in which Leprévost obtains an infinite family of genus 2 curves whose Jacobians have a point of order 30, but we have been unable to see this family.*

Howe studies mainly geometrically split Jacobians in [How14]. He finds a family of genus 2 curves parametrised by a rank-2 elliptic curve whose Jacobians are geometrically split with a point of order 48. This comes from specialising a family with a point

of order 24. He also finds a single point in $\mathcal{J}_{\text{split}}(2,70)$, a single point in $\mathcal{J}_{\text{simple}}(2,27)$, as well as several points in $\mathcal{J}_{\text{either}}(2,N)$ for $N=27,28$ and a single point in $\mathcal{J}_{\text{simple}}(2,39)$.

In the split case in genus 2, Howe et al. find a family of genus 2 curves parametrised by $\mathbb{P}^2$ whose Jacobians have a point of order 24; a family parametrised by a positive rank elliptic curve whose Jacobians have a point of order 35; a family parametrised by a positive rank elliptic surface whose Jacobians have a point of order 40; a family parametrised by a positive rank elliptic curve whose Jacobians have a point of order 45; a family parametrised by a positive rank elliptic curve whose Jacobians have a point of order 60; and a single curve whose Jacobian has a point of order 63 ([HLP00]).

We now discuss genus 3 and 4. Flynn finds a family of solutions in $\mathcal{J}_{\text{either}}(4,29)$ ([Fly90a]). Kronberg finds single points in $\mathcal{J}_{\text{either}}(3,41)$ and $\mathcal{J}_{\text{either}}(4,71)$ ([Kro15]). I checked the Jacobians are geometrically simple using Proposition 2.4.2.

Howe et al. also study geometrically split Jacobians of genus 3 curves. They find a family of genus 3 hyperelliptic curves parametrised by a positive rank elliptic curve whose Jacobians have a point of order N for $N=24,30$ ([HLP00]).

Torsion growing with genus A variant of this problem is to find families of curves with torsion points of order depending on the genus, g. Here we summarise the known families.

Flynn introduced the idea in ([Fly91]) by finding 1-parameter families of solutions in $\mathcal{J}_{\text{either}}(g,N)$, depending on the genus, for all $N\in[2g,3g]$, where $g\geq 1$. He also found a 1-parameter family of solutions in $\mathcal{J}_{\text{either}}(g,2g^2+2g+1)$. When $g\geq 2$ is even he found 1-parameter families of solutions in $\mathcal{J}_{\text{either}}(g,N)$ for all $N\in[g^2+2g+1,g^2+3g+1]$. All of these curves are hyperelliptic.

Leprévost extended this by finding a 1-parameter family of solutions in $\mathcal{J}_{\text{either}}(g,2g^2+2g+1)$ and $\mathcal{J}_{\text{either}}(g,2g^2+3g+1)$ ([Lep92]). The first family was already contained in [Fly91], but Leprévost studied it further. In [Lep97], Leprévost found a 1-parameter family of solutions in $\mathcal{J}_{\text{either}}(g,2g(2g+1))$; the curves are hyperelliptic. When $g\geq 2$ is even, he found a single point in $\mathcal{J}_{\text{either}}(g,2g^2+5g+5)$. If $g\geq 2$ and $g\equiv 1 \pmod 4$, he found a single point in $\mathcal{J}_{\text{either}}(g,(2g^2+5g+5)/4)$. And if $g\geq 2$ and $g\equiv 3 \pmod 4$ he found a single point in $\mathcal{J}_{\text{either}}(g,(2g^2+5g+5)/2)$. All of these are Jacobians of hyperelliptic curves.

Remark 3.1.3. *We verified using Proposition 2.4.2 that, when $g=4$, one of the curves in Leprévost's family with an order $2g(2g+1)$ point is geometrically simple.*

In [DS18], Daowsud and Schmidt found an infinite family of solutions in $\mathcal{J}_{\text{either}}(g,11)$ for each $g\geq 2$; their method uses continued fractions.

3.1.2 Summary of results

Tables 3.1, 3.2 and 3.3 summarise the discussion above, including the families of curves growing with genus. We also include the curves that we found using the methods described later in this chapter. To simplify the table, if there is an N-torsion point later in the table, and if M divides N then we sometimes write $*$ for the entry for M in the table. We write † to denote that the paper contains a parametrised family of curves, but this is not exhaustive: if an entry lacks the † the paper may still contain a parametrised family. The unverified column in the tables means there is a known curve of that genus whose Jacobian contains an order N point, but the Jacobian has not been shown to be geometrically simple or geometrically split.

In genus 2, we provide the first known example of a hyperelliptic curve with geometrically simple Jacobian having a point of order 25 (Example 3.1.7). Depending on whether the family mentioned by Elkies in Remark 3.1.2 consists of geometrically simple Jacobians, our example of geometrically simple Jacobian of a genus 2 curve with a point of order 30 may also be new (Example 3.1.8).

3.1.3 Original method

Flynn ([Fly90a]) introduced the following idea to find large order torsion points on Jacobians of curves. Suppose a Jacobian has the rational divisors $D_1, \ldots, D_n \in \mathcal{J}(K)$, satisfying the relations

$$\sum_{i=1}^{n} a_{ij} D_i \sim 0, \tag{3.1}$$

for $i = 1, \ldots, m$, where $a_{ij} \in \mathbb{Z}$. We can express this in matrices as $AD \sim 0$, where $A_{ij} = a_{ij}$, and $D = (D_1, \ldots, D_n)^T$. Multiplying by the adjoint of A, we find that $(\det A) I_n D \sim 0$, and so $(\det A) D_i \sim 0$ for all i. Thus each D_i has order dividing $\det A$. We refer to the matrix A as a *matrix of relations* for the divisors $D_1, \ldots, D_n$.

It is easiest to first consider the case where the curve has a single point at infinity ∞ and where each $D_i = P_i - \infty$ for an affine rational point $P_i \in \mathcal{C}$. In this case, each relation (3.1) is of the form

$$\sum_{i=1}^{n} a_i P_i \sim \sum_{i=1}^{n} a_i \infty. \tag{3.2}$$

This means there is a function in $\mathscr{L}\left(\left(\sum_{i=1}^{n} a_i\right)\infty\right)$. The space $\mathscr{L}(n\infty)$ is generated by functions of the form $A(x) + B(x)y$ where $2\deg A \leq n$ and $\deg f + 2\deg B \leq n$.

N	Geometrically simple	Geometrically split	Unverified
2	*	*	
3	*	*	
4	*	*	
5	*	*	
6	*		[Fly90a]
7	*		
8	*		
9	*		[Fly90a]
10	*		[Fly90a]
11	*		[Fly90a] [BLP09] [DS18]
12	*		
13	3.1.6		[Fly90a]
14	[PZP13] 3.1.6		
15	*		
16	3.1.12		
17	*		[Lep92]
18	[PZP13] 3.1.6		
19	3.1.6		[Lep92]
20	3.1.6		[Lep97]
21	3.1.6	[Lep95]	[Lep92]
22	[Lep95] 3.1.12		
23	[Lep95] 3.1.12		[Oga94]
24	[Lep95] 3.1.6	[Lep95] [HLP00] [How14]	
25	3.1.6	[Lep95]	
26	[Lep95] 3.1.12		
27	[How14] 3.1.12	[Lep95]	[How14]
28	[PZP13] 3.1.12	[PZP13]	[How14]
29	[Lep95] 3.3.4		
30	3.1.12		
31			
32	[Elk18] 3.3.10		
33	[PZP13] 3.3.4		
34	[Elk18] 3.1.12		
35		[HLP00]	
36		[PZP13]	
37			
38			
39	[Elk18] [How14] 3.3.4		
40	[Elk18] 3.3.12	[HLP00]	
45		[HLP00]	
48		[PZP13] [How14]	
60		[HLP00]	
63		[HLP00]	
70		[How14]	

Table 3.1: The known orders of torsion points of Jacobians of genus 2 curves.

N	Geometrically simple	Geometrically split	Unverified
11			[DS18] †
15	3.1.12		
19			[Lep97]
22	3.3.16		
24		[HLP00]	
25	3.1.6 †		[Fly91] †
26	3.1.6 †		
27	3.1.6 †		
28	3.1.6 †		[Lep97] †
29	3.1.12		
30	3.1.6	[HLP00]	
31	3.1.12		
32	3.1.6 †		
33	3.1.6		
34	3.1.6		
35	3.1.6		
36	3.1.12		
37	3.1.6 3.3.16		
38	3.1.6		
39	3.1.12		
40	3.1.12		
41	[Kro15] 3.1.6		
42	3.1.6 †		[Lep97] †
43	3.1.6		
44	3.1.12		
48	3.1.6		
49	3.1.6		
50	3.1.6		
52	3.3.10		
54	3.1.12		
56	3.1.12		
64	3.3.4		
65	3.3.4		
72	3.3.4		
91	3.3.4		

Table 3.2: The known orders of torsion points of Jacobians of hyperelliptic curves of genus 3.

N	Geometrically simple	Unverified
8-12		[Fly91] (†)
19	3.3.2	
25	*	[Fly91]
26	*	[Fly91]
27	*	[Fly91]
28	3.3.2	[Fly91] (†)
29	*	[Fly91] (†)
32	3.1.12	
33	3.1.12	
34	3.3.2	
35	3.1.12	
40	3.3.2	
41	3.1.6	[Fly91] (†)
42	3.1.6	
43	3.1.6	
44	3.1.6	
45	3.1.12	[Lep97] (†)
46	3.1.12	
47	3.1.12	
48	3.1.12	
49	3.1.12	
50	3.1.12	
51	3.1.12	
52	3.1.12	
53	3.1.12	
54	3.1.12	
55	3.1.12	
57	3.1.12	[Lep97] (†)
58	3.1.6	
59	3.1.12	
60	3.1.12	
61	3.1.12	
62	3.1.12	
63	3.1.12	
65	3.1.6	
66	3.1.6	
67	3.1.12	
68	3.1.12	
71	[Kro15]	
72	[Lep97] (†) 3.1.12	
74	3.1.12	
82	3.1.6	
88	3.1.12	

Table 3.3: The known orders of torsion points of Jacobians of hyperelliptic curves of genus 4.

Since $\infty \in \mathcal{C}(K)$, we have $y^2 = f(x)$ with $\deg f = 2g+1$. Thus $2\deg A \leq n$ and $2\deg B \leq n - 2g - 1$.

The following lemma relates this to equations involving polynomials.

Lemma 3.1.4. *Let $\mathcal{C}$ be an odd degree hyperelliptic curve with equation $y^2 = f(x)$. Let $P_1, \ldots, P_n \in \mathcal{C}(K)$, and let x_i denote the x-coordinate of P_i. If there are nonnegative integers $a_1, \ldots, a_n$ such that $\sum_{i=1}^n a_i(P_i - \infty) \sim 0$, then there are polynomials $A(x), B(x)$ such that*

$$A(x)^2 - B(x)^2 f(x) = \lambda \prod_{i=1}^{n} (x - x_i)^{a_i}. \tag{3.3}$$

Conversely, if there are polynomials $A(x), B(x)$ satisfying the above equation, then there are points $P_i' \in \mathcal{C}$ such that $\sum_{i=1}^n a_i P_i' \sim 0$, and $x(P_i') = x_i$.

Proof. Suppose $\operatorname{div} g = \sum_{i=1}^n a_i(P_i - \infty)$ for some function $g(x,y) \in K(\mathcal{C})$. Then $g \in \mathscr{L}(N\infty)$, where $N = \sum_{i=1}^n a_i$. This space has basis $\{A(x) + B(x)y \colon 2\deg A \leq N, 2\deg B + \deg f \leq N\}$. The affine intersection of $g(x,y) = 0$ and $y^2 = f(x)$ is the divisor $\sum_{i=1}^n a_i P_i$. Since all a_i are nonnegative, this imposes zeroes of the function g along $\mathcal{C}$ of multiplicity a_i at P_i. Thus the resultant of $g(x,y)$ and $y^2 - f(x)$ with respect to y must be

$$\begin{aligned} \operatorname{Res}_y(y^2 - f(x), A(x) + B(x)y) &= A(x)^2 - B(x)^2 f(x) && (3.4) \\ &= \lambda \prod_{i=1}^{n} (x - x_i)^{a_i}, && (3.5) \end{aligned}$$

where $x_i = x(P_i)$.

Conversely, suppose $A(x)^2 - B(x)^2 f(x) = \lambda \prod_{i=1}^n (x - x_i)^{a_i}$. This is the resultant of $g(x,y) = A(x) + B(x)y$ with $y^2 - f(x)$, and thus defines the intersections of $g(x,y)$ with $\mathcal{C}$. But this only describes the x-coordinates of the intersections, so the point corresponding to $(x - x_i)^{a_i}$ is either P_i or $\iota(P_i)$. Thus the intersection of $g(x,y) = 0$ with $\mathcal{C}$ is $\sum_{i=1}^n a_i P_i'$. The intersection of $g(x,y) = 0$ and $\mathcal{C}$ in the other coordinate chart is a multiple of ∞ and by degree considerations it must be that $\operatorname{div} g = \sum_{i=1}^n a_i P_i' - (\sum_{i=1}^n a_i)\infty$. □

To get a matrix relation with the divisors $D_i = P_i - \infty$, we need each relation in terms of D_i, as opposed to $\iota(D_i) = \iota(P_i) - \infty$. Whenever a solution to $A(x)^2 - B(x)^2 f(x) = \lambda \prod_{i=1}^n (x - x_i)^{a_i}$ gives rise to a relation in which $\iota(D_i)$ occurs, we just add

a multiple of $D_i + \iota(D_i) = \mathrm{div}(x - x_i)$ to replace the relation with D_i. This replaces $a_i\iota(D_i)$ with $-a_i D_i$. Thus a solution to the resultant equation gives

$$\sum_{i=1}^{n} a_i' D_i \sim 0, \tag{3.6}$$

where $|a_i'| = a_i$.

This basic idea is common to the large torsion literature, originating in [Fly90a] and further developed by Leprévost and others. The first two methods we describe are generalisations of these approaches in which we automate the search for large order torsion points. This lets us search over a large number of relation matrices in genus 2, 3 and 4. In principle we could apply these first two methods to hyperelliptic curves of any genus to find large order torsion points.

3.1.4 The difference of squares method

Consider the 2×2 matrix of relations

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}. \tag{3.7}$$

Assuming $p + q, r + s \leq 2g + 2$, this implies the simultaneous equations

$$\begin{aligned} A(x)^2 - f(x) &= \lambda x^p (x-1)^q \\ B(x)^2 - f(x) &= \mu x^r (x-1)^s, \end{aligned} \tag{3.8}$$

where $\deg A, \deg B \leq g + 1$. There is no multiple on $f(x)$, since we took the degrees of the right hand side small enough.

Subtracting the second equation from the first, we find

$$A(x)^2 - B(x)^2 = \lambda x^p (x-1)^q - \mu x^r (x-1)^s. \tag{3.9}$$

Factorising the difference of squares on the left hand side, we have

$$(A(x) + B(x))(A(x) - B(x)) = \lambda x^p (x-1)^q - \mu x^r (x-1)^s. \tag{3.10}$$

If we factor the right hand side into a product $G(x)H(x)$, we get:

$$\begin{aligned} A(x) &= \frac{1}{2}(G(x) + H(x)) \\ B(x) &= \frac{1}{2}(G(x) - H(x)). \end{aligned} \tag{3.11}$$

This gives a solution to the original problem only if $\deg A, \deg B \leq g + 1$.

The parameters λ, μ For each matrix of relations we can reduce the pair of parameters λ, μ to a single parameter. Assuming $2g+1 \leq p+q \leq r+s \leq 2g+2$, there are two cases: $r+s = 2g+1$, or $r+s = 2g+2$.

If $r+s = 2g+1$, then also $p+q = 2g+1$, so comparing the x^{2g+1} coefficients of both equations, we must have $\lambda = \mu$, and we are left to solve the equivalent equations

$$\begin{aligned} A(x)^2 - f(x) &= tx^p(x-1)^q \\ B(x)^2 - f(x) &= tx^r(x-1)^s. \end{aligned} \tag{3.12}$$

If $r+s = 2g+2$, we have $\deg B = g+1$ and $\mu = B_{g+1}^2$. Dividing both equations by μ and relabelling, we are left with the equivalent equations

$$\begin{aligned} A(x)^2 - f(x) &= tx^p(x-1)^q \\ B(x)^2 - f(x) &= x^r(x-1)^s. \end{aligned} \tag{3.13}$$

This applies for both $p+q = 2g+1$ and $p+q = 2g+2$.

An algorithm We now describe an algorithm to find curves of any genus whose Jacobians have large order torsion points.

Let

$$R(x) = \begin{cases} tx^p(x-1)^q - tx^r(x-1)^s, \text{ if } r+s = 2g+1 \\ tx^p(x-1)^q - x^r(x-1)^s, \text{ if } r+s = 2g+2 \end{cases} \tag{3.14}$$

For each factorisation $R(x) = G_1(x)G_2(x)$, let

$$\begin{aligned} A(x) &= \frac{1}{2}(G_1(x) + G_2(x)) \\ B(x) &= \frac{1}{2}(G_1(x) - G_2(x)), \end{aligned} \tag{3.15}$$

and check if this corresponds to a solution to (3.8).

My main contributions here are the following. Firstly, it often happens that there are several factorisations of the right hand side into a product; we check all of them. Secondly, the right hand side may not factor into products that give $\deg A, \deg B$ of the correct degree. In this case, we search for rational t up to bounded height for which $R(x)$ factors further. Finally, we automate this process by searching over all possible matrix relations with MAGMA.

Example 3.1.5. *The genus 3 curve*

$$y^2 = -8x^7 + 201/4x^6 - 169/2x^5 + 299/4x^4 - 39x^3 + 51/4x^2 - 5/2x + 1/4 \tag{3.16}$$

has an order 41 point on its Jacobian. This is distinct from Kronberg's example ([Kro15]).

This comes from considering the matrix

$$\begin{pmatrix} 6 & 1 \\ 1 & 7 \end{pmatrix}, \tag{3.17}$$

which gives the difference of squares equation

$$(A+B)(A-B) = x(x-1)(tx^5 - (x-1)^6), \tag{3.18}$$

and we need $\deg A \leq 3, \deg B = 4$. *This is impossible for general* t *as the sextic factor is irreducible over* $\mathbb{Q}(t)$. *After point searching we find that with* $t = 8$ *the right hand side factors as*

$$-x(x-1)(x^2+1)(x^4 - 14x^3 + 14x^2 - 6x + 1). \tag{3.19}$$

Putting $G_1 = -x(x-1)(x^2+1)$ *and* $G_2 = x^4 - 14x^3 + 14x^2 - 6x + 1$, *and letting* $A(x) = (G_1 + G_2)/2$, *we find* $f(x) = A^2 - 8x^6(x-1)$.

Computation 3.1.6. *This method finds rational points in* $\mathcal{J}_{\text{simple}}(2, N)$ *for all* N *in the set*

$$\{14, 16, 18, 19, 20, 21, 24, 25, 26, 30, 34\}; \tag{3.20}$$

rational points in $\mathcal{J}_{\text{simple}}(3, N)$ *for all* N *in the set*

$$\{26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 41, 42, 43, 48, 49, 50\}; \tag{3.21}$$

and rational points in $\mathcal{J}_{\text{simple}}(4, N)$ *for all* N *in the set*

$$\begin{gathered} \{25, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, \\ 54, 55, 57, 58, 59, 60, 61, 62, 65, 66, 72, 82\}. \end{gathered} \tag{3.22}$$

Example 3.1.7. *There was previously no known point in* $\mathcal{J}_{\text{simple}}(2, 25)$, *which shows the effectiveness of the method. Leprévost's curve with an order 25 point is* $y^2 = f_{25,1}(x)$ *while ours is* $y^2 = f_{25,2}(x)$, *where*

$$f_{25,1}(x) = 36x^6 - 156x^5 + 241x^4 - 192x^3 + 102x^2 - 36x + 9 \tag{3.23}$$

$$f_{25,2}(x) = 36x^5 + 100x^4 - 300x^3 + 165x^2 + 90x + 9. \tag{3.24}$$

Leprévost's curve has geometrically reducible Jacobian ([PZP13]). We can show that the Jacobian of $y^2 = f_{25,2}(x)$ *has geometrically simple Jacobian either with our method (Proposition 2.4.2) or Leprévost's method (Proposition 2.3.4), but with* $p = 11$.

Example 3.1.8. *Let*

$$f_{30} = x^6 - 16/3x^5 + 70/9x^4 + 131/27x^2 + 16/27x + 64/81. \tag{3.25}$$

The Jacobian of the curve $y^2 = f_{30}(x)$ is geometrically simple and has a point of order 30.

Remark 3.1.9. *For each matrix of relations, the possible torsion orders are the determinants of the matrices whose entries equal the original matrix up to sign. This motivates searching over all relation matrices.*

Remark 3.1.10. *If there is such a t for which $R(x)$ factors further, there is sometimes still a parametrised family of solutions.*

The Jacobians of the following curves lie in $\mathcal{J}_{\text{simple}}(4, 82)$:

$$\begin{aligned} y^2 = &-58/3x^9 + 4777/36x^8 - 2840/9x^7 + 394x^6 - 842/3x^5 \\ &+ 967/9x^4 - 40/3x^3 - 4x^2 + 8/9x + 1/9 \end{aligned} \tag{3.26}$$

$$\begin{aligned} y^2 = &-70/3x^9 + 7345/36x^8 - 2216/3x^7 + 13598/9x^6 - 17714/9x^5 \\ &+ 15445/9x^4 - 9080/9x^3 + 3484/9x^2 - 88x + 9. \end{aligned} \tag{3.27}$$

The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(4, 55)$:

$$\begin{aligned} y^2 = &-1/9x^9 + 79/81x^8 - 205/81x^7 + 13/3x^6 - 403/81x^5 + 277/81x^4 \\ &- 17/9x^3 + 14/9x^2 - x + 1/4 \end{aligned} \tag{3.28}$$

Example 3.1.11. *The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(2, 34)$:*

$$y^2 = -144x^5 + 793x^4 - 280x^3 + 312x^2 + 32x + 16. \tag{3.29}$$

It is isomorphic to one of Elkies' two examples ([Elk18]).

The Jacobians of the following curves lie in $\mathcal{J}_{\text{simple}}(3, 43)$:

$$y^2 = -16x^7 + 409/4x^6 - 275x^5 + 399x^4 - 334x^3 + 160x^2 - 40x + 4 \tag{3.30}$$

$$y^2 = -16x^7 + 393/4x^6 - 237x^5 + 309x^4 - 242x^3 + 116x^2 - 32x + 4. \tag{3.31}$$

3.1.5 The difference of squares method II

Leprévost generalised this method in [Lep92] to allow $r + s = 2g + 3, 2g + 4$. The resultant equations are then

$$\begin{aligned} A(x)^2 - f(x) &= \lambda x^p (x-1)^q \\ B(x)^2 - C(x)^2 f(x) &= \mu x^r (x-1)^s, \end{aligned} \tag{3.32}$$

where $\deg C \leq 1$. Leprévost writes $C(x) = x - c$. As in the previous section, there are two cases, depending on whether or not $\{p+q, r+s\}$ contains an even number. As before, we can reduce to

$$(\lambda, \mu) = \begin{cases} (1, t), & \text{if } p+q \text{ is even} \\ (t, 1), & \text{if } r+s \text{ is even} \\ (t, t), & \text{otherwise.} \end{cases} \tag{3.33}$$

Leprévost's approach is to use the first equation to substitute for $f(x)$ in the second equation. This gives the difference of squares equation

$$(B(x) + A(x)C(x))(B(x) - A(x)C(x)) = \mu x^r (x-1)^s - \lambda x^p (x-1)^q C(x)^2. \tag{3.34}$$

As before, for each factorisation $G_1(x)G_2(x)$ of the right hand side, we put

$$\begin{aligned} A(x)C(x) &= \frac{1}{2}(G_1(x) - G_2(x)) \\ B(x) &= \frac{1}{2}(G_1(x) + G_2(x)). \end{aligned} \tag{3.35}$$

This time, however, we need to impose that $C(x)$ divides $G_1(x) - G_2(x)$. Leprévost uses this idea to find a 1-parameter family of genus 2 curves whose Jacobians have an order 19 point ([Lep92]). He takes care to solve the system for general c, preserving a 1-parameter family.

But different matrices of relations can give complicated systems to solve, so instead we just search for small c such that the factorisation $G_1(x)G_2(x)$ gives $B(x)$ and $A(x)C(x)$ of the correct degrees. Since $C(x) = x - c$ is linear, the condition that $C(x)$ divides $G_1(x) - G_2(x)$ is equivalent to $G_1(c) - G_2(c) = 0$. For any factorisation $G_1(x)G_2(x)$, we find that $G_1(c) + G_2(c)$ is linear in t, so we can choose t such that this holds.

The following computation is the result of applying this algorithm to all matrices of relations with $2g+1 \leq p+q \leq 2g+2$ and $2g+3 \leq r+s \leq 2g+4$ and c bounded in height by 200.

Computation 3.1.12. *This method finds rational points in $\mathcal{J}_{\text{simple}}(2, N)$ for all N in the set*

$$\{16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 30, 34\}; \tag{3.36}$$

rational points in $\mathcal{J}_{\text{simple}}(3, N)$ for all N in the set

$$\{15, 27, 29, 31, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 49, 54, 56\}; \tag{3.37}$$

and rational points in $\mathcal{J}_{\text{simple}}(4, N)$ *for all* N *in the set*

$$\begin{aligned}\{&32, 33, 35, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55,\\ &57, 59, 60, 61, 62, 63, 67, 68, 72, 74, 88\}.\end{aligned} \tag{3.38}$$

Remark 3.1.13. *Another idea we use is: if we find an* $f(x)$ *using this method with a square factor, then we can remove the square factor and should still get a torsion point. This sometimes helps find large order torsion points. We find 39 and 54 in genus 3 while searching for genus 4 curves.*

Remark 3.1.14. *The two geometrically simple Jacobians with an order 34 point are isomorphic to Elkies' two examples of 34-torsion points:*

$$y^2 = 1/9x^5 + 73/1296x^4 - 121/108x^3 + 155/72x^2 - 7/4x + 9/16 \tag{3.39}$$

$$y^2 = -11x^6 + 20x^5 + 737/16x^4 - 2095/4x^3 + 4421/4x^2 - 610x + 100. \tag{3.40}$$

3.2 The point searching method

The methods described so far recover many torsion orders in genus 2, and already give many new torsion orders in genus 3 and 4. Of the known orders in genus 2, we are currently missing points in $\mathcal{J}_{\text{simple}}(2, N)$ for $N = 29, 32, 33, 39, 40$. We will find these using the techniques described in this section, as well as discover many new orders in genus 3 and 4.

In the previous section, we used the difference of squares approach to determine $A(x)$ and $B(x)$ given a pair of equations of the form

$$\begin{aligned}A(x)^2 - f(x) &= \lambda x^p (x-1)^q\\ B(x)^2 - f(x) &= \mu x^r (x-1)^s.\end{aligned} \tag{3.41}$$

Since two such equations already determine $A(x)$ and $B(x)$, we don't expect to solve three equations simultaneously in this way. Thus this method on its own doesn't generalise well to matrix relations larger than 2×2.

Kronberg [Kro15] introduced the idea of setting up the equations as above and searching for solutions, applying this mostly to genus 2 curves. He set up a 3 by 3 matrix of relations in the genus 2 case, and restricted to a degree 5 model for the curve. We now describe some new approaches and use them to generate large order points in higher genus.

Fix an $m \times n$ matrix of relations p_{ij} and polynomials $C_1(x), \ldots, C_n(x)$, and consider the resultant equations

$$A_i(x)^2 - B_i(x)^2 f(x) = \lambda_i \prod_{j=1}^{n} C_j(x)^{p_{ij}}, \tag{3.42}$$

for $i = 1, \ldots, m$. We have seen in Lemma 3.1.4 that a solution to such a system of equations leads to relations between rational divisors. Our main idea is to search for rational points on the variety defined by these equations.

As in the previous section, we search over many systems of equations, since the same equations can yield many torsion orders. In particular, the matrix of relations p_{ij} doesn't control the sign of the relations between divisors, which can yield large torsion orders.

We are mainly interested in automatically searching for curves whose Jacobians are geometrically simple with larger order torsion points. In genus 3 and 4, there are lots of possible torsion orders, so searching for each one by hand would be tedious. In this section we thus often just find one curve at a time, rather than families of curves; in principle it is sometimes possible to find families.

We search for curves by simultaneously solving resultant equations. We impose as many relations as we have points P_i so that the matrix of relations is square, and we can take its determinant.

3.2.1 Simplifications

We make as many reductions as possible first, to simplify the point searching and to prevent finding the same curve with different points on the variety.

Any hyperelliptic curve $\mathcal{C}\colon y^2 = f(x)$ is isomorphic to one where the x^{n-1} coefficient is zero. Indeed, the linear transformation $x = X - \frac{f_{n-1}}{n f_n}, y = Y$ sets up an isomorphism to $\tilde{\mathcal{C}}\colon Y^2 = \tilde{f}(X)$, where $\tilde{f}_{n-1} = 0$. Note that this can yield coefficients with larger height.

We also have the coprime degrees trick. If $y^2 = f(x)$ with $\deg f$ odd, then we can change coordinates so that $f_n = 1$. Explicitly, transform to $(x, y) = (f_n^i X, f_n^j Y)$. This gives the equation $Y^2 f_n^{2j} = f_n^{ni+1} X^n + \cdots$. Choose i, j such that $2j = ni + 1$, which is possible since n is coprime to 2. Then the new hyperelliptic curve is of the form $Y^2 = \tilde{f}(X)$ where $\deg \tilde{f}(X) = \deg f(x)$ and $\tilde{f}(X)$ is monic.

We can map x-coordinates of two rational points to 0, 1: if the curve $\mathcal{C}\colon y^2 = f(x)$ has two rational points (x_1, y_1) and (x_2, y_2), then we can transform via $(x, y) = ((x_2 -$

$x_1)X + x_1, y)$. This defines an isomorphism from $\tilde{\mathcal{C}}\colon Y^2 = \tilde{f}(X) = f((x_2 - x_1)X + x_1)$ to $\mathcal{C}$. Note that this has the same degree, which is very helpful.

We can also map x-coordinates of three rational points to 0, 1, 2: if the curve $\mathcal{C}\colon y^2 = f(x)$ has three rational points (x_i, y_i), $i = 1, 2, 3$, with the x_i distinct, then we can use a linear fractional transformation to take them to, e.g., 0,1,2. We first compute the unique transformation $x \mapsto L(x) = \frac{ax+b}{cx+d}$ that takes $0, 1, 2$ to x_1, x_2, x_3, respectively. Then we pull back the equation $y^2 - f(x)$ along $(x, y) = (L(X), Y)$. Thus the equation of $\tilde{\mathcal{C}}$ is $Y^2 = f\left(\frac{aX+b}{cX+d}\right) = g(X)/(cX + d)^{\deg f}$ for some $g(x)$ with $\deg g = \deg f$. We can put this back in hyperelliptic form by multiplying by $(cX + d)^m$, where $m = \lceil (\deg f)/2 \rceil$. This gives $\left(Y(cX + d)^m\right)^2 = (cX + d)^\varepsilon g(X)$ for some $\varepsilon \in \{0, 1\}$. However, the right hand side has degree $\deg f$ or $\deg f + 1$, which complicates the points at infinity.

Example 3.2.1. *Consider the genus 2 case, where* $\deg f = 5$. *Then* $n-2g-1 = n-5$. *Taking* $n = 5$ *gives* $0 \le a_{ij} \le 5$, *and* $\deg B = 0, \deg A \le 2$. *We can assume* $B(x) = 1$, *which gives* $g(x, y) = A(x) + y$.

Now fix a_{ij} *such that* $\sum_j a_{ij} = 5$. *We need two solutions to get a* 2×2 *matrix. Then search for solutions to*

$$\begin{aligned} A_1(x)^2 - f(x) &= \lambda_1 x^{a_{11}}(x-1)^{a_{12}} \\ A_2(x)^2 - f(x) &= \lambda_2 x^{a_{21}}(x-1)^{a_{22}}. \end{aligned} \tag{3.43}$$

Since each $B_i(x) = 1$, *we can eliminate* $f(x)$ *by subtracting the two equations, and leave just one equation*

$$A_1(x)^2 - \lambda_1 x^{a_{11}}(x-1)^{a_{12}} = A_2(x)^2 - \lambda_2 x^{a_{21}}(x-1)^{a_{22}}. \tag{3.44}$$

For example, if $(a_{ij}) = \begin{pmatrix} 4 & 1 \\ 1 & 4 \end{pmatrix}$, *then we get the equations*

$$A_1(x)^2 - \lambda_1 x^4(x-1)^1 = A_2(x)^2 - \lambda_2 x^1(x-1)^4. \tag{3.45}$$

Let $A_i(x) = A_{i2}x^2 + A_{i1}x + A_{i0}$ *for* $i = 1, 2$. *The equations above give equations in* λ_j *and the coefficients of* A_i, *and we can view this as a variety over the affine space* $\mathbb{A}(A_{ij}, \lambda_1, \lambda_2)$ *corresponding to the ideal generated by*

$$\begin{aligned} &A_{10}^2 - A_{20}^2, \\ &2A_{10}A_{11} - 2A_{20}A_{21} + \lambda_2, \\ &2A_{10}A_{12} + A_{11}^2 - 2A_{20}A_{22} - A_{21}^2 - 4\lambda_2, \\ &2A_{11}A_{12} - 2A_{21}A_{22} + 6\lambda_2, \\ &A_{12}^2 - A_{22}^2 + \lambda_1 - 4\lambda_2, \\ &-\lambda_1 + \lambda_2. \end{aligned} \tag{3.46}$$

Simultaneous resultant equations define a variety whose rational points correspond to solutions to the resultant equation. These hopefully give torsion points of order dividing $\det(a_{ij})$. But not always, since the solutions can define singular curves, and, if $\lambda_i = 0$, we don't get a solution to the resultant equations.

3.2.2 Strategies to find points on the varieties

Point searching Since the varieties are embedded in high-dimensional space, naive point searching is often ineffective. The solution space is too big, and this restricts to searching for solutions where all the variables have small height. Nevertheless, sometimes a naive point search does discover some solutions.

Specialising to a subvariety We can sometimes transform a curve so that some of its coefficients have small height (but the others may have large height!). One of our main innovations is to restrict to subvarieties by imposing conditions on a subset of variables. Since many examples of curves with rational torsion occur in families, specialising some of the variables can find curves in the family with small coefficients. But working over fields that aren't algebraically closed complicates things; for example, a variable may be redundant geometrically (so we could assume it equals 1, say), but not arithmetically. To solve this, we iterate over small values of specialisations to maximise the chance of finding a solution.

Irreducible components We can speed this process up by first computing the irreducible components of the variety, and discarding the components which obviously contain no rational points. Sometimes computing irreducible components is too expensive; we have two options in this case. Firstly, we can specialise variables as above: if we impose enough conditions then it is quick to compute irreducible components.

Gröbner bases The alternative to specialising variables when computing irreducible components is the following heuristic algorithm to find points on varieties using Gröbner bases.

Sometimes computing irreducible components is too expensive, but we can still compute the Gröbner basis of the ideal of the variety. In this case, work backwards from the last element in the Gröbner basis and find the first reducible element. For each of its factors, compute the Gröbner basis with this factor as an additional ideal generator. Repeat this process until all elements of all Gröbner bases are irreducible.

Each time we compute a new Gröbner basis we are working on a subvariety, and often we recover irreducible components of the variety. This lets us focus on the interesting components, and discard components with no solutions (e.g. if we adjoin an irreducible polynomial in one variable of degree greater than 1). When adjoining factors, we can often apply specialist techniques to look for rational points, e.g. if the factor is a conic we can either parametrise its solutions or show it has none. In practice, we discard irreducible factors if the degree is large (say larger than 2). We can also discard factors if they give degenerate solutions, e.g. $\lambda_1 = 0$. We can list elements that correspond to degenerate solutions in an 'avoid' set, and check whether the avoid set is contained in the subvariety.

Combining these approaches makes the technique of imposing rational divisors on curves with certain relations practical for curves of genus 3 and 4. The following example demonstrates the method on the above example. We first look at the irreducible components, and then do a point search.

Example 3.2.2. *Continuing with the example above, the variety has 6 irreducible components. Two contain the equations $\lambda_1 = \lambda_2 = 0$, which we ignore.*

We examine one of the remaining four irreducible components in more detail. Consider the component corresponding to the ideal generated by

$$\begin{aligned} &A_{10} - A_{20}, \\ &A_{11} + 6A_{20} - A_{22}, \\ &A_{12} - 6A_{20} + A_{22}, \\ &A_{20}^2 - 1/3A_{20}A_{22} - 1/12\lambda_2, \\ &A_{21} + A_{22}, \\ &\lambda_1 - \lambda_2. \end{aligned} \tag{3.47}$$

The variables $A_{10}, A_{11}, A_{12}, A_{21}$ each occur in exactly one equation and are expressed linearly in terms of A_{20}, A_{22}. The equation $A_{20}^2 - 1/3A_{20}A_{22} - 1/12\lambda_2 = 0$ is linear in λ_2, so we can solve it using

$$\lambda_2 = 12A_{20}^2 - 4A_{20}A_{22}. \tag{3.48}$$

This defines λ_2 in terms of A_{20} and A_{22} also. This gives an arithmetically 2-dimensional space of curves with an order 15 point.

In this example, point searching on this component also works, giving, amongst

other solutions,

$$\begin{aligned} A_1(x) &= 1/3 - 5/3x + 1/3x^2 \\ A_2(x) &= 1/3 - 1/3x + 1/3x^2 \\ \lambda_1 &= \lambda_2 = 8/9, \end{aligned} \tag{3.49}$$

and thus

$$f(x) = A_1(x) - \lambda_1 x^4(x-1) \tag{3.50}$$

$$= -8/9x^5 + 11/3x^4 - 50/9x^3 + 35/9x^2 - 10/9x + 1/9. \tag{3.51}$$

We can check that $(0, 1/3) - \infty$ *has order 15.*

3.3 Variations on the method

We found the following variations of the above method. We explain each variation and give the torsion orders found by the method for genus 2, 3 and 4. To save space, we don't write all the curves down in the body of the thesis. All the curves we found are available in [Nic18]. We give some of the curves in Appendix F.

3.3.1 The odd degree method

The above method can be summarised as follows. Suppose we look for a genus g hyperelliptic curve. Choose an $n \times n$ matrix (a_{ij}) of nonnegative entries such that each row satisfies $1 \leq \sum_{j=1}^{n} a_{ij} \leq 2g+1$. Assume that there are n rational points on the curve, with x-coordinates $0, 1, x_3, \ldots, x_n$. Look for simultaneous solutions to

$$A_i(x)^2 - f(x) = \lambda_i \prod_{j=1}^{n} (x - x_i)^{a_{ij}}, \tag{3.52}$$

where $\deg A_i \leq g$. Subtracting the equation for $i = 1$ from all other equations eliminates $f(x)$ and gives $n-1$ equations to be satisfied by the coefficients of $A_i(x)$ and λ_i for $i = 1, \ldots, n$. Use the methods described above to search for points on this variety.

Remark 3.3.1. *We can also get odd degree hyperelliptic curves where* $\deg A = g+1$ *by considering solutions to* $A(x)^2 - f(x) = \lambda \prod_{i=1}^{n} (x - x_i)^{e_i}$ *where* $\sum_{i=1}^{n} e_i = 2g+2$. *Here we have to match the leading coefficient of* $A(x)^2$ *with that of the right hand side. A simple approach is to impose that* $A(x)$ *is monic and that* $\lambda = 1$.

Computation 3.3.2. *The 2×2 method finds rational points in $\mathcal{J}_{\text{simple}}(4, N)$ for all N in the set*

$$\begin{gathered}\{19, 28, 34, 40, 41, 42, 43, 44, 45, 46, 47, 48, \\ 49, 50, 51, 52, 53, 54, 58, 59, 60, 66, 72\}.\end{gathered} \tag{3.53}$$

The 3×3 method finds a rational point in $\mathcal{J}_{\text{simple}}(2, 40)$.

3.3.2 Even degree hyperelliptic curves with rational points at infinity

Suppose $\mathcal{C}\colon y^2 = f(x)$. If $\deg f$ is even, then $\mathcal{C}$ has two points at infinity: ∞^+, ∞^-. These are rational points if and only if f_{2g+2} is a square. This is the case we focus on here. Without loss of generality, we can choose ∞^+ to be the base divisor.

As before, the resultant equation $A(x)^2 - B(x)^2 f(x) = \lambda \prod_{i=1}^{n} (x - x_i)^{a_i}$ (with $a_i > 0$) implies the function $g(x, y) = A(x) + B(x)y$ intersects the curve at P_i' with multiplicity a_i, where $x(P_i') = x_i$. The intersection of $g(x, y) = 0$ and $\mathcal{C}$ in the other chart is more complicated. We have $g(x, y) = A(x) + B(x)y = A(1/u) + B(1/u)v/u^g$. Choose m so that $u^{m+g}A(1/u)$ and $u^m B(1/u)$ are both polynomials in u. Then $g(x, y) = \left(u^{m+g}A(1/u) + vu^m B(1/u)\right)/u^{m+g}$, and the intersection with the curve is: zeroes along $\{\tilde{A}(u) + v\tilde{B}(u) = 0, v^2 = u^{2g+2}f(1/u)\}$ and a pole of order $m + g$ along $\{u = 0\} = \infty^+ + \infty^-$.

After adding or subtracting multiples of $\operatorname{div}(x - x_i) = P_1 + \iota(P_1) - \infty^+ - \infty^-$, the relation is of the form

$$\sum_{i=1}^{n} a_i' P_i \sim \alpha\infty^+ + \beta\infty^- \tag{3.54}$$

for some integers α, β, where $|a_i'| = |a_i|$. Thus

$$\sum_{i=1}^{n} a_i'(P_i - \infty^+) \sim \left(\alpha - \sum_{i=1}^{n} a_i'\right)\infty^+ + \beta\infty^-. \tag{3.55}$$

Since the left hand side has degree zero, so does the right hand side, which implies that $\sum_{i=1}^{n} a_i' = \alpha + \beta$, and thus the relation is really

$$\sum_{i=1}^{n} a_i'(P_i - \infty^+) - \beta(\infty^- - \infty^+) \sim 0. \tag{3.56}$$

We view this as a relation on the $n+1$ divisors: $D_i = P_i - \infty^+$ and $D_{n+1} = \infty^- - \infty^+$. We form a square matrix of relations by finding $n + 1$ relations.

The last column in the matrix is difficult to compute a priori, since it depends on how the functions $g_i(x, y)$ intersect the curve at infinity. Instead, our idea is to try all $(n+1) \times n$ matrices with nonnegative entries such that $1 \leq \sum_{j=1}^{n} a_{ij} \leq 2g+2$, and such that each row of the matrix is distinct. The last column (the coefficient of $\infty^+ - \infty^-$) is determined by the solution to the resultant equations.

We require $\infty^+ - \infty^-$ to be rational so that the resultant equations are solved rationally. This requires ∞^+, ∞^- to be rational points on the curve. Given that $\deg f = 2g+2$, there are two cases: $\deg A_i = g+1$ or $\deg A_i < g+1$. In the second case, it must be that $\sum_j a_{ij} = 2g+2$. In the first case, if $\sum_j a_{ij} < 2g+2$, then ∞^+ is rational, since the leading coefficient of f is the square of the leading coefficient of A_i. If $\sum_j a_{ij} = 2g+2$, then we need $A_{i,g+1}^2 + \lambda$ to be square.

Example 3.3.3. *The matrix*

$$\begin{pmatrix} 0 & 2 \\ 2 & 1 \\ 3 & 1 \end{pmatrix} \tag{3.57}$$

defines the resultant equations

$$A_1(x)^2 - f(x) = \lambda_1(x-1)^2 \tag{3.58}$$

$$A_2(x)^2 - f(x) = \lambda_2 x^2(x-1) \tag{3.59}$$

$$A_3(x)^2 - f(x) = \lambda_3 x^3(x-1). \tag{3.60}$$

Since the right hand sides have degree at most 4, and we want $\deg f = 6$*, it must be that* $\deg A_i = 3$ *for each* i*. Moreover, we need* ∞^+, ∞^- *to be rational, which forces the leading coefficient of* $f(x)$ *to be a square, and it may as well then be 1. Since each* $A_i(x)$ *is defined only up to sign, we can assume each* $A_i(x)$ *is a monic cubic. Now search for points on the variety defined by Equation* (3.58) *minus Equation* (3.59) *and Equation* (3.58) *minus Equation* (3.60)*. We find many solutions, including*

$$\begin{aligned} A_1(x) &= x^3 - 1/2x^2 - x \\ A_2(x) &= x^3 - 1/2x^2 - x + 1 \\ A_3(x) &= x^3 - 1/2x^2 + x - 1 \\ (\lambda_1, \lambda_2, \lambda_3) &= (-1, 2, 4). \end{aligned} \tag{3.61}$$

One can check that this gives

$$y^2 = x^6 - x^5 - 7/4x^4 + x^3 + 2x^2 - 2x + 1, \tag{3.62}$$

with the 23-torsion point $(0,1) - \infty^+$*.*

Computation 3.3.4. *This method finds rational points in $\mathcal{J}_{\text{simple}}(2, N)$ for all N in the set*

$$\{18, 21, 22, 23, 24, 26, 27, 28, 29, 30, 33, 34, 39\}; \tag{3.63}$$

rational points in $\mathcal{J}_{\text{simple}}(3, N)$ for all N in the set

$$\{64, 65, 72, 91\}. \tag{3.64}$$

Example 3.3.5. *The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(2, 33)$:*

$$y^2 = x^6 - 38/9x^5 + 559/81x^4 - 478/81x^3 + 79/27x^2 - 52/81x + 4/81. \tag{3.65}$$

The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(2, 39)$:

$$y^2 = x^6 - 10x^5 + 39x^4 - 66x^3 + 53x^2 - 20x + 4. \tag{3.66}$$

Remark 3.3.6. *We just search over all 3×2 matrices of relations, with the third column filled in from the relations between the points at infinity. We can also recover orders 65 and 91 this way. They appear to come from a family with an order 13 point, that specialises to get an order 5 and an order 7 point, separately.*

Example 3.3.7. *The Jacobian of the following curve is a rational point in $\mathcal{J}_{\text{simple}}(3, 72)$:*

$$\begin{aligned} y^2 = x^8 - 5x^7 + 55/4x^6 - 471/20x^5 + 2049/80x^4 - 135/8x^3 \\ + 2439/400x^2 - 189/200x + 81/1600 \end{aligned} \tag{3.67}$$

The Jacobian of the following curve is a rational point in $\mathcal{J}_{\text{simple}}(3, 64)$:

$$y^2 = x^8 - 8x^7 + 24x^6 - 32x^5 + 18x^4 + 8x^3 - 8x^2 + 1. \tag{3.68}$$

3.3.3 Weierstrass points

In this variation, we impose that $f(x) = g(x)h(x)$ with $1 \leq \deg g \leq 2$ and with $\deg f$ odd. Then the divisor $\langle g(x), 0\rangle$ is 2-torsion. We can also assume there are $n-1$ other points and then impose an $(n-1) \times n$ matrix of relations. We get an $n \times n$ matrix of relations by completing it with a row with zeroes everywhere except for a 2 in the column corresponding to the Weierstrass point. We can assume the x-coordinates of two of the points are 0, 1, as usual.

We show below that we can recover Elkies' 32-torsion curve and 34-torsion curve.

Example 3.3.8 (Elkies' 34-torsion point)**.** *Elkies has the following curve with a 34-torsion point:*

$$\mathcal{C}_{34}\colon y^2 = (10-x)(3x+2)(72x^4+96x^3+45x^2-38x+5). \tag{3.69}$$

We can recover it as follows. First assume that the Weierstrass point has x-coordinate μ, and iterate over possible μ of small height. Label the divisors $D_1 = (0,y_1)-\infty, D_2 = (1,y_2)-\infty, D_3 = (\mu,0)-\infty$. To keep $B_i(x) = 1$ and $\deg f = 5$, we iterate over matrices with row-sum either 5 or 6.

One such matrix is $\begin{pmatrix} 2 & 3 & 0 \\ 5 & 1 & 0 \end{pmatrix}$*, which gives the equations*

$$\begin{aligned} f(x) &= (x-\mu)g(x) \\ A_1(x)^2 - f(x) &= \lambda_1 x^2(x-1)^3 \\ A_2(x)^2 - f(x) &= \lambda_2 x^5(x-1), \end{aligned} \tag{3.70}$$

with $\deg g = 4, \deg A \le 2, \deg B \le 3$*. Using our method for point searching with* $\mu = -9/16$ *gives the following curve*

$$y^2 = 291600x^5 + 496441x^4 + 284616x^3 - 38394x^2 - 40824x + 6561. \tag{3.71}$$

The point $(0,81)-\infty$ *has order 17 and the Weierstrass divisor* $(-9/16,0)-\infty$ *has order 2. Thus we get an order 34 point on its Jacobian. The curve is isomorphic to* $\mathcal{C}_{34}$*.*

Remark 3.3.9. *Note that this has very large coefficients, so would be infeasible to find via naive point searching.*

Similarly, the matrix $\begin{pmatrix} 3 & 1 & 1 \\ 1 & 5 & 0 \end{pmatrix}$ and $\mu = 16/15$ gives us the following two geometrically nonisomorphic curves with a 32-torsion point:

$$\begin{aligned} y^2 = {} & 5760/5498339x^5 + 9049956/60481729x^4 - 35880336/60481729x^3 \\ & + 4785584/5498339x^2 - 34168320/60481729x + 8294400/60481729 \end{aligned} \tag{3.72}$$

$$\begin{aligned} y^2 = {} & -1718857/910141920x^5 + 377186051369/436868121600x^4 \\ & - 400896630191/109217030400x^3 + 71260492321/12135225600x^2 \\ & - 950527921/227535480x + 19018321/17065161. \end{aligned} \tag{3.73}$$

The first is geometrically isomorphic to Elkies' 32-torsion curve as listed on [Elk18]. Elkies actually finds a 1-parameter family of curves with a 32-torsion point, but refrains from giving the formula. Thus we don't know if the second curve is new.

Computation 3.3.10. *This method finds rational points in $\mathcal{J}_{\text{simple}}(2, N)$ for all N in the set*

$$\{32, 34\}; \tag{3.74}$$

a rational point in $\mathcal{J}_{\text{simple}}(3, 52)$, and a rational point in $\mathcal{J}_{\text{simple}}(4, 74)$.

The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(3, 52)$:

$$\begin{aligned} \mathcal{C}_{52}^3 \colon y^2 = {} & 36x^7 - 11/25x^6 + 19452/25x^5 \\ & - 26366/25x^4 - 510x^3 + 1657x^2 - 1050x + 225. \end{aligned} \tag{3.75}$$

The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(4, 74)$:

$$\begin{aligned} \mathcal{C}_{74}^4 \colon y^2 = {} & -x^9 + 12618359905/2268426384x^8 - 3217721621/252047376x^7 \\ & + 330039943/16003008x^6 - 149997/5488x^5 + 39521/1372x^4 \\ & - 239283/10976x^3 + 59049/5488x^2 - 59049/19208x + 59049/153664. \end{aligned} \tag{3.76}$$

3.3.4 More general $B_i(x)$

In this variation, we allow some of the resultant equations to include a nonconstant $B(x)$ term. This means the exponents on the right hand side can be larger. This is similar to difference of squares method II, but we can allow several equations to have an extra term.

We illustrate this method by recovering Howe's example of an order 70 point on the Jacobian of a genus 2 curve ([How14]). The original method to find this curve involves gluing together two elliptic curves: one with a 5-torsion point and one with a 7-torsion point.

Example 3.3.11. *Howe has the curve $y^2 = f_{70}(x)$, where*

$$f_{70}(x) = 22x^5 + 697/144x^4 - 645/4x^3 + 1045/4x^2 - 162x + 36. \tag{3.77}$$

This has the rational points ∞, $P_1 = (0, 6), P_2 = (1, 11/12), P_3 = (3/4, 27/64)$. Let $D_i = P_i - \infty$ for $i = 1, 2, 3$. MAGMA *computes $70D_1 \sim 0, 35D_2 \sim 0$ and $70D_3 \sim 0$.*

Given the curve, we can compute the relations $\sum_{i=1}^3 a_i D_i$ with $\sum_{i=1}^3 |a_i| \leq n$, where we gradually increase n. With $n \leq 8$ we find

$$\begin{pmatrix} 3 & -1 & -1 \\ 2 & 3 & 0 \\ 0 & 2 & -6 \end{pmatrix} \begin{pmatrix} D_1 \\ D_2 \\ D_3 \end{pmatrix} \sim 0. \tag{3.78}$$

We can recover Howe's curve as an odd degree hyperelliptic curve with three rational points by imposing the conditions $f_5 = 1, x(P_3) = 3/4$. We search over 3×3 matrices where two of the rows sum to at most 5 and one row sums to either 7 or 8. The resultant equation corresponding to the row-sum of 8 has $\deg B(x) \leq 2$. From the Gröbner bases, we can see there is a solution over $\mathbb{Q}(\sqrt{22})$. After twisting by 22, we recover Howe's curve.

The Jacobian of the following genus 2 curve lies in $\mathcal{J}_{\text{simple}}(2, 40)$. It is isomorphic to Elkies' order 40 curve ([Elk18]):

$$y^2 = -6x^5 + 19x^4 - 22x^3 + 185/16x^2 - 11/4x + 1/4. \tag{3.79}$$

The Jacobian of the following genus 2 curve lies in $\mathcal{J}_{\text{either}}(2, 40)$ (I couldn't show the Jacobian is geometrically simple):

$$y^2 = -48t^5 + 169t^4 - 210t^3 + 125t^2 - 36t + 4. \tag{3.80}$$

We record the curve (3.79) in a computation.

Computation 3.3.12. *This method finds a rational point in $\mathcal{J}_{\text{simple}}(2, 40)$.*

3.3.5 Specialising a family of curves

Given a family of curves whose Jacobians all contain an N-torsion point, we can look for a specialisation of the family that also has an M-torsion point for some M coprime to N, or such that the N-torsion point is a multiple of M. This technique has been applied in the literature to find, for example, a 48-torsion curve. In particular, [How14] first finds a family of curves with a 24-torsion point, and then specialises to get 48-torsion.

Example 3.3.13. *We apply this idea to get an order 82 point on the Jacobian of a genus 4 curve. Flynn has the following 1-parameter family [Fly91] of genus g curves with an order $2g^2 + 2g + 1$ point. He defines $\psi(x) = x^{g+1} - t(x-1)^g - x^g(x-1)$ and then defines the curve by $y^2 = f(x)$, where*

$$f(x) = \frac{\psi(x)^2}{4} - tx^g(x-1)^{g+1}. \tag{3.81}$$

We check for $g = 4$ that there is a specialisation for which the curve has geometrically simple Jacobian. We then search for small values of t and find that f has a root when

$t = 256/3$. *After clearing denominators of f by multiplying by 36 (which is square), we obtain the following genus 4 curve:*

$$\begin{aligned} y^2 = &-3072x^9 + 79369x^8 - 548864x^7 + 1856512x^6 - 3679232x^5 \\ &+ 4589056x^4 - 3670016x^3 + 1835008x^2 - 524288x + 65536, \end{aligned} \tag{3.82}$$

giving a point in $\mathcal{J}_{\text{simple}}(4, 82)$.

3.3.6 Curves with small coefficients

We can also search over curves with small coefficients, as in [How14]. We searched for both simple and split Jacobians. For simple Jacobians, we can just search over all polynomials $f(x)$ of a given degree, with coefficients bounded in height by some constant. For split Jacobians, we searched for curves of the form $y^2 = f(x^2)$ with $f(x) \in \mathbb{Z}[x]$ and $\deg f = 3$. We also searched over curves of the form $y^2 = (x^2 - a)f(x^2)$ where $a \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$ such that $\deg f = 2$. Both classes of curves have split Jacobians by construction, but this reduces the space to search. We searched over all integral coefficients bounded by 30 in absolute value. We used MAGMA to compute the torsion subgroup in each case. We find the following curves with small coefficients:

$$\mathcal{C}_{48,1} \colon y^2 = x^6 - 14x^4 + 37x^2 + 12 \tag{3.83}$$

$$\mathcal{C}_{48,2} \colon y^2 = x^6 - 56x^4 + 592x^2 + 768 \tag{3.84}$$

$$\mathcal{C}_{48,3} \colon y^2 = x^6 + 42x^4 + 261x^2 + 1620. \tag{3.85}$$

The curves are pairwise geometrically nonisomorphic, as can be seen by their Igusa invariants. The curve $\mathcal{C}_{48,1}$ already appears in [PP12b], but $\mathcal{C}_{48,2}$ and $\mathcal{C}_{48,3}$ are geometrically nonisomorphic to the two examples in [PP12b].

Howe gives a 1-parameter family of genus 2 curves whose Jacobians are geometrically split with a point of order 24, and gives a subfamily whose Jacobians have a point of order 48; the curves in the subfamily correspond to rational points on a rank 2 elliptic curve ([How14]).

We now show that $\mathcal{C}_{48,2}$ and $\mathcal{C}_{48,3}$ do not lie in Howe's family of curves $\mathcal{C}_s \to \mathbb{A}^1$, analogously to the method used in [BLP09]. The curve is geometrically isomorphic to one lying in the family if and only if there is $s \in \mathbb{Q}$ such that the Igusa invariants of $\mathcal{C}_s$ equal those of $\mathcal{C}_{48,2}$ or $\mathcal{C}_{48,3}$ in weighted projective space. Let

$$(\alpha(s), \beta(s), \gamma(s)) = (I_4/I_2^2, I_6/I_2^3, I_{10}/I_2^5) \tag{3.86}$$

denote the normalised Igusa invariants for $\mathcal{C}_s$. Let $(\alpha_2, \beta_2, \gamma_2)$ and $(\alpha_3, \beta_3, \gamma_3)$ denote the normalised Igusa invariants for $\mathcal{C}_{48,2}$ and $\mathcal{C}_{48,3}$, respectively. For each $i = 2, 3$, the condition that $(\alpha(s), \beta(s), \gamma(s)) = (\alpha_i, \beta_i, \gamma_i) \in \overline{\mathbb{Q}}^3$ gives three polynomials that s must satisfy. In each case, we find that there is no $s \in \overline{\mathbb{Q}}$ that simultaneously solves these. The MAGMA file `howefamily48.m` in [Nic18] verifies this. We have thus shown the following proposition.

Proposition 3.3.14. *The curves $\mathcal{C}_{48,2}$ and $\mathcal{C}_{48,3}$ are new examples of genus 2 curves whose Jacobians are split with a rational point of order 48.*

Remark 3.3.15. *Howe also gives three example curves from the family, which are geometrically nonisomorphic to my two examples.*

We also find the following genus 2 curves whose Jacobians are split with 40-torsion points. We can see they are split because they only contain even terms in x:

$$y^2 = 25x^6 - 10x^4 + 25x^2 + 24 \tag{3.87}$$

$$y^2 = 24x^6 + 25x^4 - 10x^2 + 25 \tag{3.88}$$

$$y^2 = x^6 + 10x^4 + 49x^2 + 264 \tag{3.89}$$

$$y^2 = x^6 - 10x^4 + x^2 + 72. \tag{3.90}$$

Geometrically simple genus 3 Jacobians We find geometrically simple Jacobians of genus 3 curves with large order points by searching through curve equations with small coefficients. To allow us to search with some coefficients being larger, we impose that some of the coefficients vanish or are equal to one. For example, imposing that $f_8 = f_0 = 1$ and $f_7 = f_5 = 0$, and searching for integral coefficients in the range $[-6, 6]$, we find the following two genus 3 curves whose Jacobians are geometrically simple. The first has an order 22 point and the second an order 37 point on its Jacobian:

$$\mathcal{C}_{22}^3 \colon y^2 = x^8 + 2x^6 + 3x^4 - 4x^3 + 6x^2 - 4x + 1 \tag{3.91}$$

$$\mathcal{C}_{37}^3 \colon y^2 = x^8 - 4x^6 + 2x^4 + 4x^2 - 4x + 1. \tag{3.92}$$

Computation 3.3.16. *The small coefficients method finds rational points in the space $\mathcal{J}_{\text{simple}}(3, N)$ for all N in the set*

$$\{22, 37\}. \tag{3.93}$$

3.4 In higher genus

3.4.1 Genus 5

Computation 3.4.1. *The difference of squares and difference of squares II methods give rational points in* $\mathcal{J}_{\text{simple}}(5, N)$ *for all* N *in the set*

$$\begin{aligned}\{&26, 39, 61, 62, 63, 64, 65, 66, 68, 72, 73, 74,\\ &75, 76, 77, 81, 84, 85, 86, 87, 88, 92, 110\}.\end{aligned} \tag{3.94}$$

3.4.2 Genus 6

We can do the same computation for the difference of squares and difference of squares II method. We give the following examples, neither of which occurs as a known order in one of the families growing with genus. Neither curve is defined for all t – we have to search for specialisations on which the right hand side difference of squares splits into a product of degree 6 factors.

Example 3.4.2. *The Jacobian of the following curve lies in* $\mathcal{J}_{\text{simple}}(6, 103)$*:*

$$\begin{aligned}y^2 = {} & 1/128x^{13} + 142081/65536x^{12} - 22913/4096x^{11} + 40765/32768x^{10}\\ & + 56155/4096x^9 - 1544433/65536x^8 + 31283/2048x^7 + 13755/16384x^6\\ & - 16693/2048x^5 + 371727/65536x^4 - 7173/4096x^3 + 6717/32768x^2\\ & + 15/4096x + 1/65536.\end{aligned} \tag{3.95}$$

The Jacobian of the following curve lies in $\mathcal{J}_{\text{simple}}(6, 113)$*:*

$$\begin{aligned}y^2 = {} & 81x^{13} + 1144x^{12} - 10570x^{11} + 37409x^{10} - 76261x^9 + 100794x^8\\ & - 89985x^7 + 216405/4x^6 - 20743x^5 + 8387/2x^4 - 51/2x^3 - 615/4x^2\\ & + 27/2x + 9/4.\end{aligned} \tag{3.96}$$

3.5 Examples where our method fails

We found some examples of known torsion orders that our methods cannot immediately recover. These are interesting to analyse as they may suggest extensions to the methods that would recover these curves, and hopefully also find new torsion orders.

3.5.1 Order 48

The following is an example where our method fails.

Example 3.5.1 (Finding 48-torsion)**.** *Platonov [PP12b] has the curve*

$$y^2 = (x-2)(x+2)(x^4 - 10x^2 - 3), \tag{3.97}$$

with the 48-torsion point $(0,6) - \infty^+$*.*

First transform so that it has points with x*-coordinates* $0, 1$*, giving*

$$y^2 = (x-3/2)(x+1/2)(x^4 - 2x^3 - x^2 + 2x - 3/4). \tag{3.98}$$

In particular, this has the three rational points $(0,3/4), (1,3/4)$ *and* $(3/2,0)$*. Using* ∞^+ *as the base point, we define* $D_1 = (0,3/4) - \infty^+, D_2 = (1,3/4) - \infty^+, D_3 = (3/2,0) - \infty^+$*. This gives the following matrix of relations:*

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & -1 & -4 \\ 1 & 2 & 3 \end{pmatrix}. \tag{3.99}$$

To recover the relation $D_1 - D_2 - 4D_4 = \operatorname{div} g$*, we write*

$$\begin{aligned} D_1 - D_2 - 4D_4 &\sim D_1 - D_2 + (D_2 + \iota D_2) - 4D_4 + 4(D_4 + \iota D_4) && (3.100)\\ &= D_1 + \iota D_2 + 4\iota D_4 && (3.101)\\ &= (0,3/4) + (1,-3/4) + 4(3/2,0) - \infty^+ - 5\infty^-. && (3.102) \end{aligned}$$

To see the form of the function g *we rewrite in terms of* $\infty^+ + \infty^-$*. Indeed, we know that* $\mathscr{L}(n(\infty^+ + \infty^-)) = \{A(x) + B(x)y \colon \deg A \le n, \deg B \le n-3\}$ *(since* $x \in \mathscr{L}(\infty^+ + \infty^-)$ *and* $y \in \mathscr{L}(3\infty^+ + 3\infty^-)$*). This gives*

$$\begin{aligned} \operatorname{div} g &= D_1 - D_2 - 4D_4 && (3.103)\\ &\sim (0,3/4) + (1,-3/4) + 4(3/2,0) + 4\infty^+ - 5(\infty^+ + \infty^-). && (3.104) \end{aligned}$$

Thus $g(x) = A(x) + B(x)y$ *where* $\deg A \le 5, \deg B \le 2$*. This is too many coefficients to search over naively. Similarly, the relation* $D_1 + 2D_2 + 3D_3 = \operatorname{div} h$ *gives too many coefficients to search over.*

Remark 3.5.2. *This curve is in fact* $\mathcal{C}_{48,1}$*, which we found using the small coefficients method in Section 3.3.6.*

As usual, we can make the problem tractable by guessing small values for some of the variables, but when there are so many variables this method is unlikely to find a solution.

3.6 Other examples

3.6.1 A parametrised family with $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-torsion

In this subsection we find a one parameter family of genus 2 curves whose Jacobians have a rational copy of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The method is also interesting as it allows us to find relations on a higher genus curve and then try to drop the genus by imposing a singularity. I believe this idea is novel.

In Chapter 5 we focus on finding subgroups isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ for various n, but via a different method. In that chapter we also impose that the n-Weil pairing acts trivially on the subgroup, which turns out to be false in this case. We will find more families of curves admitting $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ torsion in Chapter 5.

Proposition 3.6.1. *Let $p(x), q(x) \in K[x]$ be linear and let $\lambda, \mu \in K$. Define $A(x) + C(x) = \lambda p(x)^4 - \mu q(x)^4$ and $A(x) - C(x) = 1$. Then $A(x)^2 - C(x)^2 = \lambda p(x)^4 - \mu q(x)^4$, and we define $h(x) = A(x)^2 - \lambda p(x)^4 = C(x)^2 - \mu q(x)^4$. This is a genus 3 curve, and generically has two independent 4-torsion points, given by $p(x) = 0, y = A(x)$ and $q(x) = 0, y = C(x)$.*

The idea is to take a general solution to the above proposition and impose that $h(x)$ has a square factor. This means the genus 3 curve $y^2 = h(x)$ has a singularity. We transform the genus 3 curve to a genus 2 curve that also has the torsion property.

If we can write $A(x)^2 - B(x)^2 f(x) = \lambda p(x)^4$ and $C(x)^2 - D(x)^2 f(x) = \mu q(x)^4$ for some λ, μ, A, B, C, D, we should get 2 independent 4-torsion points. Our strategy is to try and solve

$$\begin{aligned} A(x)^2 - h(x) &= \lambda p(x)^4 \\ C(x)^2 - h(x) &= \mu q(x)^4, \end{aligned} \tag{3.105}$$

with $\deg A, \deg C \leq 4$. Up to a birational transformation, we can assume $p(x) = x, q(x) = x - 1$. Subtracting the two equations gives

$$A(x)^2 - C(x)^2 = \lambda x^4 - \mu(x-1)^4. \tag{3.106}$$

The left hand side factors as $(A(x) + C(x))(A(x) - C(x))$ and the right hand side factors as $(\lambda x^4 - \mu(x-1)^4) \cdot 1$.

This gives

$$\begin{aligned} A(x) &= \frac{1}{2}(\lambda x^4 - \mu(x-1)^4 + 1) \\ C(x) &= \frac{1}{2}(\lambda x^4 - \mu(x-1)^4 - 1). \end{aligned} \tag{3.107}$$

Then $h(x) = A(x)^2 - \lambda x^4$ is degree 8. The curve $y^2 = h(x)$ is generically of genus 3, and has two independent 4-torsion points. We now find a subfamily that degenerates down to genus 2.

To impose that $h(x)$ has a square factor, it suffices to impose that $\mathrm{disc}(h) = 0$. We have

$$\begin{aligned}\mathrm{disc}(h) = 16\lambda^4\mu^4(\lambda-1)^4(\mu-1)^4(\lambda-\mu)^4 \\ \cdot (\lambda^2\mu^2 - 2\lambda^2\mu + \lambda^2 - 2\lambda\mu^2 - 2\lambda\mu + \mu^2).\end{aligned} \tag{3.108}$$

If $\lambda = 0$ or $\mu = 0$, we find that $h(x)$ factors as the square of a quartic, so we cannot recover a genus 2 curve. If $\lambda = 1$ or $\mu = 1$, we find that the square factor of $h(x)$ is $(x-1)^2$ or x^2. This means the resultant equation no longer gives a 4-torsion divisor on the Jacobian.

If $\lambda = \mu$, then $h(x)$ is degree 6 already, so $y^2 = h(x)$ is a genus 2 hyperelliptic curve. However, in this case, the resultant equations are

$$\begin{aligned}A(x)^2 - h(x) &= \lambda x^4 \\ C(x)^2 - h(x) &= \lambda(x-1)^4,\end{aligned} \tag{3.109}$$

where $\deg A = \deg C = 3$, and $\deg h = 6$. Since the right hand sides are of degree 4, the corresponding relation in divisors for the first equation is $4(0, A(0)) + 2P_\infty - 3(\infty^+ + \infty^-) \sim 0$, where $P_\infty \in \{\infty^+, \infty^-\}$, and similarly for the second equation. In either case, this does not give a 4-torsion relation.

We are left with the last factor:

$$\lambda^2\mu^2 - 2\lambda^2\mu + \lambda^2 - 2\lambda\mu^2 - 2\lambda\mu + \mu^2 = 0. \tag{3.110}$$

As a quadratic in λ, its discriminant is $16\mu^3$. Thus to have a solution over K, we need $\mu = t^2$ for some $t \in K$. This gives $\lambda = t^2/(t \pm 1)^2$. Without loss of generality, we put $\lambda = t^2/(t-1)^2$, since $(-t)^2/(-t-1)^2 = t^2/(t+1)^2$. The repeated factor of $h(x)$ is $B(x) = tx - t + 1$. Dividing out by $B(x)^2$ and the leading coefficient of $h(x)$ (which is square) gives $f(x)$ of degree 6. The resultant equations are now of the form

$$\begin{aligned}A(x)^2 - B(x)^2 f(x) &= \lambda x^4 \\ C(x)^2 - B(x)^2 f(x) &= \mu(x-1)^4,\end{aligned} \tag{3.111}$$

where $\deg A = \deg C = 4$, $\deg B = 1$ and $\deg f = 6$. The first resultant equation implies that $\mathrm{div}(A(x) - B(x)y) = 4P_0' + 4P_\infty' - 4(\infty^+ + \infty^-)$, where $x(P_0') = 0$ and $x(P_\infty') = \infty$; a similar result holds for the second equation. An explicit computation

then shows that $4(0, A(0)/B(0)) - P_\infty$ and $4(1, A(1)/B(1)) - Q_\infty$ are both 4-torsion divisors, where $P_\infty, Q_\infty \in \{\infty^+, \infty^-\}$.

Specialising $f(x)$ at various t, we check its Jacobian is geometrically simple using Proposition 2.4.2. Thus generically the Jacobian is geometrically simple.

One can also check that there are at least two different curves in the family with different Igusa invariants, so that the family is not trivial.

This proves the following proposition.

Proposition 3.6.2. *Let $\lambda = \frac{t^2}{(t-1)^2}$ and $\mu = t^2$, for $t \in K$. Let*

$$\begin{aligned} A(x) &= \frac{1}{2}(\lambda x^4 - \mu(x-1)^4 + 1) \\ B(x) &= \frac{1}{2}(\lambda x^4 - \mu(x-1)^4 - 1). \end{aligned} \tag{3.112}$$

Let $h(x) = A(x)^2 - \lambda x^4$. Then $h(x) = B(x)^2 f(x)$, where $B(x) = \frac{t^2(t-2)}{2(t-1)^2}(tx - t + 1)$ and $f(x)$ is monic of degree 6. The curve $y^2 = f(x)$ has two independent 4-torsion points: $\left(0, \frac{(t-1)^2(t+1)}{t^2(t-2)}\right) - \infty^+$ and $\left(1, \frac{2t-1}{t^2(t-2)}) - \infty^+\right)$. The Jacobian of the generic member of the family is geometrically simple.

Remark 3.6.3. *If we try the same trick to get a parametrised $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ then we find the repeated factor is either $p(x)$ or $q(x)$, which means that we actually get $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

3.6.2 Large order points over extensions of $\mathbb{Q}$

We have focused on finding large order points on Jacobians of curves over $\mathbb{Q}$. Kronberg provides examples in [Kro15] of genus 2 curves defined over low-degree number fields with large order torsion points. In particular, he finds a Jacobian of a genus 2 curve defined over a cubic number field with a point of order 31, and a Jacobian of a genus 2 curve defined over a quadratic number field with a point of order 37. In this section we provide two more such examples, also for Jacobians of genus 2 curves.

Order 35 over a quadratic field We first give an example of a Jacobian of a genus 2 curve over a quadratic field with a point of order 35. There are no known examples of points of order 35 on a geometrically simple Jacobian of a genus 2 curve over $\mathbb{Q}$. Howe's example of a point of order 70 (and thus a point of order 35) is on a geometrically split Jacobian of a genus 2 curve ([How14]). This therefore provides the first known example of a geometrically simple Jacobian of a genus 2 curve with an

order 35 point defined over a quadratic extension. The curve we find is defined over $\mathbb{Q}$, in contrast to Kronberg's examples, which are defined over the extensions.

We try to solve $A^2 - f = \lambda x^7$ and $B^2 - f = \mu(x-1)^7$ with f containing a square factor. Removing a square factor from such an f gives a lower genus curve. Putting $\lambda = \mu = 1$ we get

$$A(x)^2 - B(x)^2 = x^7 - (x-1)^7. \tag{3.113}$$

Let $K = \mathbb{Q}(\sqrt{-7})$, and let $\bar{\cdot}$ denote the order 2 automorphism in K. Over $\mathbb{Q}(\sqrt{-7})$, the polynomial $x^7 - (x-1)^7$ factors as $7g_1(x)g_2(x)$, where

$$g_1(x) = (x^3 - \frac{3+\sqrt{-7}}{2}x^2 + \frac{1+\sqrt{-7}}{2}x - \frac{\sqrt{-7}}{7}), \tag{3.114}$$

and $g_2(x) = \overline{g_1}(x)$.

These factors are conjugate over $\mathbb{Q}$. Thus we can write $(A+B)(A-B) = 7g_1(x)g_2(x)$. For any nonzero u in $\mathbb{Q}(\sqrt{-7})$, we can put $A + B = 7ug_1(x), A - B = g_2(x)/u$ and find $A = \frac{7u}{2}g_1 + \frac{1}{2u}g_2$ and $B = \frac{7u}{2}g_1 - \frac{1}{2u}g_2$. Let $f(x) = A(x)^2 - x^7$. The discriminant of $f(x)$ is zero for $u = \pm 1/\sqrt{-7}$, and $f(x) = (x-1)^2 h(x)$ in both cases, where $h(x) = -x^5 - 2x^4 - 3x^3 + 33/4x^2 - 5x + 1$.

This leaves us with the resultant equations

$$\begin{aligned} A(x)^2 - (x-1)^2 h(x) &= x^7 \\ B(x)^2 - (x-1)^2 h(x) &= (x-1)^7. \end{aligned} \tag{3.115}$$

The first equation gives a 7-torsion point, but the second equation only gives a 5-torsion point.

Proposition 3.6.4. *Let $\mathcal{C}$ be the curve $y^2 = -4x^5 - 8x^4 - 12x^3 + 33x^2 - 20x + 4$, and let $\mathcal{J}$ be its Jacobian. Then $\mathcal{J}$ has a 7-torsion point over $\mathbb{Q}$ and a 5-torsion point over $\mathbb{Q}(\sqrt{-7})$. Thus $\mathcal{J}$ has a 35-torsion point over $\mathbb{Q}(\sqrt{-7})$. The Jacobian is geometrically simple.*

Proof. The Jacobian of this curve has the rational 7-torsion point $(0,2) - \infty$ and the 5-torsion point $(1, \sqrt{-7}) - \infty$ defined over $\mathbb{Q}(\sqrt{-7})$. Twisting by -7 makes the 5-torsion point rational and the 7-torsion point defined over $\mathbb{Q}(\sqrt{-7})$. □

Remark 3.6.5. *This example arose by trying to find a $(7,7)$-subgroup (see Chapter 5).*

3.6.3 Order 42 over a quartic field

We now give an example of a Jacobian of a genus 2 curve defined over a quartic extension of $\mathbb{Q}$ with a point of order 42. Consider

$$\begin{aligned} A(x)^2 - h(x) &= \lambda x^6(x-1) \\ B(x)^2 - h(x) &= \mu(x-1)^7, \end{aligned} \tag{3.116}$$

with $\deg A, \deg B \leq 3$ and $\deg h = 7$. A solution to this would give an order 42 point on the Jacobian of the genus 3 curve $y^2 = h(x)$. We then try to degenerate to get a genus 2 curve. We find that if $\lambda = \mu$, then $\lambda x^6(x-1) - \mu(x-1)^7$ factors as

$$6\lambda(x-1)(x-1/2)(x^2-x+1)(x^2-x+1/3). \tag{3.117}$$

We can solve this with the constraints on the degrees of $A(x), B(x)$ by putting

$$\begin{aligned} A(x) &= \frac{1}{2}(G_1(x) + G_2(x)) \\ B(x) &= \frac{1}{2}(G_1(x) - G_2(x)), \end{aligned} \tag{3.118}$$

where

$$\begin{aligned} G_1(x) &= 6\lambda(x-1/2)(x^2-x+1/3) \\ G_2(x) &= (x-1)(x^2-x+1). \end{aligned} \tag{3.119}$$

Then define $h(x) = A(x)^2 - \lambda x^6(x-1)$. This is degree 7, and its discriminant has the factor

$$\lambda^4 + 43/9\lambda^3 + 68/243\lambda^2 - 94/243\lambda + 1/27, \tag{3.120}$$

which is an irreducible polynomial in λ. A simpler defining polynomial for the quartic number field $\mathbb{Q}(\lambda)$ is

$$m(t) = t^4 - t^3 - 7t^2 + t + 9. \tag{3.121}$$

Let α be a root of m; then $\lambda = (10\alpha^3 - 67\alpha - 63)/27 \in \mathbb{Q}(\alpha)$. Let $f(x)$ be the degree 5 polynomial resulting from removing the square factor from $h(x)$. Let

$$P_0 = \left(0, \frac{-4\alpha^3 - 5\alpha^2 + 35\alpha + 45}{18}\right), \tag{3.122}$$

$$P_1 = \left(1, \frac{7\alpha^3 - 2\alpha^2 - 42\alpha - 36}{18}\right) \tag{3.123}$$

be two points on the curve $\mathcal{C}\colon y^2 = f(x)$. Let $D_0 = P_0 - \infty$, $D_1 = P_1 - \infty$. Then we find that $7D_1 \sim 0$ and $6D_0 - D_1 \sim 0$. Consequently, $42D_0 \sim 0$. A direct calculation shows that this is the order of D_0.

This proves the following, in which we have multiplied f by 18^2 to clear denominators in the coefficients.

Proposition 3.6.6. *Let α be a root of the quartic* (3.121)*. The Jacobian of the curve*

$$\begin{aligned} y^2 = {} & (-120\alpha^3 + 804\alpha + 756)x^5 \\ & + (-4488\alpha^3 - 1068\alpha^2 + 30024\alpha + 32805)x^4 \\ & + (9302\alpha^3 + 2058\alpha^2 - 62114\alpha - 67356)x^3 \\ & + (-7677\alpha^3 - 1582\alpha^2 + 51134\alpha + 55125)x^2 \\ & + (2946\alpha^3 + 532\alpha^2 - 19526\alpha - 20862)x \\ & - 421\alpha^3 - 34\alpha^2 + 2733\alpha + 2808 \end{aligned} \tag{3.124}$$

has a point of order 42 defined over $\mathbb{Q}(\alpha)$.

Chapter 4

Kummer coordinates

4.1 Introduction

An explicit embedding of the Kummer variety of a curve provides many tools. For elliptic curves of the form $y^2 = f(x)$ where $f(x)$ is a cubic, the Kummer variety is the projective line above which the curve is a double cover. This encodes the x-coordinate of points. For genus 2 curves, the Kummer variety is a surface, which Flynn embedded into $\mathbb{P}^3$ using a single quartic equation ([Fly90b]). Recently, Bruin et al. used this explicit embedding of the Kummer variety of a family of genus 2 curves to do explicit descent ([BFT14]). They consider the family of genus 2 curves $\mathcal{C}$ admitting a rational copy of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ in $\mathcal{J}(\mathcal{C})[3]$. Let Σ be such a subgroup; then there is an isogeny $\varphi\colon \mathcal{J} \to \mathcal{J}/\Sigma$, given by $P \mapsto P + \Sigma$. The quotient $\mathcal{J}' \coloneqq \mathcal{J}/\Sigma$ is the Jacobian of another genus 2 curve, $\mathcal{C}'$, and they find an explicit equation for $\mathcal{C}'$.

To do this, they descend the map φ to the Kummer varieties $\mathcal{K}$ of $\mathcal{J}$ and $\mathcal{K}'$ of $\mathcal{J}'$. As we will see in Section 5.4.1, the explicit embedding of the Kummer variety of a genus 2 curve encodes the equation of the curve, up to twist. They then use this to find the equation of $\mathcal{C}'$ for $\mathcal{K}'$, and thus for $\mathcal{J}'$. Once they have the equation of the curve, they use the theory in [Sch98] to compute the Selmer groups of specific Jacobians in the family, and exhibit examples of Jacobians of genus 2 curves with nontrivial 3-part of Ш. We discuss this further in Chapter 5 and Chapter 6.

An explicit embedding of the Kummer variety can also give a theory of heights for Jacobians of curves. This is required to compute the Mordell–Weil group $\mathcal{J}(K)$ given a full rank subgroup. Flynn and Smart compute canonical heights for Jacobians of genus 2 curves using the Kummer embedding in [FS97].

Stoll derives an explicit embedding of the Kummer variety of genus 3 hyperelliptic curves and computes the theory of heights in [Sto17]. This improves upon earlier work by Stubbs in his thesis ([Stu00]) and Müller ([Mül14]).

Genus 3 curves are either hyperelliptic or smooth plane quartic. Genus 3 superelliptic curves form a subclass of the smooth plane quartics; assuming the characteristic is not 2 or 3, such curves have a model $y^3z = f(x, z)$, where f is homogeneous of degree four. In the following, we find an explicit embedding of the Kummer variety of genus 3 superelliptic curves.

4.2 Background

4.2.1 Embedding varieties into projective space

We first review how to embed varieties into projective space using line bundles. Let X be a variety over a field K, and let $\mathscr{L}$ be a line bundle on X. We say that $\mathscr{L}$ is *globally generated* if there are global sections $s_0, \ldots, s_n \in \Gamma(X, \mathscr{L})$ such that for every point $\mathfrak{p} \in X$, there is at least one s_i with $s_i \notin \mathfrak{m}_\mathfrak{p}\mathscr{L}_\mathfrak{p}$.

Let R be a ring, and let X be an R-scheme. Let $\mathscr{L}$ be a globally generated line bundle, and let $s_0, \ldots, s_n$ be global sections that generate it. There is a unique morphism $\varphi\colon X \to \mathbb{P}^n_R = \operatorname{Proj} R[x_0, \ldots, x_n]$ such that $\mathscr{L} \cong \varphi^*\mathscr{O}(1)$ and $s_i = \varphi^*(x_i)$ for each $i = 0, \ldots, n$.

Conversely, given a morphism $X \to \mathbb{P}^n_R$ of R-schemes, the pullback $\mathscr{L} = \varphi^*\mathscr{O}(1)$ is a line bundle and globally generated by the sections $s_i = \varphi^*(x_i)$ for $i = 0, \ldots, n$. Thus, morphisms $X \to \mathbb{P}^n_R$ are determined by globally generated line bundles. Note that such morphisms are defined over R. We are interested in morphisms $X \to \mathbb{P}^n_R$ that are embeddings. For this, we introduce the concept of a very ample line bundle.

Let X be an scheme over a ring R and let $\mathscr{L}$ be a line bundle on X. We say that $\mathscr{L}$ is *very ample relative to* R, if there is an embedding $\varphi\colon X \to \mathbb{P}^n_R$ such that $\mathscr{L} \cong \varphi^*(\mathscr{O}(1))$. We conclude that finding an embedding of a variety V into projective space is equivalent to finding a very ample line bundle $\mathscr{L}$ on V. Let K be a field, and let X be a K-scheme. If $\mathscr{L}$ is a subsheaf of the constant sheaf $K(X)$ of rational functions on X, then we have a simple interpretation of the morphism associated to $\mathscr{L}$. On a nonsingular K-variety, $\Gamma(X, \mathscr{L})$ is a finite dimensional vector space. Choose a basis $s_0, \ldots, s_n$ of $\Gamma(X, \mathscr{L})$; then the map to projective space is given by

$$x \mapsto [s_0(x)\colon \cdots \colon s_n(x)]. \tag{4.1}$$

We shall use this theory to embed the Kummer variety of a curve into projective space. We formally define the Kummer variety of a curve in Section 4.2.3.

Let V be a variety and let D be a divisor on V. Then we write $\mathscr{L}(D)$ for the line bundle associated to D, and we write $L(D)$ for the space $\Gamma(V, \mathscr{L}(D))$. We say a line bundle $\mathscr{L}$ is *ample* if $\mathscr{L}^m$ is very ample for some positive integer m.

If D is an ample divisor on an abelian variety A, then $3D$ is very ample (see [Mil, II.6]). Moreover, there is an ample divisor, denoted Θ, on A. Thus 3Θ is very ample, and we can use a basis for $\Gamma(\mathcal{J}(\mathcal{C}), \mathscr{L}(3\Theta))$ to embed the Jacobian. We discuss this space in Section 4.2.2.

For the Kummer, it suffices to use a basis for $L(2\Theta)$ (see [BL04, Section 4.7], for example). Thus we must find global sections of $\mathscr{L}(2\Theta)$ to embed the Kummer of a curve, and global sections of $\mathscr{L}(3\Theta)$ to embed the Jacobian of a curve.

We refer to [Mil] for standard facts about the theta divisor. Firstly, $\dim L(n\Theta) = n^g$. One can see this by using Riemann-Roch for abelian varieties. Let $h^i(\mathscr{L})$ denote the dimension of the cohomology group $H^i(A, \mathscr{L})$. Then the Euler characteristic is $\chi(\mathscr{L}) = \sum_{i=0}^{\infty}(-1)^i h^i(\mathscr{L})$. For an ample divisor $\mathscr{L}$, we have $h^i(\mathscr{L}) = 0$ for all $i > 0$. Let $(L)^n$ denote the nth self-intersection of L. Then Milne shows that $(\Theta)^g = g!$. The Riemann-Roch theorem for abelian varieties (Theorem 2.2.4) implies $\chi(\mathscr{L}) = (L)^g/g!$, and so we see that $\dim L(n\Theta) = n^g$, as required.

To find the explicit embedding corresponding to the line bundle $\mathscr{L}$, we must also find the relations between the basis of $\Gamma(X, \mathscr{L})$. In the case of an abelian variety, the corollary on page 349 of [Mum66] implies that $L(4\Theta)$ is defined by an intersection of quadrics. This also implies that the elements of $L(2\Theta)$ satisfy quartic relations, since quadratic combinations of elements of $L(2\Theta)$ lie in $L(4\Theta)$. See [Mül14] for more details.

Example 4.2.1. *Let E be an elliptic curve over a field K, given by the equation $y^2 = x^3 + Ax + B$, and let ∞ denote the identity point. Then the theta divisor can be taken as the point ∞. The global sections of the line bundle $\mathscr{L}(2\Theta)$ has K-basis $\{1, x\}$; indeed, 1 is regular on E, and x has a double pole at ∞. This agrees with the description of the Kummer variety being the copy of $\mathbb{P}^1$ that E is a double cover of. Moreover, the global sections of the line bundle $\mathscr{L}(3\Theta)$ has K-basis $\{1, x, y\}$. One can see that $\mathscr{L}(3\Theta)$ is very ample, since there is an embedding $y^2 = x^3 + Ax + B$, in terms of the global sections.*

Note, however, that we must go to $\mathscr{L}(4\Theta)$ in order to have the projective embedding be cut out by quadratic equations. Indeed, $\Gamma(E, \mathscr{L}(4\Theta)) = \{1, x, y, x^2\}$. Denoting these by z_0, z_1, z_2, z_3, respectively, we see that there is a projective embedding given by the two equations $z_2^2 = z_1 z_3 + A z_1 z_0 + B z_0^2$ and $z_1^2 = z_3 z_0$.

4.2.2 Divisors on normal varieties

We follow Wamelen ([Wam98]) and Iitaka ([Iit82]) for this subsection. Let V be a normal variety over a field K; that is, the stalks $\mathscr{O}_{V,\mathfrak{p}}$ are integrally closed domains for all $\mathfrak{p} \in V$. We define a *prime divisor* as an irreducible subvariety of V of codimension 1. We denote by $\operatorname{Div} V$ the abelian group of all finite formal linear combinations of prime divisors on V. Thus any *divisor* $D \in \operatorname{Div} V$ is of the form $\sum_Y n_Y Y$ for some $n_y \in \mathbb{Z}$, with all but finitely many n_Y equal to zero. We define the *degree* of D as $\deg D = \sum_Y n_Y$, and we write $\operatorname{Div}^n V \subset \operatorname{Div} V$ for the subset of degree n divisors of V. The degree-0 divisors, $\operatorname{Div}^0 V \subset \operatorname{Div} V$, are a subgroup.

Since V is normal, the local ring of a prime divisor is a discrete valuation ring, so each prime divisor Y comes with a valuation v_Y. Let $K(V)$ denote the function field of V. Then we can define the divisor of a function $f \in K(V)$ as

$$\operatorname{div} f = \sum_Y v_Y(f) Y, \tag{4.2}$$

where the sum ranges over all prime divisors $Y \subset V$. This sum is finite.

We say that two divisors D, D' are *linearly equivalent* if $D - D' = \operatorname{div} f$ for some $f \in K(V)$; in this case, we write $D \sim D'$. We say a divisor is *principal* if it is linearly equivalent to zero. Fix an algebraic closure $\overline{K}$ of K; the Galois group $\operatorname{Gal}(\overline{K}/K)$ acts on $\operatorname{Div} V$, and we define $\operatorname{Div}_K V$ as the subgroup $(\operatorname{Div} V)^{\operatorname{Gal}(\overline{K}/K)} \subset \operatorname{Div} V$ consisting of divisors that are fixed under this action.

We can compute pullbacks of divisors on normal varieties using the following theorems from [Iit82]. Let $\varphi\colon V \to W$ be a finite map of normal varieties. Let D be a divisor on W. Write $\varphi^{-1}(D) = \bigcup_{i=1}^r Y_i \cup \bigcup_{i=1}^s Z_i$, where $\varphi(Y_i)$ is dense in D for each i, and $\varphi(Z_i)$ is not dense in D for each i.

To each divisor D_i we associate a positive integer e_i called the *ramification index*. These satisfy the following theorem.

Theorem 4.2.2. *Let $\varphi\colon V \to W$ be as above. Then*

$$\sum_{i=1}^r e_i \deg(\varphi|_{Y_i}) = \deg \varphi. \tag{4.3}$$

We never need to explicitly compute the ramification indices, as they will turn out to be 1 whenever we compute pullbacks of divisors. The next theorem lets us compute $\varphi^*(D)$.

Theorem 4.2.3. *For $\varphi\colon V \to W$ as above, we have*

$$\varphi^*(D) = \sum_{i=1}^{r} e_i Y_i, \tag{4.4}$$

where e_i are the ramification indices.

Finally, we can compute the order of a function along certain divisors on a product variety using the following theorem.

Theorem 4.2.4. *Let V be a normal variety and let W be a nonsingular variety. Let $\pi_V\colon V \times W \to V$ be the projection to V. If D is a divisor on V and $\xi \in K(V)$, then*

$$\operatorname{ord}_{D\times W}(\pi_V^*\xi) = \operatorname{ord}_D \xi. \tag{4.5}$$

4.2.3 The Kummer variety of a curve

We now consider the situation above where the variety V is replaced by either a smooth curve $\mathcal{C}$ or the Jacobian $\mathcal{J}$ of a smooth curve. We refer to [Har77] for background material. In particular, by a *smooth curve*, we mean a noetherian normal integral separated scheme of dimension one. Divisors on $\mathcal{C}$ are finite formal linear combinations of points on $\mathcal{C}$.

We defined the Jacobian in Section 2.1. We write $\mathcal{O}$ for the identity element of $\mathcal{J}(\mathcal{C})$; that is, the class of all principal divisors on $\mathcal{C}$.

Definition 4.2.5. *We define the* Kummer *variety of $\mathcal{C}$ as $\mathcal{J}(\mathcal{C})/\langle -1\rangle$; that is, the quotient of $\mathcal{J}(\mathcal{C})$ by negation.*

Example 4.2.6. *For example, on the smooth plane quartic curve $\mathcal{C}\colon y^3z = x^4 + z^4$ contained in $\mathbb{P}^3$, we have the degree zero divisor $D = (0,1)+(0,\omega)+(0,\omega^2)-3(0\colon 1\colon 0)$, where ω is a primitive cube root of unity.*

Then D is rational, since it is fixed by the absolute Galois group of $\mathbb{Q}$. This is also the divisor of the function x/z on $\mathcal{C}$, since the points where x equals zero satisfy $z(y^3 - z^3) = 0$, and the points where $z = 0$ satisfy $x^4 = 0$. This shows $\operatorname{ord}_{(0,\omega^i)}(x) = 1$ for $i = 0, 1, 2$, and $\operatorname{ord}_{(0\colon 1\colon 0)}(x) = 1$, and also $\operatorname{ord}_{(0\colon 1\colon 0)}(z) = 4$. Thus

$$\operatorname{div}(x/z) = (0,1) + (0,\omega) + (0,\omega^2) - 3\infty, \tag{4.6}$$

so D is zero in the Jacobian of $\mathcal{C}$.

Write g for the genus of $\mathcal{C}$, and let $P_\infty \in \mathcal{C}(K)$ be a given point. We define the *theta divisor* with respect to the base point P_∞ as

$$\Theta_{P_\infty} \coloneqq \{\sum_{i=1}^{g-1} P_i - (g-1)P_\infty \colon P_i \in \mathcal{C}\} \subset \mathcal{J}(\mathcal{C}). \tag{4.7}$$

In words, Θ_{P_∞} is the subset of all points of $\mathcal{J}(\mathcal{C})$ that only require $g-1$ points to represent them with the base divisor $(g-1)P_\infty$. We drop the subscript P_∞ and just write Θ when the base point is clear.

We refer to [Mil] for basic properties of the theta divisor. Importantly, Θ is a prime divisor on the Jacobian; that is, a codimension one irreducible subvariety.

The symmetric group S_n acts on the fibre product $\mathcal{C}^n$ by permuting the factors. We define the *symmetric product* of a curve $\mathcal{C}$ as the quotient of $\mathcal{C}^n$ by this action. If K is a perfect field, with algebraic closure $\overline{K}$, then the K-points $(\operatorname{Sym}^n C)(K)$ are the formal sums of points $\sum_{i=1}^n P_i$ such that $P_i \in \mathcal{C}(\overline{K})$ for each $i = 1, \dots, n$ and such that the sum is fixed under the natural action of $\operatorname{Gal}(\bar{K}/K)$.

Let $D_0 \in \operatorname{Div}^g \mathcal{C}$ be a given divisor. We follow [Wam98] in defining the surjections

$$\mathcal{C}^g \xrightarrow{\pi} \operatorname{Sym}^g C \xrightarrow{I} \mathcal{J}(\mathcal{C}), \tag{4.8}$$

by $\pi \colon (P_1, \dots, P_g) \mapsto \sum_{i=1}^g P_i$, and $I \colon \sum_{i=1}^g P_i \mapsto \sum_{i=1}^g P_i - D_0$. We also define $\varphi = I \circ \pi$ as the composition $\mathcal{C}^g \to \mathcal{J}(\mathcal{C})$.

These maps are important for us, because we will understand functions on $\mathcal{J}(\mathcal{C})$ by pulling them back to functions on $\operatorname{Sym}^g \mathcal{C}$.

Lemma 4.2.7. *Let $\mathcal{C}$ be a nonsingular curve over a field K of genus g, and let $P_\infty \in \mathcal{C}(K)$ be a given point. Consider the maps in* (4.8) *with respect to the base divisor gP_∞. The map I is surjective and birational. Consequently* $\deg I = 1$. *Moreover,* $\deg \pi = g!$.

Proof. To see that $\deg \pi = g!$, note that if $\sum_{i=1}^g P_i \in \operatorname{Sym}^g \mathcal{C}$ is a point in the symmetric product with P_i distinct points in $\mathcal{C}(K)$, then there are $g!$ points in $\mathcal{C}^g$ that map to $\sum_{i=1}^g P_i$, each with multiplicity one. The set of such points in the symmetric product is open, and so the degree of π is $g!$.

For the result on I, we will show that if D is a point in the Jacobian of a nonsingular curve, then there is a unique effective divisor E over K of minimal degree $0 \le m \le g$ such that $E - mP_\infty \sim D$. This is also shown in [GPS00], but we give the argument

here for completeness. First note that the Riemann-Roch dimension $\ell(D+mP_\infty)$ can increase by either 0 or 1 as m increases by 1. Indeed,

$$\ell(D+(m+1)P_\infty)-\ell(D+mP_\infty)\geq 0, \tag{4.9}$$

and the Riemann-Roch formula gives

$$\begin{aligned}\ell(D+(m+1)P_\infty)-\ell(D+mP_\infty) &= \ell(\kappa-D-(m+1)P_\infty)\\ &\quad +(m+1)+1-g \qquad (4.10)\\ &\quad -\ell(\kappa-D-mP_\infty)-m-1+g\\ &= \ell(\kappa-D-(m+1)P_\infty)\\ &\quad -\ell(\kappa-D-mP_\infty)+1 \qquad (4.11)\\ &\leq 1, \qquad (4.12)\end{aligned}$$

since $\ell(\kappa-D-(m+1)P_\infty)\leq\ell(\kappa-D-mP_\infty)$.

Since $D\in\operatorname{Div}^0\mathcal{C}$, then $\ell(D)>0$ if and only if D is principal: for any $f\in L(D)$, we have $\operatorname{div} f+D\geq 0$, but then by degrees we see that $\operatorname{div} f+D=0$, so D is principal. In this case, we can take $m_0=0$. We may thus assume that D is not principal. The Riemann-Roch formula shows that $\ell(D+gP_\infty)\geq 1$, and so there must exist a minimal m such that $\ell(D+mP_\infty)>0$; let m_0 denote the minimal such m. Let f be a nonzero element of $L(D+m_0P_\infty)$, and define $E\coloneqq\operatorname{div}(f)+D+m_0P_\infty$. Then $E\geq 0$, and $D\sim E-m_0P_\infty$. By construction, E is the unique divisor of minimal degree with this property: we already showed $\ell(D+mP_\infty)$ increases by at most 1 when m increases by 1, and for $m<m_0$, we have $\ell(D+mP_\infty)=0$.

Let $D\in\operatorname{Div}^0\mathcal{C}$. We have just shown that there is an effective divisor $E\in\operatorname{Div}\mathcal{C}$ of degree at most g such that $E-(\deg E)P_\infty\sim D$. Thus $E+(g-\deg E)P_\infty\in\operatorname{Sym}^g\mathcal{C}$ maps to D under I. Hence I is surjective.

Since Θ is precisely the subset of $D\in\mathcal{J}(\mathcal{C})$ for which the minimal degree m is at most $g-1$, this shows that points in $\mathcal{J}(\mathcal{C})\setminus\Theta$ have precisely one preimage in $\operatorname{Sym}^g\mathcal{C}$ (since the effective divisor E is unique). Thus I is bijective between an open subset of $\operatorname{Sym}^g\mathcal{C}$ and the open subset $\mathcal{J}(\mathcal{C})\setminus\Theta$ of $\mathcal{J}(\mathcal{C})$. □

4.2.4 Functions on $\mathcal{J}(\mathcal{C})$

As noted by Wamelen ([Wam98]), since the map $I\colon\operatorname{Sym}^g\mathcal{C}\to\mathcal{J}(\mathcal{C})$ is birational, the function fields of $\operatorname{Sym}^g\mathcal{C}$ and $\mathcal{J}(\mathcal{C})$ are isomorphic, and so to study functions on $\mathcal{J}(\mathcal{C})$ we may instead study functions on $\operatorname{Sym}^g\mathcal{C}$. Explicitly, I induces the map $K(\mathcal{J}(\mathcal{C}))\xrightarrow{\sim}K(\operatorname{Sym}^g\mathcal{C})$ given by pullback: $(\xi\colon\mathcal{J}(\mathcal{C})\to K)\mapsto(\xi\circ I\colon\operatorname{Sym}^g\mathcal{C}\to K)$.

Since it is easier to study functions on $\mathrm{Sym}^g \mathcal{C}$, it is more helpful to have an explicit map in the other direction. This is provided by Lemma 4.2.7, which gives a map

$$\begin{aligned} I' \colon \mathcal{J}(\mathcal{C}) \setminus \Theta_{P_\infty} &\to \mathrm{Sym}^g \mathcal{C} \\ D &\mapsto \sum_{i=1}^{g} P_i, \end{aligned} \tag{4.13}$$

where $\sum_{i=1}^{g} P_i$ is the unique effective divisor of degree g from the lemma such that $D \sim \sum_{i=1}^{g} P_i - gP_\infty$. Since $\mathcal{J}(\mathcal{C}) \setminus \Theta_{P_\infty}$ is an open subset of $\mathcal{J}(\mathcal{C})$, this gives a natural map $I'^* \colon K(\mathrm{Sym}^g \mathcal{C}) \to K(\mathcal{J}(\mathcal{C}))$.

Motivated by the discussion at the start of this section, we want to compute $L(n\Theta)$ on $\mathcal{J}(\mathcal{C})$. It is easier, however, to work with functions on $\mathrm{Sym}^g \mathcal{C}$, so we first determine what $L(n\Theta)$ corresponds to in $K(\mathrm{Sym}^g \mathcal{C})$. Write $\mathcal{O}'$ for the divisor $I^{-1}(\mathcal{O})$ on $\mathrm{Sym}^g \mathcal{C}$. Every divisor on $\mathrm{Sym}^g \mathcal{C}$ is mapped with degree 1 to a divisor on $\mathcal{J}(\mathcal{C})$, except for $\mathcal{O}'$, which is mapped to the point $\mathcal{O} \in \mathcal{J}(\mathcal{C})$. We can thus ignore poles along $\mathcal{O}'$ of functions on $\mathrm{Sym}^g \mathcal{C}$ when considering them as functions on $\mathcal{J}(\mathcal{C})$.

Let $\xi \in K(\mathrm{Sym}^g \mathcal{C})$. Then $I'^*\xi$ is a function on $\mathcal{J}(\mathcal{C})$, and has divisor $\operatorname{div} I'^*\xi = I'^* \operatorname{div} \xi$. At any divisor D of $\mathrm{Sym}^g \mathcal{C}$ except $\mathcal{O}'$, we have $I'^* D = I'^{-1}(D) = I(D)$. Thus $\operatorname{div} I'^*\xi = \sum_{D \neq \mathcal{O}'} n_D I(D)$, where n_D is the order of ξ along D.

There is also a natural injection $K(\mathrm{Sym}^g \mathcal{C}) \hookrightarrow K(\mathcal{C}^g)$, given by pullback by π. The image of the map consists of functions on $\mathcal{C}^g$ invariant under the action of the symmetric group S_g on the factors of $\mathcal{C}^g$.

Remark 4.2.8. *These are also known as multisymmetric functions. In the language of [Vac05], the function field $K(\mathrm{Sym}^g \mathcal{C})$ is denoted $A_K(g, 2)$.*

Suppose that the curve has an affine model $f(x, y) = 0$, with coordinates x, y. Let $P_i = (x_i, y_i)$ in $(P_1, \ldots, P_g) \in \mathcal{C}^g(K)$. Then a function in $K(\mathrm{Sym}^g \mathcal{C})$ is an element of $K(x_1, y_1, \ldots, x_g, y_g)^{S_g}$.

Example 4.2.9. *Let $\mathcal{C} \colon y^2 = f_6(x)$ be a genus 2 hyperelliptic curve. Then the function $x_1 + x_2 \in K(\mathcal{C}^2)$ is invariant under the action of S_2, and so in fact lies in $K(\mathrm{Sym}^2 \mathcal{C})$. Note that the symmetric functions on $\mathcal{C}^2$ are not just generated by the elementary symmetric functions in x_1, x_2 and y_1, y_2 respectively. For example, $x_1 y_1 + x_2 y_2$ is symmetric, but not a polynomial combination of $x_1 + x_2, x_1 x_2, y_1 + y_2, y_1 y_2$.*

4.2.5 Computing divisors of functions on $\mathcal{J}(\mathcal{C})$

We now discuss how to compute divisors of functions on $\mathcal{J}(\mathcal{C})$, mainly following [Wam98]. First fix a base divisor $D_0 \in \mathrm{Div}^g \mathcal{C}$, so that the map I is given by

$\sum_{i=1}^{g} P_i \mapsto \sum_{i=1}^{g} P_i - D_0$. Usually, $D_0 = gP_\infty$ for some point $P_\infty \in \mathcal{C}(K)$. Then the degree of the first map is $g!$ and the degree of the second is 1. To compute the order of a divisor on $\mathcal{J}(\mathcal{C})$, we compute its order on one of the factors $\mathcal{C}$ of the fibre product $\mathcal{C}^g$, and then use the formulas from before. Recall that φ is the composition $\mathcal{C}^g \xrightarrow{\pi} \operatorname{Sym}^g \mathcal{C} \xrightarrow{I} \mathcal{J}(\mathcal{C})$. We aim to compute $\varphi^* D$, for divisors D of $\mathcal{J}$, since then we will be able to read off the order of our function along $\varphi^* D$.

This allows us to compute $\operatorname{div}(\xi)$ for certain functions ξ on $\mathcal{C}^g$. Let $Q \in \mathcal{C}(K)$ be a point, and let $\pi_1 \colon \mathcal{C}^g \to \mathcal{C}$ denote projection to the first factor. If D is a divisor on $\mathcal{C}^g$ of the form $\{Q\} \times \mathcal{C}^{g-1}$, then $\operatorname{ord}_D(\pi_1^* \eta) = \operatorname{ord}_Q(\eta)$, where $\eta \in K(\mathcal{C})$ is any function such that $\pi_1^* \eta = \xi$.

4.2.6 How to compute $\operatorname{ord}_\Theta \xi$ for a function ξ on $\mathcal{J}(\mathcal{C})$

The proof of the following lemma is inspired by the proof of Theorem 4 in [Wam98].

Lemma 4.2.10. *Suppose Θ is given with respect to the base point $P_\infty \in \mathcal{C}(K)$, and that $D_0 = gP_\infty$ is the basepoint for I. For each $i = 1, \ldots, g$, define*

$$T_i = \mathcal{C} \times \cdots \times \{P_\infty\} \times \cdots \times \mathcal{C}, \tag{4.14}$$

where P_∞ appears in the ith factor. Then $\varphi^*(\Theta) = \sum_{i=1}^{g} T_i$.

Proof. The T_i are prime divisors on $\mathcal{C}^g$ and we have $T_i \subset \varphi^{-1}(\Theta)$ for each i. Moreover, $\varphi(T_i)$ is dense in Θ for each i. By Theorem 4.2.3, there are prime divisors Y_j on $\mathcal{C}^g$ such that $\varphi(Y_j)$ is dense in Θ, such that

$$\varphi^*(\Theta) = \sum_{i=1}^{g} e_i T_i + \sum_j f_j Y_j. \tag{4.15}$$

By Theorem 4.2.2,

$$\sum_{i=1}^{g} e_i (\deg \varphi|_{T_i}) + \sum_j f_j (\deg \varphi|_{Y_j}) = \deg \varphi = g!. \tag{4.16}$$

Moreover, $\deg(\varphi|_{T_i}) = (g-1)!$ for each i. Thus $e_i = 1$ for $i = 1, \ldots, g$. We conclude that there are no Y_j, and so

$$\varphi^*(\Theta) = \sum_{i=1}^{g} T_i. \tag{4.17}$$

□

Let ξ be a function on $\mathcal{J}(\mathcal{C})$. We can compute $\mathrm{ord}_\Theta(\xi)$ as follows. Since $\varphi^*(\Theta) = \sum_{i=1}^g T_i$, it suffices to compute the order of $\varphi^*(\xi)$ along $\varphi^*(\Theta)$. We first compute the order of $\varphi^*(\xi)$ along T_1 (the order is the same along any T_i, by symmetry). For this, we find a function η on $\mathcal{C}$ such that $\pi_1^*\eta = \xi$, where $\pi_1 \colon \mathcal{C}^g \to \mathcal{C}$ is the projection to the first factor. Thus the problem reduces to finding $\mathrm{ord}_{P_\infty} \eta$, where P_∞ is the basepoint for Θ.

Example 4.2.11. *Let $\mathcal{C} \colon y^2 = f_5(x)$ be a genus 2 hyperelliptic curve. Then ∞ is a rational point on $\mathcal{C}$, and we let Θ denote the theta divisor with base point ∞. Let ξ be the function $y_1 + y_2$ on $\mathrm{Sym}^2 \mathcal{C}$, and by abuse of notation consider it also as a function on $\mathcal{J}(\mathcal{C})$. Let $\pi_i \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ denote the projection from the ith factor; then $y_i = \pi_i^* y$. We use that $\varphi^*\Theta = \sum_{i=1}^g T_i$ as before, and recall that to compute $\mathrm{ord}_\Theta \xi$ it suffices to compute $\mathrm{ord}_{T_1} \xi$. Then $\mathrm{ord}_{T_1}(\pi_i^* y) = \mathrm{ord}_\infty(y) = -5$. Moreover, $\mathrm{ord}_{T_1}(y_2) = 0$, and so $\mathrm{ord}_{T_1}(y_1 + y_2) = -5$, whence $\mathrm{ord}_\Theta(y_1 + y_2) = -5$.*

The following lemma is useful for computations.

Lemma 4.2.12 (Hyperelliptic odd degree case)**.** *Let $\mathcal{C} \colon y^2 = f(x)$ be a hyperelliptic curve of genus g, with $\deg f = 2g - 1$. Define the following weight on functions on $\mathrm{Sym}^g \mathcal{C}$. Since the functions are symmetric, we need only define w on x_1, y_1:*

$$\begin{aligned} w(x_1) &= \mathrm{ord}_\infty(x) \\ w(y_1) &= \mathrm{ord}_\infty(y), \end{aligned} \tag{4.18}$$

and extend to monomials additively. Then extend to polynomials as a valuation, and extend to rational functions by $w(g/h) = w(g) - w(h)$. Then $\mathrm{ord}_\Theta(\xi) = w(\xi)$.

Proof. It suffices to show that $\mathrm{ord}_\Theta(\xi) = w(\xi)$ for functions in the coordinate ring of $\mathrm{Sym}^g \mathcal{C}$. These can be written as sums of monomials, and the order of the pole at Θ is simply the order of the pole along T_1, which is the weight as described above. □

4.2.7 How to show that a function is regular away from Θ

Showing that a function is regular away from Θ is usually straightforward. We give an example to illustrate this, with this particular idea originating in [Wam98].

Example 4.2.13. *Let $\mathcal{C} \colon y^2 = f(x)$, where $\deg f = 5$ be a genus 2 curve, and consider the function $\xi = (y_1 - y_2)/(x_1 - x_2)$ on $\mathrm{Sym}^2 \mathcal{C}$. Then $\mathcal{C}$ has a unique rational point at infinity, denoted ∞. Consider the theta divisor with base point ∞. Then $\mathrm{ord}_\Theta \xi =$*

$\operatorname{ord}_{T_1}\xi$, *as before. Since* $y_1 - y_2$ *has a pole of order 5 along* Θ *and* $x_1 - x_2$ *has a pole of order 2 along* Θ*, it follows that* ξ *has a pole of order 3 along* Θ*.*

The only other possible subset of $\operatorname{Sym}^2 \mathcal{C}$ *on which* ξ *can have a pole is* $U = \{P_1 + P_2 \colon x_1 = x_2\}$*. This decomposes into two irreducible divisors* $D_1 \cup D_2$*, where*

$$D_1 = \{P_1 + P_2 \colon x_1 = x_2, y_1 = y_2\} \tag{4.19}$$

$$D_2 = \{P_1 + P_2 \colon x_1 = x_2, y_1 = -y_2\}. \tag{4.20}$$

Now, $D_2 = I^{-1}(\mathcal{O})$ *is the inverse image of the identity point of the Jacobian, and so* $I(D_2)$ *is not dense in any divisor of* $\mathcal{J}(\mathcal{C})$*. Consequently, considering* ξ *as a function on the Jacobian, the divisor* $I(D_2)$ *does not contribute to* $\operatorname{div}\xi$*. However,* $I(D_1)$ *is a prime divisor of* $\mathcal{J}(\mathcal{C})$*, and so we do have to show that* ξ *is regular on* $I(D_1)$*. Write*

$$\xi = \frac{y_1 - y_2}{x_1 - x_2} = \frac{y_1^2 - y_2^2}{(x_1 - x_2)(y_1 + y_2)} = \frac{f(x_1) - f(x_2)}{x_1 - x_2}\frac{1}{y_1 + y_2}. \tag{4.21}$$

Now, $1/(y_1 + y_2)$ *is regular on* D_1*, and* $x_1 - x_2$ *divides* $f(x_1) - f(x_2)$*; thus* ξ *is regular on* D_1*, and so also on* $I(D_1)$*.*

4.3 The Kummer embedding in genus 2

Throughout this section, $\mathcal{C}$ denotes a genus 2 hyperelliptic curve with a model of the form $y^2 = f(x)$, with $f(x)$ degree five or six. We write $\mathcal{K}$ for its Kummer surface and $\mathcal{J}$ for its Jacobian.

4.3.1 The Theta divisor

To embed the Kummer and Jacobian we require a basis for $\mathscr{L}(2\Theta)$ and $\mathscr{L}(4\Theta)$, respectively. However, Θ is defined relative to a basepoint, so if $\mathcal{C}(K) = \emptyset$, then Θ is not rationally defined. Instead, we look for another very ample divisor that is rationally defined. We write Θ^+ for the theta divisor with base point ∞^+, and Θ^- for that with base point ∞^-. Then note that $\Theta^+ + \Theta^-$ is defined over K, since it is fixed by the action of Galois.

Moreover, $\Theta^+ + \Theta^-$ is ample, and $2(\Theta^+ + \Theta^-)$ is very ample, so we can use $\mathscr{L}(2(\Theta^+ + \Theta^-))$ to embed $\mathcal{J}(\mathcal{C})$, and $\mathscr{L}(\Theta^+ + \Theta^-)$ to embed the Kummer. We are reduced to finding bases for each of these spaces, and then finding the polynomial relations between them.

4.3.2 Poles along Θ

Lemma 4.3.1. *For a hyperelliptic curve $\mathcal{C}\colon y^2 = f(x)$ of genus g, defined over a field K, the divisor $\Theta^+ + \Theta^-$ is K-rational. Moreover, the order of the pole of the function $\xi \in K(\mathcal{C})$ at $\Theta^+ + \Theta^-$ is given by the weight*

$$\begin{aligned} w(x_1) &= 2 \\ w(y_1) &= \deg f. \end{aligned} \tag{4.22}$$

This is extended to monomials, then polynomials, then rational functions.

Proof. This follows, since

$$\begin{aligned} w(x) &= -\operatorname{ord}_{\infty^+}(x) - \operatorname{ord}_{\infty^-}(x) = 2 \\ w(y) &= -\operatorname{ord}_{\infty^+}(y) - \operatorname{ord}_{\infty^-}(y) = \deg f. \end{aligned} \tag{4.23}$$

□

4.3.3 Some algorithms for computing with polynomials

The following algorithms for computing relations between polynomials are not believed to be novel, but we give them for completeness and clarity.

Computing linear relations between polynomials We first give some algorithms for computing relations between polynomials. Let $\mathbf{x} = (x_1, \ldots, x_r)$ be a vector of indeterminates, and let $K[\mathbf{x}]$ be the polynomial ring over K generated by $x_1, \ldots, x_r$. Suppose $p_1(\mathbf{x}), \ldots, p_n(\mathbf{x}) \in K[\mathbf{x}]$. We often want to compute the relations between these polynomials. For example, the linear relations can be described by $\mathbf{v} \in K^n$ such that $v_1 p_1(\mathbf{x}) + \cdots + v_n p_n(\mathbf{x}) = 0$. This is a subspace of the vector space K^n.

Given a set of polynomials $p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})$, we first list all monomials $m_1, \ldots, m_k$ occurring in the $p_i(\mathbf{x})$. Then form the k-dimensional K-vector space V with basis $m_1, \ldots, m_k$. For a monomial $m \in K[x_1, \ldots, x_r]$, let $c_m\colon K[x_1, \ldots, x_r] \to K$ be the function that takes a polynomial $p(\mathbf{x})$ to the coefficient of m in $p(\mathbf{x})$. The monomials $(m_1, \ldots, m_k)$ define a map

$$\begin{aligned} \varphi_{m_1,\ldots,m_k}\colon K[x_1, \ldots, x_r] &\to V \\ p(x) &\mapsto (c_{m_1}(p), \ldots, c_{m_k}(p)). \end{aligned} \tag{4.24}$$

Given n polynomials $p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})$, we can form an $n \times k$ matrix M with rows the vectors $\varphi_{m_1,\ldots,m_k}(p_i(x))$; we have $M_{ij} = c_{m_j}(p_i)$. Any linear combination $v_1 p_1 + \cdots + v_n p_n$ of the p_i contains only the monomials $m_1, \ldots, m_k$; moreover, $v_1 p_1 + \cdots + v_n p_n = 0$

if and only if $c_{m_i}(v_1p_1 + \cdots + v_np_n) = 0$ for all $i = 1, \ldots, k$; that is, if and only if $v_1c_{m_i}(p_1) + \cdots + v_nc_{m_i}(p_n) = 0$ for all $i = 1, \ldots, k$. In particular, $\mathbf{v} = (v_1, \ldots, v_n)$ satisfies $vM = 0$. Thus the relations between the p_i are the vectors in the left nullspace of M.

Algorithm: Compute linear relations between polynomials
Input: Polynomials $p_i(\mathbf{x})$ for $i = 1, \ldots, n$ over a field K.
Output: Basis for the subspace of $\mathbf{v} \in K^n$ such that $v_1p_1 + \cdots + v_np_n = 0$.
Compute the monomials $m_1, \ldots, m_k$ occurring in $p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})$
For each $1 \leq i \leq n, 1 \leq j \leq k$, let $M_{ij} = \texttt{Coefficient}(p_i, m_j)$
Compute the left nullspace: $\mathbf{v} \in K^n$ such that $\mathbf{v}M = 0$
Return a basis for the left nullspace

Algorithm 1: Compute linear relations between polynomials

Computing higher degree relations between polynomials To compute all degree d relations between the polynomials $p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})$, we would first compute all degree d combinations of the p_i, and then compute the linear relations between these.

Example 4.3.2. *Let $p_1(x_1, x_2) = x_1 - x_2, p_2(x_1, x_2) = x_1 + x_2, p_3(x_1, x_2) = x_1x_2$, and consider the linear relations between the polynomials $p_1, p_2, p_3, p_1^2, p_1p_2, p_1p_3, p_2^2, p_2p_3, p_3^2$. The monomials occurring are $x_1, x_2^2, x_2, x_1^2x_2^2, x_1^2x_2, x_1^2, x_1x_2^2, x_1x_2$, and the matrix M is*

$$M = \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{4.25}$$

We check the left nullspace is 1-dimensional, generated by $(0, 0, 4, 1, 0, 0, -1, 0, 0)$. This corresponds to $4p_3 + p_1^2 - p_2^2 = 0$.

Computing relations in function fields We want to apply these algorithms not just to polynomials but to functions on varieties. We assume such functions have a representative in a polynomial ring $K[\mathbf{x}]$. If we can define a reduction of such polynomials to a unique element in $K[\mathbf{x}]$, then we can simply apply the above algorithms to the reduced polynomials. If the functions lie in the function field $K(\mathbf{x})$, then we first multiply all the functions by their least common denominator and instead compute relations between polynomials.

On a curve of the form $\mathcal{C}\colon y^n = f(x)$, we can reduce any polynomial in $K[x,y]$ by repeatedly replacing y^n by $f(x)$ until the maximum degree of y that occurs is at most $n-1$. For functions on the symmetric product $\mathrm{Sym}^g \mathcal{C}$, we do this to y_i for each $i = 1, \ldots, g$ using $y_i^n = f(x_i)$.

Example 4.3.3. *Consider the genus 2 hyperelliptic curve* $\mathcal{C}\colon y^2 = x^5+1$. *The function* $\eta = y^3 - x + 1$ *reduces to* $y(x^5+1) - x + 1 = x^5 y + y - x + 1$.

Computing the symmetric and antisymmetric subspace Let $\mathcal{C}\colon y^n = f(x)$ be a superelliptic curve, with $n \geq 2$. To compute functions on $\mathrm{Sym}^g \mathcal{C}$ we will need to compute the subspace of symmetric polynomials and the subspace of antisymmetric polynomials. Recall that the symmetric group S_g acts on $K[x_1, y_1, \ldots, x_g, y_g]$ by permuting the indices of x_i and y_i; if $p \in K[x_1, y_1, \ldots, x_g, y_g]$ and $\sigma \in S_g$, then we write ${}^\sigma p$ for this action. We say $p \in K[x_1, y_1, \ldots, x_g, y_g]$ is *symmetric* if ${}^\sigma p = p$ for all $\sigma \in S_g$ and that it is *antisymmetric* if ${}^\sigma p = -p$ for all $\sigma \in S_g^-$, where S_g^- denotes the subset of odd permutations in S_g.

Let V be the vector space spanned by the monomials $m_1, \ldots, m_k$. Then the symmetric polynomials spanned by $m_1, \ldots, m_k$ are a subspace, which we denote by V^+; the antisymmetric polynomials spanned by $m_1, \ldots m_k$ are also a subspace, which we denote by V^-.

By explicitly computing the action of the permutation $\sigma \in S_g$ on the monomials, we can define a linear map on $\varphi_\sigma\colon V \to V$. For the symmetric subspace, we require $\varphi_\sigma(v) = v$ for all $\sigma \in S_g$; for the antisymmetric subspace we require $\varphi_\sigma(v) = -v$ for all $\sigma \in S_g^-$. Thus

$$V^+ = \bigcap_{\sigma \in S_g} \ker(\varphi_\sigma - \mathrm{id}) \tag{4.26}$$

$$V^- = \bigcap_{\sigma \in S_g^-} \ker(\varphi_\sigma + \mathrm{id}), \tag{4.27}$$

where id denotes the identity map $V \to V$.

See [Nic18] `vector_space_polynomials.m` for an implementation of this in MAGMA.

4.3.4 Method to find $\mathscr{L}(n\Theta)$

We first construct some functions in $\mathscr{L}_J(n\Theta)$ and then show that this gives all functions. Let $\Delta = \{2P\colon P \in \mathcal{C}\} \subset \mathrm{Sym}^2 \mathcal{C}$ and let $\mathcal{O}' = \{P + \iota(P)\colon P \in \mathcal{C}\} \subset \mathrm{Sym}^2 \mathcal{C}$, where $\iota\colon \mathcal{C} \to \mathcal{C}$ is the hyperelliptic involution sending (x,y) to $(x,-y)$. Then Δ and $\mathcal{O}'$ are both divisors of $\mathrm{Sym}^2 \mathcal{C}$, but $\mathcal{O}'$ gets blown down to a point on $\mathcal{J}$.

Let $d = x_1 - x_2$ and consider an arbitrary $g \in K[x_1, y_1, x_2, y_2]$. If the function g/d^m is symmetric, then it is regular on $\mathrm{Sym}^2 \mathcal{C}$ apart from poles along Δ and $\mathcal{O}'$ of weight at most m and a pole along Θ of order $n = w(g) - mw(d)$. This gives an element of $\mathscr{L}_J(n\Theta + m\Delta)$. We fix the pole along Δ by imposing that g has a zero along Δ of weight at least m. For such a g, we have $g/d^m \in \mathscr{L}_J(n\Theta)$. Our strategy is to search for such g by increasing m until we find the full space.

Lemma 4.3.4. *Let $d = x_1 - x_2$ and let $\varphi \in L_{\mathcal{J}}(n\Theta)$. Then there is $m \geq 0$ and $g \in K[x_1, y_1, x_2, y_2]^{S_2}$ such that φ equals g/d^{2m} in $K(\mathrm{Sym}^2 \mathcal{C})$ and g has a zero along Δ of order at least $2m$.*

Proof. Let $\mathcal{C}_0 \colon y^2 = f(x)$ denote the affine curve consisting of just the affine coordinate chart. Then $\mathrm{Sym}^2 \mathcal{C}_0$ is an open subset of $\mathrm{Sym}^2 \mathcal{C}$ and $\Theta \cap \mathrm{Sym}^2 \mathcal{C}_0 = \emptyset$. Functions on $\mathrm{Sym}^2 \mathcal{C}_0$ are precisely symmetric functions in $K(x_1, y_1, x_2, y_2)$. Moreover, if a function on $\mathrm{Sym}^2 \mathcal{C}_0$ has no poles, then it is regular, meaning that it lies in $K[x_1, y_1, x_2, y_2]^{S_2}$.

Let h represent φ on $\mathrm{Sym}^2 \mathcal{C}$; then $h \in L_{\mathrm{Sym}^2 \mathcal{C}}(n\Theta + k\mathcal{O}')$ for some $k \in \mathbb{Z}$, since $\mathcal{O}'$ gets blown down to a point on $\mathcal{J}$ but is a divisor on $\mathrm{Sym}^2 \mathcal{C}$.

If $k \geq 0$, then h potentially has a pole along $\mathcal{O}'$ of order k. Let $m = k$. Then d^{2m} is symmetric, and $hd^{2m} \in L_{\mathrm{Sym}^2 \mathcal{C}}(n\Theta - 2m\Delta) \subseteq L_{\mathrm{Sym}^2 \mathcal{C}}(n\Theta)$.

If $k < 0$, then h only has poles along Θ, and is forced to have a zero of order $-k$ along $\mathcal{O}'$. It follows that $h \in L_{\mathrm{Sym}^2 \mathcal{C}}(n\Theta)$. In this case we take $m = 0$.

Thus in either case there is $m \geq 0$ such that hd^{2m} is regular away from Θ on $\mathrm{Sym}^2 \mathcal{C}$. Consider the restriction of hd^{2m} to the affine chart $\mathrm{Sym}^2 \mathcal{C}_0$. Since $\Theta \cap \mathrm{Sym}^2 \mathcal{C}_0 = \emptyset$, the function hd^{2m} is regular, and thus has a representative $g \in K[x_1, y_1, x_2, y_2]^{S_2}$. Moreover, g has a zero of order $2m$ along Δ since h is regular along Δ and d^2 has a zero of order 2 along Δ. □

Remark 4.3.5. *To make the above lemma easier to state, we used the denominator d^{2m}, so that the power of d is always even and d^{2m} is symmetric. To avoid working with such large m it is sometimes helpful to use g/d^m where m can be odd; in this case, g should be symmetric if m is even and antisymmetric if m is odd.*

Thus if $\varphi \in L_{\mathcal{J}}(n\Theta)$, then $\varphi \in \bigcup_{m \geq 0} \{g/d^{2m} \colon g \in L_{\mathrm{Sym}^2 \mathcal{C}}(n\Theta - 2m\Delta)\}$. Also recall $\dim L_{\mathcal{J}}(n\Theta) = n^2$ for the Jacobian $\mathcal{J}$ of the genus 2 curve $y^2 = f(x)$. We will use this in Algorithm 2, but we first discuss how to compute the functions g that have a zero along Δ of a given order.

Functions with zeroes along Δ Let $\mathcal{C}$ be the hyperelliptic curve with affine coordinate chart $\mathcal{C}_0\colon y^2 = f(x)$. Then $\mathrm{Sym}^2 \mathcal{C}_0$ is an open affine subset of $\mathrm{Sym}^2 \mathcal{C}$, and so functions on $\mathrm{Sym}^2 \mathcal{C}_0$ determine functions on $\mathrm{Sym}^2 \mathcal{C}$.

Let w be the weight function $w(x) = 2$, $w(y) = \deg f$, giving the order of the pole along Θ of any polynomial. Let $V(w, N)$ be the vector space of monomials in x_1, y_1, x_2, y_2 of weight at most N. This is a finite subspace of $K[x_1, y_1, x_2, y_2]$. Recall we can reduce functions in this polynomial ring modulo $y^2 = f(x)$.

For any finite-dimensional subspace $U \subset K[x_1, y_1, x_2, y_2]$ and integer $N \geq 0$, let $U(-N\Delta)$ denote the subspace of functions that have a zero of order at least N along Δ. We can compute the order of a polynomial $g \in K[x_1, y_1, x_2, y_2]$ along Δ by putting $x_2 = x_1 + \varepsilon$ where ε is a formal parameter. Then y_2 is determined by $y_2^2 = f(x_2) = f(x_1 + \varepsilon)$; we know which root to take for y_2 since y_2 is near y_1 on Δ. Using Taylor series, we get

$$y_2^2 = f(x_1) + \varepsilon f'(x_1) + \frac{\varepsilon}{2} f''(x_1) + \cdots \tag{4.28}$$

$$= y_1^2 (1 + \varepsilon \frac{f'(x_1)}{f(x_1)} + \varepsilon^2 \frac{f''(x_1)}{2f(x_1)} f''(x_1) + \cdots). \tag{4.29}$$

Since $y_2 \approx y_1$, we get

$$y_2(\varepsilon) = y_1 (1 + \varepsilon \frac{f'(x_1)}{f(x_1)} + \varepsilon^2 \frac{f''(x_1)}{2f(x_1)} f''(x_1) + \cdots)^{1/2}, \tag{4.30}$$

and we finally just use the Taylor series for $(1 + \eta)^{1/2}$ to expand the right hand side. Then we compute the order of ε in $g(x_1, y_1, x_1 + \varepsilon, y_2(\varepsilon))$. We may need many terms of the Taylor series to compute the order.

We can compute $U(-N\Delta)$ as follows. First take a basis $g_1, \ldots, g_r$ of functions in U. Then $g_i(x_1, y_1, x_1 + \varepsilon, y_2(\varepsilon))$ is a polynomial in $K[x_1, y_1][\varepsilon]$. For $j = 0, \ldots, N-1$, define $g_{ij}(x_1, y_1)$ as the coefficient of ε^j in $g_i(x_1, y_1, x_1 + \varepsilon, y_2(\varepsilon))$. The conditions that $g_{ij} = 0$ for $i = 1, \ldots, r$ and $j = 0, \ldots, N-1$ define a subspace of U.

Computing $L(n\Theta)$ Algorithm 2 computes a basis for $L(n\Theta)$ on the Jacobian of the genus 2 hyperelliptic curve $y^2 = f(x)$.

Remark 4.3.6. *The algorithm necessarily terminates, because if $\varphi_1, \ldots, \varphi_N$ is a basis of $L(n\Theta)$, then for each φ_i there is a corresponding g_i from Lemma 4.3.4; this arises from some finite m_i in the lemma. Since the basis is finite, the algorithm finds the basis with m up to the maximum m_i.*

Algorithm: Compute $L(n\Theta)$ for the Jacobian of the genus 2 hyperelliptic curve $y^2 = f(x)$

Data: n, a nonnegative integer; a weight function w
Result: A basis for $L(n\Theta)$
$m \coloneqq 0$
Initialise empty list b
while `len`$(b) < n^2$ **do**
    Compute $V(w, 2m + n)$
    Let V be the subspace of reduced polynomials
    if *m odd* **then**
        Let $U \coloneqq V^-$
    else
        Let $U \coloneqq V^+$
    end
    Compute a basis b for $U(-m\Delta)$
    $m \coloneqq m + 1$
end

Algorithm 2: Computing $L(n\Theta)$

4.3.5 The Kummer embedding

Algorithm 2 in the case $n = 2$ gives a basis for $L(\Theta^+ + \Theta^-)$, which we give as $\xi_0, \xi_1, \xi_2, \xi_3$ in Proposition 4.3.7 and refer to as the Kummer coordinates. The proposition also computes the relations between the Kummer coordinates; the coordinates and the single quartic equation they satisfy agree with Flynn's original computation in [Fly90b].

Proposition 4.3.7. *Let $\mathcal{C}\colon y^2 = f(x)$ be a genus 2 curve and let $\mathcal{K}$ be the Kummer surface of $\mathcal{C}$. The following is a basis for $L(\Theta^+ + \Theta^-)$:*

$$\xi_0 = 1 \tag{4.31}$$

$$\xi_1 = x_1 + x_2 \tag{4.32}$$

$$\xi_2 = x_1 x_2 \tag{4.33}$$

$$\xi_3 = (F_0(x_1, x_2) - 2y_1 y_2)/(x_1 - x_2)^2, \tag{4.34}$$

where

$$\begin{aligned} F_0(x_1, x_2) = 2f_0 + f_1(x_1 + x_2) + 2f_2 x_1 x_2 + f_3(x_1 + x_2)(x_1 x_2) \\ + 2f_4(x_1 x_2)^2 + f_5(x_1 + x_2)(x_1 x_2)^2 + 2f_6(x_1 x_2)^3. \end{aligned} \tag{4.35}$$

The coordinates $\xi_0, \xi_1, \xi_2, \xi_3$ satisfy the quartic equation $Q(\xi_0, \xi_1, \xi_2, \xi_3) = 0$, where

$$Q(z_0, z_1, z_2, z_3) = z_3^2(z_1^2 - 4z_0 z_2) + z_3\Phi(z_0, z_1, z_2) + \Psi(z_0, z_1, z_2) = 0, \tag{4.36}$$

where

$$\begin{aligned}\Phi(z_0,z_1,z_2) &= -4f_0z_0^3 - 2f_1z_0^2z_1 - 4f_2z_0^2z_2 - 2f_3z_0z_1z_2 \\ &\quad - 4f_4z_0z_2^2 - 2f_5z_1z_2^2 - 4f_6z_2^3,\end{aligned} \tag{4.37}$$

$$\begin{aligned}\Psi(z_0,z_1,z_2) &= -4f_0f_2z_0^4 + f_1^2z_0^4 - 4f_0f_3z_0^3z_1 - 2f_1f_3z_0^3z_2 - 4f_0f_4z_0^2z_1^2 \\ &\quad + 4f_0f_5z_0^2z_1z_2 - 4f_1f_4z_0^2z_1z_2 - 4f_0f_6z_0^2z_2^2 + 2f_1f_5z_0^2z_2^2 \\ &\quad - 4f_2f_4z_0^2z_2^2 + f_3^2z_0^2z_2^2 - 4f_0f_5z_0z_1^3 + 8f_0f_6z_0z_1^2z_2 \\ &\quad - 4f_1f_5z_0z_1^2z_2 + 4f_1f_6z_0z_1z_2^2 - 4f_2f_5z_0z_1z_2^2 \\ &\quad - 2f_3f_5z_0z_2^3 - 4f_0f_6z_1^4 - 4f_1f_6z_1^3z_2 - 4f_2f_6z_1^2z_2^2 \\ &\quad - 4f_3f_6z_1z_2^3 - 4f_4f_6z_2^4 + f_5^2z_2^4.\end{aligned} \tag{4.38}$$

Proof. As discussed in Section 4.2, functions in $L(2(\Theta^+ + \Theta^-))$ satisfy quadratics. Since quadratic combinations of the Kummer coordinates are elements of $L(2(\Theta^+ + \Theta^-))$, they themselves satisfy quadratics, which give quartics in the original functions. See [Mül14, Proposition 3.1] for more details.

We compute all quartic combinations of the basis elements and find the relations between them using the algorithms in Section 4.3.3. □

Remark 4.3.8. *In higher genus it is infeasible to find all quartic combinations of the basis elements since the functions are larger and there are more of them.*

4.3.6 The Jacobian embedding

Algorithm 2 also computes a basis for $L(2(\Theta^+ + \Theta^-))$. In order to compare with Flynn's original embedding in [Fly90b], it is helpful to follow him and introduce the weights w_x, w_y, defined on x, y and the coefficients f_i in Table 4.1; the equation of the curve is homogeneous with respect to w_x and w_y.

	w_x	w_y
x_i	1	0
y_i	0	1
f_i	$-i$	2

Table 4.1: Weights for functions on $\mathrm{Sym}^2\,\mathcal{C}$.

This gives the functions more structure. We write the basis that we find so that all elements lie in $\mathbb{Z}[f_0,\ldots,f_6][x_1,y_1,x_2,y_2]$, and are homogeneous with respect to both weights. We arrive at a slightly different basis to Flynn, but can find the space of

quadratics spanned by these using the relation finding method between polynomials as in Section 1. It is 72 dimensional, as originally computed by Flynn ([Fly90b]). See Appendix E for the Jacobian coordinates.

4.4 Superelliptic genus 3

4.4.1 Superelliptic genus 3 curves

Let K be a field of characteristic $p \notin \{2, 3\}$. Let $\mathcal{C}$ be a genus 3 curve over K. Then $\mathcal{C}$ is either hyperelliptic or is isomorphic over K to a smooth plane quartic. As discussed in Section 4.3, over a field of characteristic not equal to 2, hyperelliptic curves of genus g can be written in the form $y^2 = f(x)$, for $\deg f \in \{2g+1, 2g+2\}$. For genus 3, this means $y^2 = f(x)$ with $\deg f \in \{7, 8\}$.

On the other hand, a smooth plane quartic is defined by an irreducible homogeneous quartic $F(x, y, z) = 0$ as a subset of $\mathbb{P}^3$ (see [Vak17, Section 19.7]). The canonical divisor κ_C is degree 4, and has $g = 3$ sections. Also, κ_C is base-point-free, so gives a map to $\mathbb{P}^2$. If this is an embedding, then the map embeds $\mathcal{C}$ as a degree 4 curve in $\mathbb{P}^2$ (since $\deg \kappa_C = 4$). If it isn't an embedding then the curve is hyperelliptic.

The superelliptic curves are a subset of the smooth plane quartics. These have a model of the form: $y^3 = f(x)$, where $\deg f = 4$. A nice feature of these curves is that the homogenisation of the equation is smooth in $\mathbb{P}^3$; that is, $y^3 z = F(x, z)$, where $F(x, z)$ is homogeneous of degree 4 with $F(x, 1) = f(x)$. Moreover, they have a rational point at infinity, given by $\infty = (0\colon 1\colon 0)$. Let $I\colon \operatorname{Sym}^3 \mathcal{C} \to \mathcal{J}(\mathcal{C})$ denote the surjection from Section 4.2 with base point ∞.

In this section, $\mathcal{C}$ denotes the projective curve $y^3 z = F(x, z)$ in $\mathbb{P}^3$ and $\mathcal{C}_0$ denotes the affine curve $y^3 = f(x)$, where $f(x) = F(x, 1)$.

As in the previous section, we will consider functions on the symmetric product and then relate them to functions on the Jacobian. We first need to know how divisors on $\mathcal{J}(\mathcal{C})$ relate to divisors on $\operatorname{Sym}^3 \mathcal{C}$.

Fix a primitive cube root of unity ω. Then $\mathcal{C}$ admits the automorphism $(x, y) \mapsto (x, \omega y)$, which we also denote by ω.

Lemma 4.4.1. *The inverse images of Θ and $\mathcal{O}$ under $I\colon \operatorname{Sym}^3 \mathcal{C} \to \mathcal{J}(\mathcal{C})$ are*

$$I^{-1}(\Theta) = \Theta' \coloneqq \Delta_\infty \cup \Delta_{\text{aff}} \subset \operatorname{Sym}^3 \mathcal{C} \tag{4.39}$$

$$I^{-1}(\mathcal{O}) = \mathcal{O}' \coloneqq \{P + \omega(P) + \omega^2(P)\colon P \in \mathcal{C}\} \subset \operatorname{Sym}^3 \mathcal{C}, \tag{4.40}$$

respectively, where

$$\Delta_\infty = \{P_1 + P_2 + \infty \colon P_1, P_2 \in \mathcal{C}\} \tag{4.41}$$

$$\Delta_{\text{aff}} = \{P_1 + P_2 + P_3 \colon P_1, P_2, P_3 \in \mathcal{C} \setminus \{\infty\},\ \ell(5\infty - P_1 - P_2 - P_3) > 0\}. \tag{4.42}$$

Proof. We first consider $I^{-1}(\Theta)$. The point $P_1 + P_2 + P_3 - 3\infty \in \mathcal{J}(\mathcal{C})$ lies in Θ if and only if $P_1 + P_2 + P_3 - 3\infty \sim Q_1 + Q_2 - 2\infty$ for some $Q_1, Q_2 \in \mathcal{C}$. This happens if and only if there is h such that $P_1 + P_2 + P_3 - 3\infty + \operatorname{div} h = Q_1 + Q_2 - 2\infty$. Equivalently, $P_1 + P_2 + P_3 - \infty + \operatorname{div} h = Q_1 + Q_2 \geq 0$; that is, if and only if $\ell(P_1 + P_2 + P_3 - \infty) > 0$. Riemann-Roch with the canonical divisor $\kappa = 4\infty$ gives $\ell(4\infty - P_1 - P_2 - P_3 + \infty) - \ell(P_1 + P_2 + P_3 - \infty) = 2 + 1 - g = 0$. Thus $\ell(P_1 + P_2 + P_3 - \infty) > 0$ if and only if $\ell(5\infty - P_1 - P_2 - P_3) > 0$. Since $\mathscr{L}_C(5\infty)$ has basis $\{1, x, y\}$, such functions are lines $a + bx + cy = 0$ that pass through the points P_1, P_2, P_3 with the correct multiplicity. Thus $P_1 + P_2 + P_3 \in \operatorname{Sym}^3 \mathcal{C}$ maps into Θ if and only if P_1, P_2, P_3 are the intersection of $\mathcal{C}$ with a line with the correct multiplicities.

There are two cases: $P_1, P_2, P_3 \in \mathcal{C} \setminus \{\infty\}$, and $P_i = \infty$ for some i. These correspond to $P_1 + P_2 + P_3 \in \Delta_{\text{aff}}$ and $P_1 + P_2 + P_3 \in \Delta_\infty$, respectively.

Now suppose that $P_1 + P_2 + P_3 \in I^{-1}(\mathcal{O})$. Then $P_1 + P_2 + P_3 - 3\infty = \operatorname{div} g$. It follows that $g \in \mathscr{L}_C(3\infty)$, which is generated by $1, x$. Either $g = 1$ or $g = x - a$ for some $a \in K$. The first case implies $P_1 = P_2 = P_3 = \infty$. In the second case, the resultant of $y^3 - f(x)$ and $x - a$ is $y^3 - f(a)$, which implies that each P_i satisfies $x(P_i) = a, y(P_i)^3 = f(a)$. Thus the points must be $(x_0, y_0), (x_0, \omega y_0), (x_0, \omega^2 y_0)$ in some order, where $y_0^3 = f(a)$. Both cases give $P_1 + P_2 + P_3 \in \mathcal{O}'$. □

Lemma 4.4.2. *If $g \in K(\mathcal{J}(\mathcal{C}))$, then we can ignore poles along Δ_{aff} and $\mathcal{O}'$ of $I^* g \in K(\operatorname{Sym}^3 \mathcal{C})$.*

Proof. First we show that Δ_{aff} is codimension one inside $\operatorname{Sym}^3 \mathcal{C}$, and thus is a divisor. Associate the point $(a \colon b \colon c) \in \mathbb{P}^2$ with the line $\ell = ax + by + cz = 0$. This line intersects $\mathcal{C}$ at the divisor $P_1 + P_2 + P_3 + P_4$, and any choice of three P_i gives $P_1 + P_2 + P_3 \in \Delta_{\text{aff}}$. Also, $P_1 + P_2 + P_3 - 3\infty \sim \omega(P_4) + \omega^2(P_4) - 2\infty$, by using $\operatorname{div}(x - x(P_4)) = P_4 + \omega(P_4) + \omega^2(P_4) - 3\infty$. Hence $I(\Delta_{\text{aff}})$ lies inside $\{P + \omega(P) - 2\infty \colon P \in \mathcal{C}\} \subset \mathcal{J}(\mathcal{C})$, which is dimension 1. Since $I(\Delta_{\text{aff}})$ has codimension 2 inside $\mathcal{J}(\mathcal{C})$, it does not correspond to a divisor. Also, $\mathcal{O}'$ maps down to the point $\mathcal{O} \in \mathcal{J}(\mathcal{C})$, which is not a divisor. □

However, Δ_∞ is a divisor on $\operatorname{Sym}^3 \mathcal{C}$ that maps to the divisor Θ on $\mathcal{J}(\mathcal{C})$.

4.4.2 The space $L(n\Theta)$

As in Section 4.2, the space $L_J(n\Theta)$ is in bijection with functions on $\mathrm{Sym}^3 \mathcal{C}$ that have poles of order at most n along Δ_∞ and a pole of any order along $\mathcal{O}'$ or Δ_{aff}. This subspace is $I^*L(n\Theta)$. We work with the space $I^*L(n\Theta)$, since it is easier to write down functions on $\mathrm{Sym}^3 \mathcal{C}$ than on $\mathcal{J}(\mathcal{C})$.

Since $\mathrm{ord}_\infty(x) = 3$ and $\mathrm{ord}_\infty(y) = 4$, we see from the previous section that $I^*L(n\Theta)$ consists of functions on $\mathrm{Sym}^3 \mathcal{C}$ that are regular away from $\Delta_\infty, \Delta_{\mathrm{aff}}, \mathcal{O}'$, and which have weight at most n according to the weight $w(x_1) = 3, w(y_1) = 4$, extended as in Lemma 4.2.12.

4.4.3 Kummer coordinates

We now find a basis for $L(2\Theta)$ by generalising Algorithm 2. The minimum weight of any nonconstant function in $K[x_1, y_1, x_2, y_2, x_3, y_3]^{S_3}$ is 3, since $w(x) = 3$ and $w(y) = 4$. Thus, to find functions of weight at most 2, we must use a nontrivial denominator. Since the only pole we are allowed apart from Θ is along $\mathcal{O}'$ or Δ_{aff}, we focus on functions whose divisor intersects $\mathcal{O}'$ or Δ_{aff}.

Since $P_1 + P_2 + P_3 \in \Delta_{\mathrm{aff}}$ if and only if P_i are affine and lie on the intersection of a line with $\mathcal{C}$, we consider the condition that three points lie on a line.

Lemma 4.4.3. *Let $P_i = (x_i, y_i) \in \mathbb{A}^2$ for $i = 1, 2, 3$. Then P_3 lies on the line spanned by P_1 and P_2 if and only if*

$$d \coloneqq x_1(y_2 - y_3) + x_2(y_3 - y_1) + x_3(y_1 - y_2) \tag{4.43}$$

equals 0.

Proof. The line spanned by (x_1, y_1) and (x_2, y_2) has equation

$$\ell_{12}(x, y) = (y_2 - y_1)x + (x_1 - x_2)y + x_2y_1 - x_1y_2 = 0. \tag{4.44}$$

The condition that (x_3, y_3) lies on the line is simply $\ell_{12}(x_3, y_3) = 0$. Since $d = \ell_{12}(x_3, y_3)$, the result follows. □

But $d = 0$ also if two of the three points P_1, P_2, P_3 coincide. Let

$$\Delta = \{2P + Q \colon P, Q \in \mathcal{C}\} \tag{4.45}$$

be this divisor on $\mathrm{Sym}^3 \mathcal{C}$. Then $\operatorname{div} d^2 = 2\Delta + 2\Delta_{\mathrm{aff}} - 8\Theta$.

Remark 4.4.4. *Ideally we would like to say* $\operatorname{div} d = \Delta + \Delta_{\mathrm{aff}} - 4\Theta$*, but d is not defined on* $\mathrm{Sym}^2 \mathcal{C}$ *as it is antisymmetric.*

Functions we find easily The first few functions are easy to find:

$$\sigma_5 = 1 \tag{4.46}$$

$$\sigma_6 = (x_1^2y_2 - x_1^2y_3 - y_1x_2^2 + y_1x_3^2 + x_2^2y_3 - y_2x_3^2)/d \tag{4.47}$$

$$\sigma_7 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)/d \tag{4.48}$$

$$\sigma_8 = (x_1^2x_2y_3 + x_1^2y_2x_3 + x_1x_2^2y_3 + x_1y_2x_3^2 + y_1x_2^2x_3 + y_1x_2x_3^2)/d. \tag{4.49}$$

These are the only possibilities for functions of the form g/d. Indeed, the maximum weight of a monomial in g when $m = 1$ is $2 + w(d) = 6$.

Generalising the algorithm As in Algorithm 2, we look for functions g/d^m where $g \in K[x_1, y_1, x_2, y_2, x_3, y_3]$ and $m \geq 0$, such that g has a zero of order at least m along Δ. To ensure g/d^m is symmetric, we look for g symmetric, if m is even, and g antisymmetric, if m is odd. To impose the zero along Δ, we approximate g near Δ using Taylor series: write $x_2 = x_1 + \varepsilon$ and $y_2 = f(x_1 + \varepsilon)^{1/3}$, and ensure that ε^m divides $g(x_1, y_1, x_2 + \varepsilon, y_2(\varepsilon), x_3, y_3)$. This ensures that $g/d^m \in L_{\mathcal{J}}(2\Theta)$ as a function on $\mathcal{J}$.

We fix $m \geq 0$, and search for functions g vanishing to order at least m on Δ such that g/d^m is symmetric and $w(g) \leq mw(d) + n$. If the subspace has too small a dimension, then we increase m and repeat, knowing when to stop, since $\dim L(n\Theta) = n^3$.

Running the algorithm up to $m = 2$ finds eight linearly independent functions on the Kummer variety, $\eta_1, \ldots, \eta_8$, which therefore form the Kummer coordinates. We then change basis so that the leading terms according to the lexicographical order with $x_1 > y_1 > x_2 > y_2 > x_3 > y_3$ are

$$\begin{aligned}
&2f_4^2x_1^3x_2^3x_3^2,\\
&2f_4x_1^3x_2^3,\\
&2f_4x_1^3x_2^3y_3,\\
&2f_4x_1^3x_2^3x_3,\\
&x_1^2y_2^2,\\
&x_1^3y_2^2,\\
&x_1^3x_2y_2,\\
&x_1^3x_2y_2y_3,
\end{aligned} \tag{4.50}$$

respectively.

Explicitly, we change basis to

$$\begin{aligned}
\sigma_1 &= \frac{1}{f_3}(f_1f_4 + f_2f_3)\eta_3 - \frac{1}{f_3}\eta_4,\\
\sigma_2 &= -\eta_3,\\
\sigma_3 &= -\eta_6,\\
\sigma_4 &= \frac{1}{f_3}\eta_2 + \frac{f_2}{f_3}\eta_3,\\
\sigma_5 &= \eta_7,\\
\sigma_6 &= -\eta_8,\\
\sigma_7 &= \eta_1,\\
\sigma_8 &= \eta_5,
\end{aligned} \tag{4.51}$$

where $\sigma_5, \sigma_6, \sigma_7, \sigma_8$ are as in (4.46)-(4.49).

We first introduce some notation to make the exposition more manageable. Let

$$\langle g(x_1, x_2, x_3, y_1, y_2, y_3)\rangle_{S_3} = \sum_{\sigma\in S_3} g(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}, y_{\sigma 1}, y_{\sigma 2}, y_{\sigma 3}) \tag{4.52}$$

$$\langle g(x_1, x_2, x_3, y_1, y_2, y_3)\rangle^-_{S_3} = \sum_{\sigma\in S_3} \mathrm{sign}(\sigma) g(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}, y_{\sigma 1}, y_{\sigma 2}, y_{\sigma 3}). \tag{4.53}$$

In this notation, $d = \langle x_1y_2\rangle^-_{S_3}$, and the functions we already found are

$$\begin{array}{cc}
\sigma_5 = 1 & d\sigma_6 = \langle x_1^2y_2\rangle^-_{S_3}\\
d\sigma_7 = \langle x_1^2x_2\rangle^-_{S_3} & d\sigma_8 = \langle x_1^2x_2y_3\rangle^-_{S_3}
\end{array} \tag{4.54}$$

We can now express $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ as follows:

$$\begin{aligned}
d^2\sigma_1 = {} & f_4^2\langle x_1^3x_2^3x_3^2\rangle_{S_3} - f_2f_4\langle x_1^3x_2^3\rangle_{S_3} + 2f_3f_4\langle x_1^3x_2^2x_3^2\rangle_{S_3}\\
& + 4f_2f_4\langle x_1^3x_2^2x_3\rangle_{S_3} + (f_1f_4 - f_2f_3)\langle x_1^3x_2^2\rangle_{S_3} - 2f_4\langle x_1^3x_2y_2y_3^2\rangle_{S_3}\\
& + (f_1f_4 + f_2f_3)\langle x_1^3x_2x_3\rangle_{S_3} + 2f_0f_4\langle x_1^3x_2\rangle_{S_3} - f_4\langle x_1^2y_1x_2^2y_3^2\rangle_{S_3}\\
& + f_4\langle x_1^2y_1x_2y_2x_3y_3\rangle_{S_3} + f_2\langle x_1^2y_1y_2^2\rangle_{S_3} - f_2\langle x_1^2y_1y_2y_3\rangle_{S_3}\\
& + (-f_2f_4 + f_3^2)\langle x_1^2x_2^2x_3^2\rangle_{S_3} + 2f_2f_3\langle x_1^2x_2^2x_3\rangle_{S_3}\\
& + (f_0f_4 + f_1f_3 - f_2^2)\langle x_1^2x_2^2\rangle_{S_3} - 3f_3\langle x_1^2x_2y_2y_3^2\rangle_{S_3}\\
& + (-f_0f_4 + f_1f_3 + 2f_2^2)\langle x_1^2x_2x_3\rangle_{S_3} + 3f_0f_3\langle x_1^2x_2\rangle_{S_3}\\
& + f_3\langle x_1y_1x_2y_2x_3y_3\rangle_{S_3} + 2f_2\langle x_1y_1x_2y_2y_3\rangle_{S_3} - 4f_2\langle x_1y_1x_2y_3^2\rangle_{S_3}\\
& - f_1\langle x_1y_1y_2^2\rangle_{S_3} + f_1\langle x_1y_1y_2y_3\rangle_{S_3} + (-f_0f_3 + 2f_1f_2)\langle x_1x_2x_3\rangle_{S_3}\\
& + (2f_0f_2 + f_1^2)\langle x_1x_2\rangle_{S_3} - 2f_1\langle x_1y_2^2y_3\rangle_{S_3} + 2f_0f_1\langle x_1\rangle_{S_3}\\
& + \langle y_1^2y_2^2y_3^2\rangle_{S_3} - 3f_0\langle y_1^2y_2\rangle_{S_3} + f_0\langle y_1y_2y_3\rangle_{S_3} + f_0^2\langle 1\rangle_{S_3}
\end{aligned} \tag{4.55}$$

$$
\begin{aligned}
d^2\sigma_2 = {} & f_4\langle x_1^3x_2^3\rangle_{S_3} - 2f_4\langle x_1^3x_2^2x_3\rangle_{S_3} + f_3\langle x_1^3x_2^2\rangle_{S_3} - f_3\langle x_1^3x_2x_3\rangle_{S_3} - \langle x_1^2y_1y_2^2\rangle_{S_3} \\
& + \langle x_1^2y_1y_2y_3\rangle_{S_3} + f_4\langle x_1^2x_2^2x_3^2\rangle_{S_3} + f_2\langle x_1^2x_2^2\rangle_{S_3} - f_2\langle x_1^2x_2x_3\rangle_{S_3} \\
& + f_1\langle x_1^2x_2\rangle_{S_3} - \langle x_1^2y_2^2y_3\rangle_{S_3} + f_0\langle x_1^2\rangle_{S_3} - \langle x_1y_1x_2y_2y_3\rangle_{S_3} \\
& + 2\langle x_1y_1x_2y_3^2\rangle_{S_3} - f_1\langle x_1x_2x_3\rangle_{S_3} - f_0\langle x_1x_2\rangle_{S_3} \\
d^2\sigma_3 = {} & f_4\langle x_1^3x_2^3y_3\rangle_{S_3} - 2f_4\langle x_1^3x_2^2x_3y_3\rangle_{S_3} + f_3\langle x_1^3x_2^2y_3\rangle_{S_3} \\
& - f_3\langle x_1^3x_2y_2x_3\rangle_{S_3} + f_4\langle x_1^2y_1x_2^2x_3^2\rangle_{S_3} + f_3\langle x_1^2y_1x_2^2x_3\rangle_{S_3} + f_2\langle x_1^2y_1x_2x_3\rangle_{S_3} \\
& + f_1\langle x_1^2y_1x_2\rangle_{S_3} - \langle x_1^2y_1y_2^2y_3\rangle_{S_3} + f_0\langle x_1^2y_1\rangle_{S_3} - f_3\langle x_1^2x_2^2x_3y_3\rangle_{S_3} \\
& + f_2\langle x_1^2x_2^2y_3\rangle_{S_3} - 2f_2\langle x_1^2x_2y_2x_3\rangle_{S_3} - f_1\langle x_1^2x_2y_2\rangle_{S_3} + f_1\langle x_1^2x_2y_3\rangle_{S_3} \\
& + \langle x_1y_1x_2y_2y_3^2\rangle_{S_3} - f_1\langle x_1y_1x_2x_3\rangle_{S_3} - 2f_0\langle x_1y_1x_2\rangle_{S_3} + f_0\langle x_1x_2y_3\rangle_{S_3} \\
d^2\sigma_4 = {} & f_4\langle x_1^3x_2^3x_3\rangle_{S_3} - f_4\langle x_1^3x_2^2x_3^2\rangle_{S_3} + f_3\langle x_1^3x_2^2x_3\rangle_{S_3} + f_2\langle x_1^3x_2x_3\rangle_{S_3} \\
& + f_1\langle x_1^3x_2\rangle_{S_3} - \langle x_1^3y_2^2y_3\rangle_{S_3} + f_0\langle x_1^3\rangle_{S_3} + \langle x_1^2y_1x_2y_2y_3\rangle_{S_3} \\
& - \langle x_1^2y_1x_2y_3^2\rangle_{S_3} - f_3\langle x_1^2x_2^2x_3^2\rangle_{S_3} - f_2\langle x_1^2x_2^2x_3\rangle_{S_3} - f_1\langle x_1^2x_2^2\rangle_{S_3} \\
& + 2\langle x_1^2x_2y_2y_3^2\rangle_{S_3} - 2f_0\langle x_1^2x_2\rangle_{S_3} - \langle x_1y_1x_2y_2x_3y_3\rangle_{S_3} + f_0\langle x_1x_2x_3\rangle_{S_3}
\end{aligned}
\tag{4.56}
$$

$$
\tag{4.57}
$$

$$
\tag{4.58}
$$

The MAGMA file `kummer_coordinates/find_kummer_coordinates.m` in [Nic18] gives the code to compute these, and contains the full expressions.

4.4.4 Finding relations

The eight coordinates $\sigma_1, \ldots, \sigma_8$ define a map $\mathcal{K}(\mathcal{C}) \to \mathbb{P}^7$, and we now describe the image of this map.

As discussed in Section 4.3, the Kummer coordinates satisfy quartic equations. However, since each σ_i is already complicated, we first look for lower degree relations. One can explicitly check there are no quadratic relations between the σ_i. But there are eight linearly independent cubic relations. Scaling each cubic relation by $\sigma_1, \ldots, \sigma_8$, we find 64 linearly independent quartic relations.

To get an upper bound on the dimension of the space of relations, note that if we specialise the coefficients $f_0, \ldots, f_4$ to constants in the ground field, then any relation that holds over $K(f_0, \ldots, f_4)$ still holds for the specialised σ_i. The curve $y^3 = x^4 + 1$ gives 70 linearly independent quartic relations among $\sigma_1, \ldots, \sigma_8$; thus we are missing at most 6 quartics.

Searching for these naively proved infeasible. Instead, we introduce weights on the functions σ_i and coefficients f_j, analogously to [Fly90b]. We define the weights w_x, w_y on $L(2\Theta)$ in Table 4.2. The coordinates σ_i are homogeneous with respect to both

	w_x	w_y
x_i	1	0
y_i	0	1
f_i	$-i$	3

Table 4.2: Weights for functions on $\mathrm{Sym}^3 \mathcal{C}$.

	w_x	w_y
σ_1	0	6
σ_2	2	3
σ_3	2	4
σ_4	3	3
σ_5	2	2
σ_6	3	2
σ_7	4	1
σ_8	4	2

Table 4.3: The weights of the functions σ_i.

weights, as shown in Table 4.3. We can write any homogeneous degree n polynomial relation between the σ_i as a $\mathbb{Z}[f_0, \ldots, f_4]$-linear combination of monomials of degree n in the σ_i. Moreover, using the weights w_x, w_y, any such relation decomposes into its homogeneous parts with respect to each weight. We thus reduce to searching for relations that are homogeneous in both w_x and w_y.

Example 4.4.5. *For example* $w_x(x_1x_2y_1f_3) = 1 + 1 + 0 - 3 = -1$.

Define $V_{a,b}$ as the vector space generated by the monomials $m = \prod_i f_i^{e_i} \prod_j \sigma_j^{n_j}$ such that $w_x(m) = a$ and $w_y(m) = b$. Since each relation is homogeneous with respect to w_x and w_y, we can search for relations just within $V_{a,b}$.

Note that the coefficients f_i can have nonzero weight. For example, the only quadratic monomials in σ_i of weight 3 under w_x are $\sigma_1\sigma_4, \sigma_1\sigma_6$. However, $f_1\sigma_2\sigma_3$ is also weight 3 under w_x. In practice, we restrict to monomials with bounded degree of the f_i. Let $w_f(\prod_i f_i^{e_i} \prod_j \sigma_j^{n_j}) = \sum_i e_i$ be the f-degree of the monomial. Let $V_{a,b,c}$ be the space generated by the monomials $m \in V_{a,b}$ such that $w_f(m) \leq c$; this is now finite-dimensional.

We fix a, b, c and then look for relations in $V_{a,b,c}$ using the algorithms in Section 4.3.3. Looping over many combinations of a, b, c, each time we find a relation, we check if it is linearly independent with the currently known relations. This method suffices to compute the six remaining quartic relations. Finally we apply the `LLL` algorithm ([Len82]) in MAGMA to try to express the relations more simply. The MAGMA file `kummer_coordinates/kummer_relations.m` in [Nic18] gives the 70 quartic relations.

Remark 4.4.6. *Before applying* LLL*, it turned out that over some specialisations, for example if $f_2 = 0$, the rank of the relations was 69. After applying* LLL *the rank appears to be 70 for more specialisations.*

4.4.5 Jacobian coordinates

The same approach as in Section 4.4.3 can compute a basis for $L(3\Theta)$, which thus gives the Jacobian coordinates for superelliptic genus 3 curves. For this, we use d^2 as the denominator and find functions g of weight at most $2w(d) + 3 = 11$ that vanish to order 2 along Δ. We find $3^3 = 27$ linearly independent coordinates. We can even find all quadratic combinations of these, but it proved too computationally intensive to find relations between these.

We can also compute $L(4\Theta)$, to get $4^3 = 64$ coordinates. Again, computing the quadratic relations naively is infeasible.

Remark 4.4.7. *The same method should apply to the hyperelliptic genus 3 case.*

4.4.6 Evaluating the Kummer coordinates on points

Recall that a multisymmetric function is an element of $K(x_1, \ldots, x_g, y_1, \ldots, y_g)$ that is invariant under the action of the symmetric group S_g via

$$^{\sigma}p(x_1, \ldots, x_g, y_1, \ldots, y_g) = p(x_{\sigma(1)}, \ldots, x_{\sigma(g)}, y_{\sigma(1)}, \ldots, y_{\sigma(g)}), \tag{4.59}$$

as in Remark 4.2.8.

Let $\mathcal{C}$ be the superelliptic curve $y^3 = f(x)$, where $\deg f = 4$. The Kummer coordinates of $\mathcal{C}$ are multisymmetric functions $\varphi \in K(x_1, y_1, x_2, y_2, x_3, y_3)^{S_3}$. We now discuss how to evaluate a multisymmetric function at an element of $\mathrm{Sym}^3 \mathcal{C}$. Let $P_1 + P_2 + P_3$ be an element of $\mathrm{Sym}^3 \mathcal{C}$. If we are willing to move to the field over which each P_i is defined individually, then we can compute each point $P_i = (x_i, y_i)$ in the sum $P_1 + P_2 + P_3$ and then easily compute the multisymmetric function. But we want to work over the ground field. Similarly to Mumford representation of divisors, we can represent $P_1 + P_2 + P_3$ as a pair $\langle a(x), b(x) \rangle$, where $a(x)$ is monic of degree at most 3, whose roots are the x-coordinates of P_1, P_2, P_3, and $b(x)$ is a polynomial of degree at most 2 such that $b(x(P_i)) = y(P_i)$ for each $i = 1, 2, 3$.

Remark 4.4.8. *In the case that one or more of the P_i is the point ∞, we let $a(x) = \prod_{P_i \neq \infty}(x - x(P_i))$, and let $b(x)$ be the corresponding polynomial, ignoring points at infinity.*

It is a nontrivial problem to express multisymmetric functions in $x_1, x_2, x_3, y_1, y_2, y_3$ in terms of a point on $\mathrm{Sym}^3 \mathcal{C}$ (Vaccarino studies the generators of the multisymmetric functions in [Vac05]). We solve this problem by representing the general point on $\mathrm{Sym}^3 \mathcal{C}$ by the pair $\langle a(x), b(x) \rangle$ where $a(x) = (x - x_1)(x - x_2)(x - x_3)$ and $b(x) = b_2 x^2 + b_1 x + b_0$, with x_1, x_2, x_3 and b_0, b_1, b_2 considered as indeterminates. We then replace each y_i by $b(x_i)$ in the multisymmetric function φ. The function $\varphi(x_1, x_2, x_3, b(x_1), b(x_2), b(x_3))$ is then a symmetric function in x_1, x_2, x_3 over $K(b_0, b_1, b_2)$. We can now evaluate φ in terms of the elementary symmetric polynomials $s_1 = x_1 + x_2 + x_3$, $s_3 = x_1x_2 + x_2x_3 + x_3x_1$ and $s_3 = x_1x_2x_3$. We have $s_1 = -a_2$, $s_2 = a_1$ and $s_3 = -a_0$, which is defined over the same field as $a(x)$.

We can do this for all the Kummer coordinates, and thus are able to evaluate them on arbitrary divisors.

Example 4.4.9. *Recall, $d = (x_1 - x_2)y_3 + (x_2 - x_3)y_1 + (x_3 - x_1)y_2$. Since d isn't symmetric, it doesn't make sense to evaluate d on $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - 3\infty$. But d^2 is symmetric. Writing $\langle A(x), B(x) \rangle$ as above, we find*

$$d^2 = b_2^2 \operatorname{disc}(A). \tag{4.60}$$

4.4.7 Evaluating on inverses of divisors

In the hyperelliptic case, the negation of $(x_1, y_1) + (x_2, y_2) - \mathfrak{m}_\infty$ is the divisor $(x_1, -y_1) + (x_2, -y_2) - \mathfrak{m}_\infty$, so a function is invariant under negation if and only if it is invariant under the automorphism that the hyperelliptic involution $(x, y) \mapsto (x, -y)$ induces on the Jacobian. The Kummer coordinates constructed in Proposition 4.3.7 are thus clearly invariant under negation.

Let $\mathcal{C}$ be the superelliptic curve $y^3 = f(x)$, where $\deg f = 4$. In this case, the negation of a point on the Jacobian is more complicated. If $\langle a(x), b(x) \rangle$ represents an element of $\mathcal{J}(\mathcal{C})$ then we can write $b(x)^3 - f(x) = \lambda a(x)c(x)$ for some polynomial $c(x)$; generically, $a(x)$ and $c(x)$ are cubics. Then $\langle a(x), b(x) \rangle + \langle c(x), b(x) \rangle$ is linearly equivalent to 0, meaning that $\langle c(x), b(x) \rangle$ is the negation of $\langle a(x), b(x) \rangle$ in $\mathcal{J}$. The Kummer coordinates, being invariant under negation on $\mathcal{J}$, should be projectively invariant on replacing $\langle A, B \rangle$ by $\langle C, B \rangle$. Our construction of the Kummer coordinates does not make this obvious, and we are yet to find a proof that our Kummer coordinates are invariant under negation. We give the following example.

Example 4.4.10. *Consider the curve $y^3 = -4x^4 - 4x^3 - 9x^2 + 10x + 8$. This has the rational points $(1, 1), (-1/2, 1), (0, 2), (9, -31)$. Let's compute the Kummer coordinates*

for the point $(1,1)+(-1/2,1)+(0,2)-3\infty$*, as well as its inverse. The point is represented by* $\langle A,B\rangle = \langle x^3-1/2x^2-1/2x, -2x^2+x+2\rangle$*. The inverse is* $\langle C,B\rangle = \langle x^3-x^2-11/4x+1/2, -2x^2+x+2\rangle$*. Indeed, we can compute* $B(x)^3-f(x) = -8A(x)C(x)$*. The Kummer coordinates evaluated on* $\langle A,B\rangle$ *are*

$$(67\colon 3\colon -2\colon 0\colon 1\colon 1/2\colon 1/2\colon 1). \tag{4.61}$$

The Kummer coordinates on $\langle C,B\rangle$ *are the same.*

Chapter 5

Isogenies between Jacobians of genus 2 curves

In this chapter we study (n, n)-isogenies between Jacobians of genus 2 curves over a field K. These are isogenies $\varphi\colon \mathcal{J} \to \mathcal{J}'$ whose kernel is an (n, n)-subgroup: a subgroup $\Sigma \subset \mathcal{J}[n]$ such that $\Sigma \cong (\mathbb{Z}/n\mathbb{Z})^2$ over $\overline{K}$ and such that Σ is maximally isotropic with respect to the Weil pairing; that is, the n-Weil pairing restricts to the trivial pairing on $\Sigma \times \Sigma$.

In practice, we try to describe (n, n)-isogenies by starting with an (n, n)-subgroup $\Sigma \subset \mathcal{J}[n]$ and taking the quotient $\mathcal{J} \to \mathcal{J}/\Sigma$. We then hope to explicitly compute the isogeny, and describe the image. We are interested in the case where $\mathcal{J}/\Sigma$ is isomorphic to a Jacobian of a curve. Jacobians of genus 2 curves are dense in the space of principally polarised abelian surfaces (see Corollary 2.2.13); thus if $\mathcal{J}/\Sigma$ is principally polarised, we expect it to be the Jacobian $\mathcal{J}'$ of another genus 2 curve $\mathcal{C}'$.

Many researchers have studied (n, n)-isogenies for small n. The most studied case is the $(2, 2)$-isogeny, classically called the Richelot isogeny. This was originally discovered by Richelot ([Ric37]), and is subsequently well described in [BJF88] and [CF96]. Bruin et al. study $(3, 3)$-isogenies in [BFT14]. They determine the space of genus 2 curves whose Jacobians have a $(3, 3)$-subgroup with all elements defined over the ground field, and then compute the corresponding $(3, 3)$-isogeny explicitly. Smith studies $(4, 4)$-isogenies in [Smi05] for Jacobians of genus 2 curves, but focuses on the finite field case. He shows that a $(4, 4)$-isogeny can be written as a composition of two Richelot isogenies, and determines when a composition of two Richelot isogenies gives a $(4, 4)$-isogeny. Bruin and Doerksen study $(4, 4)$-isogenies when the image is a split Jacobian ([BD11]). Flynn studies $(5, 5)$-isogenies in [Fly15]. He finds a single geometric example of a genus 2 curve with a $(5, 5)$-isogeny and computes the isogeny explicitly on Kummer surfaces.

In this chapter, we consider (n, n)-isogenies for $n = 2, 4, 5$. We rederive the $(2, 2)$-isogeny using the method due to Bruin et al. ([BFT14]), computing the explicit projective map the Richelot isogeny induces on Kummer surfaces. We also give the method of computing the Richelot isogeny due to Flynn ([Fly90b]). We later use this to compute the full 4-torsion subgroup of a Jacobian over $\overline{K}$.

We characterise $(4, 4)$-isogenies for Jacobians of genus 2 curves, and find large families of curves where the $(4, 4)$-subgroup is defined completely over the ground field. We generalise Flynn's example of a $(5, 5)$-isogeny to infinitely many geometrically nonisomorphic genus 2 curves, and also compute the isogeny explicitly on Kummer surfaces, using a similar method to Flynn, with the general idea originating in [BFT14]. We also describe an algorithm to compute the full 4-torsion subgroup of the Jacobian of a genus 2 curve over $\overline{K}$, which we believe is original.

Throughout this chapter $\mathcal{J}$ denotes the Jacobian of a genus 2 curve $\mathcal{C}$ over a number field K, unless otherwise stated.

5.1 (n, n)-subgroups and the Weil pairing

We say a subgroup $\Sigma \subset \mathcal{J}[n]$ is an (n, n)-subgroup if $\Sigma \cong (\mathbb{Z}/n\mathbb{Z})^2$ over $\overline{K}$ and if Σ is isotropic with respect to the n-Weil pairing; that is, e_n restricts to the trivial pairing on Σ. Corollary 2.2.16 shows that $\mathcal{J}/\Sigma$ is principally polarised if and only if Σ is maximally isotropic under the n-Weil pairing.

5.2 The Weil pairing

We first collect a few results about Weil pairings. We say that a subgroup $\Sigma \subseteq \mathcal{J}[n](\overline{K})$ is *isotropic* under the Weil pairing if the pairing e_n restricts to the trivial pairing on Σ.

The following proposition appears to be well-known in the literature, but I couldn't find a reference for it.

Proposition 5.2.1. *Let $\mathcal{J}$ be the Jacobian of a genus g curve over a field K, and let $n \geq 2$. Let $\Sigma \subseteq \mathcal{J}[n]$ be isotropic with respect to the e_n-Weil pairing. Then Σ is maximally isotropic if and only if $\#\Sigma = n^g$.*

Proof. Let $\Sigma \subseteq \mathcal{J}[n]$ be isotropic with respect to the Weil pairing. We have the

following commutative diagram

$$\begin{array}{ccc} \Sigma & \xrightarrow{\alpha} & \mathrm{Hom}(\mathcal{J}[n]/\Sigma, \mu_n) \\ & \searrow^{\beta} & \downarrow q \\ & & \mathrm{Hom}(\mathcal{J}[n], \mu_n), \end{array} \tag{5.1}$$

where β is the map $\beta(P)(Q) = e_n(P, Q)$, and q is the natural map arising from the quotient $\mathcal{J}[n] \to \mathcal{J}[n]/\Sigma$. Since Σ is isotropic, we have $e_n(P, Q+R) = e_n(P, Q)$ for all $P, R \in \Sigma$ and $Q \in \mathcal{J}[n]$; thus β factors through α. The Weil pairing is nondegenerate, which means that if $P \in \mathcal{J}[n]$ satisfies $e_n(P, Q) = 1$ for all $Q \in \mathcal{J}[n]$, then $P = 0$. This implies that β is injective, which further implies that α is injective.

We now consider the sizes of the Hom groups. First note that $\mathcal{J}[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$ over $\overline{K}$. Suppose H is a subgroup of $\mathcal{J}[n]$; then we can write $H \cong \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$ for some positive integers d_i, such that each d_i divides n. We have

$$\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mu_n) \cong \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/\gcd(d, n)\mathbb{Z}. \tag{5.2}$$

Since $\gcd(d_i, n) = d_i$ for each i, we have $\#\mathrm{Hom}(H, \mu_n) = \#H$.

Since α is injective, we thus have $\#\Sigma \leq \#\mathcal{J}[n]/\#\Sigma$, and thus $\#\Sigma \leq n^g$. This shows that if Σ is isotropic and $\#\Sigma = n^g$, then Σ is maximally isotropic.

Conversely, suppose that Σ is maximally isotropic. Consider the composition

$$\mathcal{J}[n] \xrightarrow{\gamma} \mathrm{Hom}(\mathcal{J}[n], \mu_n) \xrightarrow{\delta} \mathrm{Hom}(\Sigma, \mu_n), \tag{5.3}$$

where δ is the map that restricts a homomorphism to Σ. The map γ is an isomorphism since e_n is a perfect pairing. We thus get an isomorphism

$$\mathcal{J}[n]/\ker \delta\gamma \xrightarrow{\delta\gamma} \mathrm{im}\, \delta, \tag{5.4}$$

which implies

$$\#\mathcal{J}[n] = \#\,\mathrm{im}\, \delta \cdot \#\ker \delta\gamma. \tag{5.5}$$

Suppose Σ is maximally isotropic. Then we claim $\Sigma = \ker \delta\gamma$. To see this, suppose $P \in \ker \delta\gamma$; then $e_n(P, Q) = 1$ for all $Q \in \Sigma$, so $\Sigma + \langle P \rangle$ is isotropic and contains Σ (since also $e_n(P, P) = 1$), which implies that $\ker \delta\gamma \subseteq \Sigma$. We already know that $\Sigma \subseteq \ker \delta\gamma$, as Σ is isotropic.

Consequently $\#\mathcal{J}[n] = \#\,\mathrm{im}\, \delta \cdot \#\ker \delta\gamma$, which implies $n^{2g} = \#\,\mathrm{im}\, \delta \cdot \#\Sigma \leq (\#\Sigma)^2$. Thus if Σ is maximally isotropic, then $\#\Sigma \geq n^g$. Since we know $\#\Sigma \leq n^g$ if Σ is isotropic, we deduce that $\#\Sigma = n^g$. □

Example 5.2.2. *A maximally isotropic subgroup of $\mathcal{J}[4]$ is isomorphic to one of $(\mathbb{Z}/4\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^4$. If $\Sigma \cong (\mathbb{Z}/2\mathbb{Z})^4$, then $\Sigma = \mathcal{J}[2]$. The corresponding isogeny is multiplication by 2 or -2 on $\mathcal{J}$.*

To see that $\mathcal{J}[2]$ is a maximal 4-Weil isotropic subgroup of $\mathcal{J}[4]$, note that if $D, E \in \mathcal{J}[2]$, then $e_4(D, E) = e_2(2D, E) = e_2(0, E) = 1$, using compatibility of the Weil pairing.

Corollary 5.2.3. *Let $\mathcal{J}$ be the Jacobian of a genus g curve over a field K, and let p be a prime. If $\Sigma \subseteq \mathcal{J}[p](\overline{K})$ is maximally isotropic with respect to the e_p-Weil pairing, then $\Sigma \cong (\mathbb{Z}/p\mathbb{Z})^g$ (over $\overline{K}$).*

The following proposition is from [Fly15] (originally communicated by Ed Schaefer).

Proposition 5.2.4 ([Fly15], Lemma 2)**.** *Let $m \geq 2$ be an integer. Let K be a field of characteristic 0, let $\mathcal{C}/K$ be a curve of genus at least 2 with $\mathcal{C}(K) \neq \emptyset$. Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$ and let $\alpha_1, \alpha_2 \in \mathcal{J}[m]$; let $K(\alpha_1, \alpha_2)$ denote the minimal field of definition of α_1, α_2. Then $e_m(\alpha_1, \alpha_2) \subseteq \mu_m(K(\alpha_1, \alpha_2))$. If $m = p$ is prime and the field of definition K of the elements of Σ does not contain a primitive pth root of unity, then e_p acts trivially on Σ.*

Proof. Since $\mathcal{C}(K) \neq \emptyset$, we can find degree 0 divisors D_1, D_2 with disjoint support such that $\alpha_i = [D_i]$. Their fields of definition are $K(\alpha_1), K(\alpha_2)$, respectively. Moreover, we can find functions h_1, h_2 such that $\operatorname{div} h_i = mD_i$. The Weil pairing is $e_m(\alpha_1, \alpha_2) = h_2(D_1)/h_1(D_2)$, which lies in the field $K(\alpha_1, \alpha_2)$. The Weil pairing also lies in $\mu_m(\overline{K})$, which proves the proposition. □

We can uniquely represent 2-torsion on the Jacobian of a genus 2 curve as the divisor classes of $w_i - w_j$ where $w_1, \ldots, w_6$ are the Weierstrass points. These are uniquely associated to pairs $\{\alpha, \beta\}$ of roots of $f(x)$, where we allow $\alpha = \infty$ if $\deg f = 5$. These in turn correspond to quadratics $(x - \alpha)(x - \beta)$ dividing $f(x)$, where we allow the quadratic to be linear if one of the roots is ∞.

The following proposition is also well-known, but we give the proof for completeness.

Proposition 5.2.5. *Let G_1, G_2 be factors of $f(x)$ representing distinct 2-torsion points T_1, T_2 on the Jacobian of $y^2 = f(x)$. Then*

$$e_2(T_1, T_2) = \begin{cases} 1, & \text{if } G_1, G_2 \text{ have distinct roots} \\ -1, & \text{if } G_1, G_2 \text{ have a common root,} \end{cases} \tag{5.6}$$

where we treat ∞ as a root of $G_i(x)$ if $G_i(x)$ has degree 1. If $T_1 = T_2$, then $e_2(T_1, T_2) = 1$.

Proof. Without loss of generality, we can assume $\deg f = 6$, as otherwise we can transform to move all Weierstrass points into the affine chart. Under such a transformation, the factors $G_i(x)$ are both taken to quadratics. If $G_i(x)$ was linear, then it now has two roots in the affine chart, with the extra root being the image of ∞. Thus we are reduced to showing that if G_1, G_2 are distinct quadratic factors of $f(x)$, then $e_2(T_1, T_2) = 1$ if and only if $G_1(x), G_2(x)$ are coprime (and otherwise $e_2(T_1, T_2) = -1$).

Let α_i, β_i be the two roots of G_i for $i = 1, 2$. Let $h_i(x, y) = (x - \alpha_i)/(x - \beta_i)$; then $\operatorname{div} h_i = 2(\alpha_i, 0) - 2(\beta_i, 0) = 2T_i$.

Suppose G_1, G_2 are coprime; this implies $\alpha_1, \beta_1, \alpha_2, \beta_2$ are pairwise distinct. We have

$$\begin{aligned} e_2(T_1, T_2) &= h_2((\alpha_1, 0) - (\beta_1, 0))/h_1((\alpha_2, 0) - (\beta_2, 0)) && (5.7)\\ &= h_2((\alpha_1, 0) - (\beta_1, 0)) \cdot h_1((\beta_2, 0) - (\alpha_2, 0)) && (5.8)\\ &= \frac{\alpha_1 - \alpha_2}{\alpha_1 - \beta_2}\frac{\beta_1 - \beta_2}{\beta_1 - \alpha_2} \cdot \frac{\beta_2 - \alpha_1}{\beta_2 - \beta_1}\frac{\alpha_2 - \beta_1}{\alpha_2 - \alpha_1} && (5.9)\\ &= 1. && (5.10) \end{aligned}$$

We now conclude by using the basic properties of the Weil pairing. Since the Weil pairing is alternating, we have $e_2(T_1, T_1) = 1$; we also have $e_2(T_1, 0) = 1$. Let $T_1 \in \mathcal{J}[2]$, and let q_1 be its quadratic polynomial. There are 6 nontrivial elements of $\mathcal{J}[2]$ whose quadratics are coprime to q_1, and there are 8 nontrivial elements of $\mathcal{J}[2]$ whose quadratics have precisely one root in common with q_1. So far, we have shown that for 8 of the points $T_2 \in \mathcal{J}[2]$, we have $e_2(T_1, T_2) = 1$. But e_2 is non-degenerate, so there exists $T_2 \in \mathcal{J}[2]$ such that $e_2(T_1, T_2) \neq 1$. Since e_2 takes values in $\{\pm 1\}$, we must have $e_2(T_1, T_2) = -1$ in this case. Moreover, e_2 is bilinear, so for any T satisfying $e_2(T_1, T) = 1$, we must have $e_2(T_1, T + T_2) = -1$. It follows that for the remaining 8 points in $\mathcal{J}[2]$ (the ones for which the quadratics have precisely one root in common with q_1), we have $e_2(T_1, T_2) = -1$. □

Remark 5.2.6. *It is easy to compute the Weil pairing modulo K^{*2}, by replacing the divisor T_2 by a linearly equivalent divisor if it overlaps T_1 (see Remark 2.2.9), but if -1 is a square in K, then this does not help us. The main issue is that to compute $h_2(T_1)/h_1(T_2)$, we would have to first replace T_2 by a linearly equivalent divisor T_2' that has disjoint support from T_1, and then further replace h_2 by a function h_2' such that $\operatorname{div} h_2' = 2T_2'$. In this case, we find it simpler to just use properties of the Weil pairing.*

5.3 The dual isogeny

Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be an isogeny of Jacobians of curves. Let $\varphi'\colon \mathcal{J}' \to \mathcal{J}$ be the dual isogeny from Section 2.2.1; recall it is defined as the composition

$$\mathcal{J}' \xrightarrow{\lambda'} \mathcal{J}'^{\vee} \xrightarrow{\varphi^{\vee}} \mathcal{J}^{\vee} \xrightarrow{\lambda^{-1}} \mathcal{J}, \tag{5.11}$$

where $\mathcal{J}^{\vee}$ and $\mathcal{J}'^{\vee}$ are the dual abelian varieties, and $\varphi^{\vee}$ is the dual isogeny. We often abuse notation and refer to φ' as the *dual isogeny*.

5.4 Useful structures on the Jacobian of a genus 2 curve

We now explain some useful results on the Jacobian and Kummer surface of a genus 2 curve. These are mostly derived by Flynn in [Fly90b].

5.4.1 The Kummer equation determines the curve up to twist

In this section we show that the Kummer equation of a genus 2 curve determines the curve up to twist. We use this several times later to find the Kummer equation of the Jacobian $\mathcal{J}/\Sigma$ for an (n,n)-subgroup Σ, and thus to determine the isogenous curve $\mathcal{C}'$ up to twist.

Proposition 5.4.1. *Let $\mathcal{C}\colon y^2 = f(x)$ be a hyperelliptic curve of genus 2 and let $\mathcal{K}$ be its Kummer surface. Let $d \neq 0$ and let $\mathcal{C}_d\colon y^2 = df(x)$ be a twist of $\mathcal{C}$, with Kummer surface $\mathcal{K}_d$. Let $\xi_0, \xi_1, \xi_2, \xi_3$ be the Kummer coordinates for $\mathcal{C}$. The quartic equation of $\mathcal{K}$ is $Q(\xi_0, \xi_1, \xi_2, \xi_3) = 0$, where*

$$Q(z_0, z_1, z_2, z_3) = z_3^2(z_1^2 - 4z_0z_2) + z_3\Phi(z_0, z_1, z_2) + \Psi(z_0, z_1, z_2), \tag{5.12}$$

where Φ and Ψ are homogeneous of degree 3 and 4, respectively. The corresponding polynomials for $\mathcal{K}_d$ are $\Phi_d(z_0, z_1, z_2) = d\Phi(z_0, z_1, z_2)$ and $\Psi_d(z_0, z_1, z_2) = d^2\Psi(z_0, z_1, z_2)$. The map $\mathcal{K} \to \mathcal{K}_d$ given by $(z_0, z_1, z_2, z_3) \mapsto (z_0, z_1, z_2, dz_3)$ is an isomorphism. The Kummer equation $Q(z_0, z_1, z_2, z_3)$ is unique up to scaling, and determines the curve $f(x)$ up to scalar multiple.

Proof. The first part of the statement is from Proposition 4.3.7. Recall that

$$\begin{aligned}\Phi(z_0,z_1,z_2) &= -4f_0z_0^3 - 2f_1z_0^2z_1 - 4f_2z_0^2z_2 - 2f_3z_0z_1z_2 \\ &\quad - 4f_4z_0z_2^2 - 2f_5z_1z_2^2 - 4f_6z_2^3,\end{aligned} \tag{5.13}$$

$$\begin{aligned}\Psi(z_0,z_1,z_2) &= -4f_0f_2z_0^4 + f_1^2z_0^4 - 4f_0f_3z_0^3z_1 - 2f_1f_3z_0^3z_2 - 4f_0f_4z_0^2z_1^2 \\ &\quad + 4f_0f_5z_0^2z_1z_2 - 4f_1f_4z_0^2z_1z_2 - 4f_0f_6z_0^2z_2^2 + 2f_1f_5z_0^2z_2^2 \\ &\quad - 4f_2f_4z_0^2z_2^2 + f_3^2z_0^2z_2^2 - 4f_0f_5z_0z_1^3 + 8f_0f_6z_0z_1^2z_2 \\ &\quad - 4f_1f_5z_0z_1^2z_2 + 4f_1f_6z_0z_1z_2^2 - 4f_2f_5z_0z_1z_2^2 \\ &\quad - 2f_3f_5z_0z_2^3 - 4f_0f_6z_1^4 - 4f_1f_6z_1^3z_2 - 4f_2f_6z_1^2z_2^2 \\ &\quad - 4f_3f_6z_1z_2^3 - 4f_4f_6z_2^4 + f_5^2z_2^4.\end{aligned} \tag{5.14}$$

Both Φ and Ψ are homogeneous in the coefficients f_i, of degree 1 and 2, respectively. Thus $\Phi_d = d\Phi$ and $\Psi_d = d^2\Psi$. Further,

$$d^2Q(z_0,z_1,z_2,z_3) = (dz_3)^2(z_1^2 - 4z_0z_2) + (dz_3)d\Phi(z_0,z_1,z_2) + d^2\Psi(z_0,z_1,z_2) \tag{5.15}$$

$$= Q_d(z_0,z_1,z_2,dz_3), \tag{5.16}$$

which shows that the map $\mathcal{K} \to \mathcal{K}_d$ given by $(z_0,z_1,z_2,z_3) \mapsto (z_0,z_1,z_2,dz_3)$ is well-defined.

The fact that the Kummer equation is unique up to scaling follows from considering the quartic relations satisfied by the Kummer coordinates, as in Section 4.3.5. There is a single relation up to scaling, given by $Q(z_0,z_1,z_2,z_3)$ as above. We can read off the coefficients f_i from Φ. □

5.4.2 Translating by 2-torsion on the Kummer surface

For this section let $\mathcal{J}$ be the Jacobian of the genus 2 curve $\mathcal{C}\colon y^2 = g(x)h(x)$, where $g(x) = g_2x^2 + g_1x + g_0$ is a quadratic and $h(x) = h_4x^4 + \cdots + h_0$ is a quartic. Let T be the 2-torsion point on $\mathcal{J}$ corresponding to $g(x)$.

Let $D \in \mathcal{J}$, and consider $\xi(D+T)$. Cassels and Flynn show we can compute $\xi(D+T)$ as a linear function of $\xi(D)$ and the coefficients g_i, h_j.

Proposition 5.4.2 ([CF96], Lemma 2.1)**.** *Let $\mathcal{C}\colon y^2 = g(x)h(x)$ as above. Let $D \in \mathcal{J}$ and let T be the 2-torsion divisor corresponding to $g(x)$. Then $\xi(D+T) = W\xi(D)$, where W is the matrix*

$$\begin{pmatrix} g_2^2h_0 + g_0g_2h_2 - g_0^2h_4 & g_0g_2h_3 - g_0g_1h_4 & g_1g_2h_3 - g_1^2h_4 + 2g_0g_2h_4 & g_2 \\ -g_0g_2h_1 - g_0g_1h_2 + g_0^2h_3 & g_2^2h_0 - g_0g_2h_2 + g_0^2h_4 & g_2^2h_1 - g_1g_2h_2 - g_0g_2h_3 & -g_1 \\ -g_1^2h_0 + 2g_0g_2h_0 + g_0g_1h_1 & -g_1g_2h_0 + g_0g_2h_1 & -g_2^2h_0 + g_0g_2h_2 + g_0^2h_4 & g_0 \\ w_1 & w_2 & w_3 & w_4 \end{pmatrix},$$

and

$$\begin{aligned}
w_1 &= -g_2(g_0^2h_1h_3 - g_0g_1h_0h_3 + g_0g_1h_1h_2 + 4g_0g_2h_0h_2 - g_0g_2h_1^2 - g_1^2h_0h_2 \\
&\quad + g_1g_2h_0h_1) \\
w_2 &= -2g_0^2g_2h_1h_4 + g_0g_1^2h_1h_4 + 4g_0g_1g_2h_0h_4 - g_0g_1g_2h_1h_3 - 2g_0g_2^2h_0h_3 \\
&\quad - g_1^3h_0h_4 + g_1^2g_2h_0h_3 \\
w_3 &= -g_0(g_0g_1h_3h_4 + 4g_0g_2h_2h_4 - g_0g_2h_3^2 - g_1^2h_2h_4 - g_1g_2h_1h_4 + g_1g_2h_2h_3 \\
&\quad + g_2^2h_1h_3) \\
w_4 &= -g_0^2h_4 - g_0g_2h_2 - g_2^2h_0.
\end{aligned} \tag{5.17}$$

Proof. See Appendix B.0.1. □

5.4.3 The local power series

Recall from Section 4.3.6 that there are 16 Jacobian coordinates: $a_0, \ldots, a_{15}$. Define $s_i \coloneqq a_i/a_0$. Flynn shows in [Fly90b] that the Jacobian of a genus 2 curve admits a formal group with s_1, s_2 being the local parameters. In particular, we can express the other s_i as power series in s_1, s_2. The projective embedding of the Jacobian consists of 72 linearly independent quadratic equations in the a_i, of which 13 of them contain a_0a_i for $i = 3, \ldots, 15$. After dividing through by a_0^2 and rearranging for s_i, these equations express s_i in terms of s_1, s_2 and the other s_j. We refer to the equation featuring s_i as its base equation.

Remark 5.4.3. *There are more than 13 equations which include these terms but we ignore any equations that contain a_0a_i and a_0a_j for distinct $i, j \in \{3, \ldots, 13\}$.*

Example 5.4.4. *The base equation for s_3 is*

$$\begin{aligned}
s_3 &= -s_{10}^2f_2f_5^2 - s_{11}^2f_0f_5^2 + s_1^2 + 8f_0f_6s_4s_{11} - s_{10}^2f_3^2f_6 - f_4s_3^2 \\
&\quad - f_0s_5^2 + 4s_{10}^2f_1f_5f_6 + 4s_{10}^2f_2f_4f_6 - s_{10}s_3f_3f_5 + 4s_{10}s_3f_2f_6 \\
&\quad + 8f_1f_6s_{10}s_4 + f_1f_5s_{10}s_5 + 4s_{11}^2f_0f_4f_6 - s_{10}s_{11}f_1f_5^2 + 4s_{10}s_{11}f_0f_5f_6 \\
&\quad + 4s_{10}s_{11}f_1f_4f_6 + 4f_0f_5s_{12}s_4 + 2s_{12}s_{10}f_0f_5^2 + 6s_{12}s_{10}f_1f_3f_6 \\
&\quad + 8f_0f_3f_6s_{12}s_{11} + 4s_{14}s_{10}f_0f_2f_6 + 2s_{14}s_{10}f_0f_3f_5 + 3s_{14}s_{10}f_1^2f_6 \\
&\quad + 4f_0f_1f_6s_{14}s_{11} + 2f_0f_1f_5s_{14}s_{12}.
\end{aligned} \tag{5.18}$$

There are similar equations for the other s_i.

For any s_i we obtain a power series in $K[[s_1, s_2]]$ by recursively substituting the base equations for any s_j that appears. We can then extend these to obtain power series in $K[[s_1, s_2]]$ for any polynomial in $K[s_0, \ldots, s_{15}]$.

We shall need to compute the power series for s_i correctly up to a given degree in s_1, s_2. In order to make this computation more practical, it is helpful to introduce a weight on the a_i and the f_j, as in [Fly90b]. We define w by

$$\begin{aligned} w(a_0) &= 4, \\ w(a_1) = w(a_2) &= 3, \\ w(a_3) = w(a_4) = w(a_5) &= 2, \\ w(a_6) = w(a_7) = w(a_8) = w(a_9) &= 1, \\ w(a_{10}) = w(a_{11}) = w(a_{12}) = w(a_{13}) = w(a_{14}) = w(a_{15}) &= 0, \end{aligned} \tag{5.19}$$

and $w(f_i) = 2$ for $i = 0, \ldots 6$. Each of the 72 defining equations of the Jacobian are homogeneous with respect to w. The base equation for s_i is of degree $w(s_i) = w(a_i) - w(a_0)$ and the partial power series derived from recursive substitution are still homogeneous of weight $w(s_i)$. We can use the degree of a monomial with respect to $f_0, \ldots, f_6$ to bound the degree of s_1, s_2 in the monomial. If

$$s_1^{i_1} s_2^{i_2} \prod_{j=0}^{6} f_j^{e_j}, \tag{5.20}$$

occurs in the power series expansion of s_i, where $e_j \geq 0$, then, since the weight of the term is $w(s_i)$, we have

$$i_1 + i_2 = 2 \sum_{j=0}^{6} e_j - w(s_j). \tag{5.21}$$

To expand s_i accurately up to terms of degree d in s_1, s_2, we can recursively substitute in the base equations and discard terms with $\sum_{j=0}^{6} e_j > (w(s_j) + d)/2$. We continue until the resulting series contains no s_i terms for $i > 2$.

Example 5.4.5. *For example, $w(s_5) = -2$. So to compute s_5 accurately up to degree 8 in s_1, s_2, we can recursively substitute and discard any terms of degree greater than $\frac{8+w(s_5)}{2} = 3$ in $f_0, \ldots, f_6$.*

We give the partial power series in Appendix D, accurate up to the stated degree. We will use these in the following sections to compute the Kummer equation of the isogenous curve for the Richelot isogeny.

5.5 Lifting points from the Kummer to the Jacobian

Let $\mathcal{J}$ be the Jacobian of a genus 2 curve, with Kummer surface $\mathcal{K}$. The map $\kappa\colon \mathcal{J} \to \mathcal{K}$ sending a point on the Jacobian to its image on the Kummer surface is degree two, ramified at elements of $\mathcal{J}[2]$. Given a point $\alpha \in \mathcal{K}$, the preimage under κ is $\{D, -D\}$ for some points $D \in \mathcal{J}$. Flynn suggested the idea of using the explicit model of the Jacobian surface in [Fly90b] to compute these preimages explicitly.

Let D have Jacobian coordinates $a(D) = (a_0\colon \cdots a_{15})$ in $\mathbb{P}^{15}$. Then $\kappa(D)$ has Kummer coordinates $\xi(D) = (a_{14}\colon a_{13}\colon a_{12}\colon a_5)$ in $\mathbb{P}^3$. The Kummer coordinates determine all even expressions in the $a_i(D)$, so we are left to determine the odd expressions; that is, $a_i(D)$ for $i = 1, 2, 6, 7, 8, 9$.

Using the 72 quadratic equations in a_i defining the Jacobian, we find that the coordinates a_1, a_2, a_6, a_7, a_8 are all expressible in terms of even expressions and a_9. Thus, if $a_9(D)$ is K-rational, then so are a_1, a_2, a_6, a_7, a_8.

Example 5.5.1. *If the Kummer coordinates are K-rational, then y_1y_2 is determined by*

$$\xi_3 = \frac{F_0(x_1, x_2) - 2y_1y_2}{(x_1 - x_2)^2}, \tag{5.22}$$

together with $\xi_0 = 1, \xi_1 = x_1 + x_2, \xi_2 = x_1x_2$, where $F_0(x_1, x_2)$ is as in Proposition 4.3.7.

We can determine $y_1 + y_2$ using

$$\begin{aligned} y_1 + y_2 &= \frac{y_2^2 - y_1^2}{y_2 - y_1} && (5.23)\\ &= \frac{f(x_2) - f(x_1)}{y_2 - y_1} && (5.24)\\ &= \frac{f(x_2) - f(x_1)}{x_2 - x_1} \cdot \frac{x_2 - x_1}{y_2 - y_1} && (5.25)\\ &= \frac{p(x_1, x_2)}{a_9}, && (5.26) \end{aligned}$$

where $p(x_1, x_2) = \frac{f(x_2) - f(x_1)}{x_2 - x_1}$. The expression $p(x_1, x_2)$ is a symmetric polynomial in x_1, x_2, since we can use Taylor series to write

$$\begin{aligned} f(x_2) - f(x_1) &= \sum_{k=0}^{\deg f} f^{(k)}(x_1)\frac{(x_2 - x_1)^k}{k!} - f(x_1) && (5.27)\\ &= (x_2 - x_1)\sum_{k=1}^{\deg f} f^{(k)}(x_1)\frac{(x_2 - x_1)^{k-1}}{k!}. && (5.28) \end{aligned}$$

Thus $y_1 + y_2$ is defined over $K(a_9)$.

Consider $a_8 = \frac{x_2y_1 - x_1y_2}{x_1 - x_2}$. We can express

$$x_2y_1 - x_1y_2 = \frac{1}{2}\left((y_1 - y_2)(x_1 + x_2) + (y_1 + y_2)(x_2 - x_1)\right). \tag{5.29}$$

Thus

$$a_8 = \frac{a_9 \cdot (x_1 + x_2)}{2} - \frac{p(x_1, x_2)}{2a_9}. \tag{5.30}$$

The other expressions a_1, a_2, a_6, a_7 have similar expressions in terms of a_9 and the Kummer coordinates.

One of the 72 quadratic equations defining the Jacobian $\mathcal{J}$ is

$$\begin{aligned} a_9^2 = a_5a_{14} + f_2a_{14}^2 + f_3a_{14}a_{13} + f_4a_{13}^2 + 3f_5a_{13}a_{12} \\ + f_5a_{13}a_{15} + f_6a_{14}a_{10} + 6f_6a_{12}a_{15} + 8f_6a_{12}^2 + f_6a_{15}^2. \end{aligned} \tag{5.31}$$

Since a_9 is defined over K if and only if a_9^2 is square in K, this gives a method to check whether a point on the Kummer surface lifts to a point on the Jacobian.

We now express the right hand side in terms of the Kummer coordinates. Recall the a_i are only defined projectively, so we can normalise by, e.g. a_{14}^2 to get well-defined affine coordinates. Let $(\xi_0 \colon \xi_1 \colon \xi_2 \colon \xi_3)$ be the Kummer coordinates. Then

$$\xi_1/\xi_0 = a_{13}/a_{14} \tag{5.32}$$

$$\xi_2/\xi_0 = a_{12}/a_{14} \tag{5.33}$$

$$\xi_3/\xi_0 = a_5/a_{14}. \tag{5.34}$$

In terms of the Kummer coordinates, (5.31) is equivalent to

$$\begin{aligned} a_9^2a_{14}^2 = \xi_3\xi_0^3 + f_2\xi_0^4 + f_3\xi_1\xi_0^3 + f_4\xi_1^2\xi_0^2 + 3f_5\xi_1\xi_2\xi_0^2 + f_5\xi_1(\xi_1^2 - 4\xi_2\xi_0)\xi_0 \\ + f_6\xi_2^2\xi_0^2 + 6f_6\xi_2(\xi_1^2 - 4\xi_2\xi_0)\xi_0 + 8f_6\xi_2^2\xi_0^2 + f_6(\xi_1^2 - 4\xi_2\xi_0)^2. \end{aligned} \tag{5.35}$$

Remark 5.5.2. *There are similar expressions for $a_1^2, a_2^2, a_6^2, a_7^2, a_8^2$, and if $a_9^2 = 0$ then we may need to use these instead.*

We have proved the following.

Proposition 5.5.3. *Let $\mathcal{K}$ be the Kummer surface and $\mathcal{J}$ the Jacobian of a genus 2 curve over a field K. Then $\alpha \in \mathcal{K}(K)$ lifts to $D \in \mathcal{J}(K)$ such that $\kappa(D) = \alpha$ if and only if a_9^2 is a square in K. Thus D is defined over $K(a_9)$.*

Lifting points in practice Suppose $a_9(D)$ is K-rational and the Kummer coordinates $\xi(D)$ are K-rational. Then we can recover D in Mumford notation $\langle a(x), b(x), d\rangle$ as follows. The first three Kummer coordinates are $(\xi_0 \colon \xi_1 \colon \xi_2) = (1 \colon x_1 + x_2 \colon x_1 x_2)$; hence $a(x) = \xi_0 x^2 - \xi_1 x + \xi_2$. We also have $b(x)^2 - f(x) = a(x)c(x)$ for some $b(x), c(x)$; in particular, $b(x)^2 \equiv f(x) \pmod{a(x)}$. If $a(x)$ is irreducible over K, then we can solve this by considering the number field $M = K[T]/a(T)$; then $f(T) = e(T)^2$ for some $e \in K[T]$, and we let $b(x) = e(x)$. If $a(x)$ is reducible then we do this for each irreducible factor and use the Chinese Remainder Theorem. We know that $f(x)$ is square modulo $a(x)$, since we assumed a_9 is K-rational, so D is defined over K.

Example 5.5.4. *Let $\mathcal{C}$ be the genus 2 curve $y^2 = x^5 + 1$ and let $\mathcal{J}$ be its Jacobian and $\mathcal{K}$ be its Kummer surface. The Kummer equation is*

$$(\xi_1^2 - 4\xi_0\xi_2)\xi_3^2 - (4\xi_0^3 + 2\xi_1\xi_2^2)\xi_3 + 4\xi_0^2\xi_1\xi_2 - 4\xi_0\xi_1^3 + \xi_2^4. \tag{5.36}$$

We see that $\alpha = (1 \colon 2 \colon 2 \colon 0)$ satisfies the equation, and can compute $a_9^2(\alpha) = 4$ using (5.35) with $f_1 = f_2 = f_3 = f_4 = f_6 = 0$, $\xi_3 = 0$, and $a_{14} = 1$. Let $D = \langle a(x), b(x), d\rangle \in \mathcal{J}$ satisfy $\kappa(D) = \alpha$. The first three Kummer coordinates are $(\xi_0 \colon \xi_1 \colon \xi_2) = (1 \colon x_1 + x_2 \colon x_1 x_2)$, where $D = (x_1, y_1) + (x_2, y_2) - \infty^+ - \infty-$; hence $a(x) = x^2 - 2x + 2$. Now $f(x) \equiv -4x + 1 \equiv (2x - 3)^2 \pmod{a(x)}$. Hence $D = \langle x^2 - 2x + 2, 2x - 3, 2\rangle \in \mathcal{J}(K)$ satisfies $\kappa(D) = (1 \colon 2 \colon 2 \colon 0) \in \mathcal{K}(K)$, as does $-D$.

Twists If $\alpha \in \mathcal{K}(K)$ is a point on the Kummer with $a_9^2(\alpha)$ not a square in K, then we can twist the curve by $a_9^2(\alpha)$ and lift the point on the Kummer to the Jacobian of $y^2 = a_9^2(\alpha) f(x)$.

5.6 Computing a basis for the Kummer surface of the isogenous curve

Let $\varphi \colon \mathcal{J} \to \mathcal{J}'$ be an (n, n)-isogeny. By Proposition 2.2.16 there is a principal polarisation on $\mathcal{J}'$ with theta divisor $\Theta_{\mathcal{J}'}$ such that $\varphi^*(\Theta_{\mathcal{J}'}) = n\Theta_{\mathcal{J}}$. We would like to understand $2\Theta_{\mathcal{J}'}$, since this gives a projective embedding of $\mathcal{K}'$. The following method is based on that used in [BFT14] and [Fly15] to derive the isogenous curves for $(3, 3)$ and $(5, 5)$-isogeny on genus 2 curves, respectively.

Remark 5.6.1. *Note that $2\Theta_{\mathcal{J}'}$ is linearly equivalent to $\Theta^+_{\mathcal{J}'} + \Theta^-_{\mathcal{J}'}$, which is rational.*

First note that $\varphi^*\mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'}) \subset \mathscr{O}_{\mathcal{J}}(2n\Theta_{\mathcal{J}})$. Since each $s \in \mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'})$ is invariant under the -1 map on $\mathcal{J}'$, and since $\varphi\colon \mathcal{J} \to \mathcal{J}' = \mathcal{J}/\Sigma$ is the quotient by Σ, then $s \circ \varphi$ is invariant by both the -1 map on $\mathcal{J}$ and also by translation by elements of Σ.

Lemma 5.6.2. *Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be an isogeny of Jacobians. Then*

$$\varphi^*\mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'}) = \mathscr{O}_{\mathcal{J}}(2n\Theta)^+ \cap \mathscr{O}_{\mathcal{J}}(2n\Theta)^{\Sigma}, \tag{5.37}$$

where the superscript $+$ denotes functions invariant by -1 and the superscript Σ denotes functions invariant by translation by Σ.

Proof. If $s \in \mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'})$ then s is invariant by $-1\colon \mathcal{J}' \to \mathcal{J}'$; since φ is an isogeny, $s\circ\varphi$ is also invariant by -1. Moreover, $\Sigma = \ker\ \varphi$, so $s \circ \varphi$ is invariant under translation by elements of Σ.

Conversely, any function t in $\mathscr{O}_{\mathcal{J}}(2n\Theta_{\mathcal{J}})^{\Sigma}$ factors through $\varphi\colon \mathcal{J} \to \mathcal{J}/\Sigma$, so is of the form $s\circ\varphi$ for some function s on $\mathcal{J}'$. Any function on $\mathcal{J}$ that is invariant under the -1 map descends to a function on the Kummer surface $\mathcal{K}$, and is therefore expressible as a homogeneous combination of the Kummer coordinates. In particular, $\mathscr{O}_{\mathcal{J}}(2n\Theta)$ consists of degree n forms in $\xi_0, \xi_1, \xi_2, \xi_3$. Thus, if $t = s \circ \varphi$ is invariant under -1, then s is also invariant under -1, so that s is a homogeneous combination of $\xi'_0, \xi'_1, \xi'_2, \xi'_3$. But φ has degree n, so it is a linear combination. That is, $s \in \mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'})$. □

We now have the following strategy for computing the curve $\mathcal{C}'$ such that $\mathcal{J}/\Sigma \cong \mathcal{J}(\mathcal{C}')$, as well as the isogeny descended to the Kummer surfaces. Consider the commutative diagram

$$\begin{array}{ccc} \mathcal{J} & \xrightarrow{\varphi} & \mathcal{J}' \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} \\ \mathcal{K} & \xrightarrow{\varphi} & \mathcal{K}' \end{array} \tag{5.38}$$

We first compute homogeneous degree n forms $\ell_0, \ell_1, \ell_2, \ell_3$ in $\xi_0, \xi_1, \xi_2, \xi_3$ that are invariant under translation by elements in Σ. By Lemma 5.6.2, each homogeneous n-form ℓ_i is of the form $\eta_i \circ \varphi$, where each η_i is a linear combination of the Kummer coordinates ξ'_i of $\mathcal{C}'$. We find a basis $\ell_0, \ldots, \ell_3$ for the space of such η, and then look for a change of basis matrix M such that $\varphi \circ \kappa = M\ell = \kappa' \circ \varphi$ in (5.38).

In practice, we find M by first finding any quartic equation satisfied by $\ell_0, \ell_1, \ell_2, \ell_3$ and then changing coordinates to put it in the same form as the Kummer equation. We discuss this in more detail in Section 5.7.2.

5.6.1 Reducing expressions modulo the Kummer equation

We also give Algorithm 3 for computing expressions modulo the Kummer equation, originally due to Flynn. This lets us reduce polynomial expressions in $\xi_0, \xi_1, \xi_2, \xi_3$ to a unique representative modulo the Kummer equation, and can be usefully combined with the algorithms for finding relations between polynomials in Section 4.3.3.

Algorithm: Reduce expressions modulo the Kummer equation
Input: Homogeneous polynomial φ in z_0, z_1, z_2, z_3; degree 5 or 6 polynomial $f(x)$
Compute the Kummer equation $Q(z_0, z_1, z_2, z_3)$ for $y^2 = f(x)$
Let $P(z_0, z_1, z_2, z_3) = Q - z_1^2 z_3^2$
`/* Replace all occurrences of` $z_1^2 z_3^2$ `with the other terms of the Kummer equation. */`
Divide with remainder: $\varphi = q(z_1^2 z_3^2) + r$
while $q \neq 0$ **do**
  $\varphi = -qP + r$
  Divide with remainder: $\varphi = q(z_1^2 z_3^2) + r$
end
return φ

Algorithm 3: Reduce expressions modulo the Kummer equation

5.7 The Richelot isogeny

We now carry out the plan above for the Richelot isogeny. We first determine the genus 2 curves whose Jacobians admit $(2,2)$-subgroups. Then we find homogeneous degree 2 functions on the Kummer surface that are invariant under translation by this subgroup, and find the quartic relations they satisfy. We use the power series to more easily compute the quartic relations. We then find the change of basis matrix so that the invariant functions map onto a Kummer surface, and determine the equation of the curve up to twist. This gives an explicit projective map between the Kummer surfaces of the original curve and the Richelot-isogenous curve, all defined over the ground field.

All of this is well-known, but I hope that the explicit explanation is helpful. We also use this approach again to derive the $(5,5)$-isogeny in Section 5.8, so it is worthwhile to see the simpler case of $(2,2)$-isogenies first.

The MAGMA file `richelot/derive_richelot_on_kummer.m` in [Nic18] explicitly derives each step of the following, and gives the projective map. I wasn't previously able to find these written in general, so I hope this is a valuable resource.

5.7.1 $(2,2)$-subgroups

We first characterise genus 2 curves over a field K whose Jacobians admit a $(2,2)$-subgroup all of whose elements are K-rational. This is well-known (see [CF96], [Smi05]). The case when the elements are not K-rational is analysed in [BD11].

Let K be a field, and let $G_1(x), G_2(x), G_3(x)$ be polynomials in $K[x]$. As in [Smi05], we define an equivalence relation on $K[x] \times K[x] \times K[x]$ by

$$(G_1(x), G_2(x), G_3(x)) \sim (G_{\sigma 1}(x), G_{\sigma 2}(x), G_{\sigma 3}(x)) \tag{5.39}$$

for all $\sigma \in S_3$, and

$$(G_1(x), G_2(x), G_3(x)) \sim (\alpha_1 G_1(x), \alpha_2 G_2(x), \alpha_3 G_3(x)) \tag{5.40}$$

for all $\alpha_1, \alpha_2, \alpha_3 \in K^*$ such that $\alpha_1\alpha_2\alpha_3 = 1$. Write $[(G_1(x), G_2(x), G_3(x))]$ for the class of a triple under this equivalence relation.

We can now classify $(2,2)$-subgroups of $\mathcal{J}[2]$ whose elements are all K-rational.

Proposition 5.7.1. *Let $f(x)$ be a square-free polynomial of degree 5 or 6, and let $\mathcal{J}$ be the Jacobian of the genus 2 curve $\mathcal{C}\colon y^2 = f(x)$. The $(2,2)$-subgroups of $\mathcal{J}$ are in one-to-one correspondence with the classes $[(G_1(x), G_2(x), G_3(x))]$ such that $G_1(x)G_2(x)G_3(x) = f(x)$ and $\deg G_i \leq 2$ for each $i = 1, 2, 3$.*

Proof. First note that $(2,2)$-subgroups of $\mathcal{J}[2]$ whose elements are all defined over K are generated by two distinct rational 2-torsion points T_1, T_2. Each T_i corresponds to a quadratic factor of $f(x)$ (one can be linear if $\deg f = 5$), and since the Weil pairing acts trivially, the quadratic factors are coprime (see Proposition 5.2.5). Then $T_3 = T_1 + T_2$ corresponds to another quadratic factor G_3 and we can scale G_1, G_2, G_3 such that $f(x) = G_1(x)G_2(x)G_3(x)$.

Conversely, to every representative triple $(H_1(x), H_2(x), H_3(x))$ in the class, the H_i correspond to 2-torsion points T_i that generate a subgroup of $\mathcal{J}[2]$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with pairwise trivial Weil pairing. Indeed, since $\operatorname{div} y = T_1 + T_2 + T_3$, we know that $T_1 + T_2 + T_3 = 0$, and since the factors are coprime, we know $e_2(T_i, T_j) = 1$ for all i, j (see Proposition 5.2.5). □

Example 5.7.2. *The genus 2 curve $y^2 = x(x^2 - 3)(x^2 + x + 1)$ admits a Richelot isogeny over $K = \mathbb{Q}$ with $G_1(x) = x, G_2(x) = x^2 - 3, G_3(x) = x^2 + x + 1$.*

The genus 2 curve $y^2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})(x^2 - 3)$ admits a Richelot isogeny over $K = \mathbb{Q}(\sqrt{2})$ with $G_1(x) = x^2 - \sqrt{2}, G_2(x) = x^2 + \sqrt{2}, G_3(x) = x^2 - 3$. Let T_i

denote the 2-torsion point corresponding to G_i. Then $\Sigma = \langle T_1, T_2 \rangle$ is $\mathbb{Q}$-rational as a set. Moreover, the 2-Weil pairing acts trivially, since the factors are coprime. Hence Σ is a $(2,2)$-subgroup over $\mathbb{Q}$ also. See [BD11] for more details on Richelot isogenies when the $(2,2)$-subgroup isn't completely defined over $\mathbb{Q}$.

5.7.2 Computing the Richelot isogeny

In this section we show how to compute the Richelot isogeny: $\mathcal{J} \to \mathcal{J}/\Sigma$, where Σ is a $(2,2)$-subgroup of $\mathcal{J}[2]$. This method is originally due to Flynn ([Fly94]).

Let Σ be a $(2,2)$-subgroup of $\mathcal{J}[2]$. The image of the map $\mathcal{J} \to \mathcal{J}/\Sigma$ is a principally polarised abelian variety, and we expect it to be the Jacobian of another genus 2 curve, $\mathcal{C}'$. One way to compute the image is to compute the induced map on Kummer surfaces, and show that it lifts to a map of Jacobians.

The map on Kummer surfaces is defined up to twists of the curves (Proposition 5.4.1). We can compute the twist for any specific curve $\mathcal{C}$ and subgroup Σ by mapping a point on $\mathcal{J}$ to a point on $\mathcal{K}'$ and then seeing which twist of f' has a rational lift of the Kummer point to the Jacobian $\mathcal{J}'$.

The isogeny can be degenerate. As shown in [CF96], this occurs if and only if $\Delta = 0$, where

$$\Delta = \det \begin{pmatrix} g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \\ g_{30} & g_{31} & g_{32} \end{pmatrix}, \tag{5.41}$$

where we write each $G_i(x) = g_{i0} + g_{i1}x + g_{i2}x^2$. Note that $\Delta = 0$ if and only if G_1, G_2, G_3 are K-linearly dependent.

Remark 5.7.3. *There is another approach to compute $\mathcal{J} \to \mathcal{J}/\Sigma$, using correspondences ([Mes09], [Smi05]). We use the method on Kummer surfaces found in [CF96], [BFT14], [Fly15] because it generalises to $(4,4)$-isogenies and $(5,5)$-isogenies.*

We also introduce the bracket notation $[A(x), B(x)] = A(x)B'(x) - A'(x)B(x)$ for polynomials $A(x), B(x)$.

In the next few sections we prove the following theorem.

Theorem 5.7.4. *Let $\mathcal{C}$ be the genus 2 curve*

$$\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x), \tag{5.42}$$

where $G_i(x) = g_{i2}x^2 + g_{i1}x + g_{i0}$*, and let* $\mathcal{J}$ *denote the Jacobian of* $\mathcal{C}$*. For* $i = 1, 2, 3$*, let* T_i *denote the 2-torsion divisor corresponding to* G_i*. Let* $\Sigma = \langle T_1, T_2 \rangle \subset \mathcal{J}[2]$*. Then* $\mathcal{J}' = \mathcal{J}/\Sigma$ *is the Jacobian of the curve* $\mathcal{C}'$ *given by*

$$\mathcal{C}' \colon y^2 = L_1(x)L_2(x)L_3(x), \tag{5.43}$$

where

$$L_i(x) = \frac{[G_{i+1}(x), G_{i+2}(x)]}{\Delta}, \tag{5.44}$$

with indices interpreted cyclically in $\{1, 2, 3\}$*. Here* Δ *is the determinant from* (5.41)*. The induced map on Kummer surfaces* $\mathcal{K} \to \mathcal{K}'$ *is given by explicit homogeneous quadratics in* $\xi_0, \xi_1, \xi_2, \xi_3$*.*

Remark 5.7.5. *Our definition of* $L_i(x)$ *agrees with [Smi05]. The definition in [CF96] is* $\tilde{L}_i(x) = [G_{i+1}(x), G_{i+2}(x)]$*; that is, not dividing by* Δ*. These are equivalent, but the isogenous curve in the second case is* $y^2 = \Delta\tilde{L}_1(x)\tilde{L}_2(x)\tilde{L}_3(x)$*. The advantage of the definition we use here is that the operation* $(G_1(x), G_2(x), G_3(x)) \mapsto (L_1(x), L_2(x), L_3(x))$ *is an involution.*

Remark 5.7.6. *Note that* Δ *changes sign with an odd permutation of the* G_i*, but the product* $L_1(x)L_2(x)L_3(x)$ *is invariant, which leaves the isogenous curve invariant under permutations of the* G_i*.*

In our characterisation of the $(2, 2)$*-subgroups, we do not distinguish the isogeny* $\mathcal{J} \to \mathcal{J}/\Sigma$ *from its composition with* -1*. This isn't a major problem for us, as we mainly work on the Kummer surface. In [Smi05], Smith distinguishes the isogenies corresponding to* $(G_1(x), G_2(x), G_3(x))$ *and* $(G_{\sigma 1}(x), G_{\sigma 2}(x), G_{\sigma 3}(x))$ *whenever* $\sigma \in S_3$ *is an odd permutation; they are related by composing with* -1*.*

We can fix this by determining where to send the coordinate a_9 *on* $\mathcal{J}$*. Since* a_9^2 *is even, it is determined by the Kummer coordinates, and by making a fixed choice of* a_9 *we determine either* φ *or* $-\varphi$*. We don't do this here.*

5.7.3 Invariant functions for a $(2, 2)$-subgroup

Let Σ be a $(2, 2)$-subgroup, corresponding to the splitting $(G_1(x), G_2(x), G_3(x))$ (with $\deg G_i(x) \leq 2$). Let T_i be the 2-torsion point corresponding to $G_i(x)$ for $i = 1, 2, 3$. Let φ be the corresponding Richelot isogeny. A basis for $\varphi^*(\mathscr{O}_{\mathcal{J}'}(\Theta^+_{\mathcal{J}'} + \Theta^-_{\mathcal{J}'}))$ consists of quadratic forms in $\xi_0, \xi_1, \xi_2, \xi_3$ that are invariant under translation by T_1 and T_2

(see Lemma 5.6.2). For other (n, n)-isogenies it can be more complicated to find such functions, but in this case the functions

$$\eta_{ij} \coloneqq \xi_i(D)\xi_j(D + T_1) + \xi_i(D + T_1)\xi_j(D), \tag{5.45}$$

for $i, j \in \{0, 1, 2, 3\}$ are invariant under translation by T_1, up to scaling. Indeed,

$$\eta_{ij}(D + T_1) = \xi_i(D + T_1)\xi_j(D + 2T_1) + \xi_i(D + 2T_1)\xi_j(D + T_1), \tag{5.46}$$

and the vector of coordinates $\xi(D + 2T_1)$ is just $c\xi(D)$ for some constant c, since the projective point $(\xi_0(D) \colon \xi_1(D) \colon \xi_2(D) \colon \xi_3(D))$ is invariant on replacing D by a linearly equivalent divisor. Hence $\eta_{ij}(D + T_1) = c\eta_{ij}(D)$, where the scalar c depends on D.

Similarly, we define

$$\mu_{ij} \coloneqq \xi_i(D)\xi_j(D + T_2) + \xi_i(D + T_2)\xi_j(D), \tag{5.47}$$

which is invariant (up to scaling) under translation by T_2. We now take the intersection of the space spanned by the η_{ij} and the space spanned by the μ_{ij}. If this is four dimensional then it gives a basis for $\varphi^*\mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'})$. To calculate the η_{ij} and μ_{ij} we need to compute $\xi_i(D + T)$ where D is a general divisor and T is a 2-torsion divisor, which we can do using the matrix W_T for translation-by-T (see Proposition 5.4.2).

For example, T_1 has Kummer coordinates

$$\xi(T_1) = \begin{pmatrix} g_{12} \\ -g_{11} \\ g_{10} \\ -g_{10}^2 g_{22} g_{32} - g_{10} g_{12}(g_{20} g_{32} + g_{21} g_{31} + g_{22} g_{30}) - g_{12}^2 g_{20} g_{30} \end{pmatrix}, \tag{5.48}$$

which we can see by computing $W_1\xi(0)$, which just extracts the last column of W_1 (since $\xi(0) = (0 \colon 0 \colon 0 \colon 1)$).

Proposition 5.4.2 explicitly gives the matrix W_T for any 2-torsion point T. We multiply by the Kummer coordinates $\xi(D)$ of D to compute $\xi(D + T) = W_T\xi(D)$. Thus we can compute each η_{ij} and μ_{ij}. Let V be the K-vector space of quadratic functions in $\xi_0, \xi_1, \xi_2, \xi_3$.

The MAGMA program `richelot/derive_richelot_on_kummer.m` in [Nic18] shows that $\{\eta_{ij} \colon i, j \in \{0, 1, 2, 3\}\}$ and $\{\mu_{ij} \colon i, j \in \{0, 1, 2, 3\}\}$ each span a 6-dimensional subspace of V. Their intersection is a 4-dimensional subspace and forms a basis for $\varphi^*(\mathscr{O}_{\mathcal{J}'}(2\Theta_{\mathcal{J}'}))$.

We can change basis to one of the form

$$\ell_0 = \xi_0\xi_3 + \cdots \tag{5.49}$$

$$\ell_1 = \xi_1\xi_3 + \cdots \tag{5.50}$$

$$\ell_2 = \xi_2\xi_3 + \cdots \tag{5.51}$$

$$\ell_3 = \xi_3^2 + \cdots . \tag{5.52}$$

Each ℓ_i is homogeneous of degree 6 in the g_{jk} and homogeneous of degree 2 in the ξ_j. The expressions are too large to display here, so we refer to the file `richelot/derive_richelot_on_kummer.m` in [Nic18].

5.7.3.1 Computing the Kummer equation of the isogenous curve

Recall that we would like to find the curve $\mathcal{C}'$ such that the Jacobian $\mathcal{J}'$ of $\mathcal{C}'$ is

$$\mathcal{J}' = \mathcal{J}/\Sigma, \tag{5.53}$$

where Σ is the copy of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in $\mathcal{J}$ generated by $\langle T_1, T_2 \rangle$.

We have explicit expressions for the map $\mathcal{J} \to \mathcal{J}/\Sigma$ on the Kummer surface. Namely,

$$(\xi_0 \colon \xi_1 \colon \xi_2 \colon \xi_3) \mapsto (\ell_0 \colon \ell_1 \colon \ell_2 \colon \ell_3). \tag{5.54}$$

The strategy is to compute a quartic equation Q' satisfied by the ℓ_i, which in this case means that $Q'(\ell_0, \ell_1, \ell_2, \ell_3)$ is divisible by $Q(\xi_0, \xi_1, \xi_2, \xi_3)$, where Q is the Kummer equation of $\mathcal{K}$. Unfortunately, the expressions for ℓ_i are too large to do this naively. Instead, Flynn suggested to use the local power series. They encode the equation Q, so if ℓ_i satisfy an equation, then it should also be satisfied when we substitute in the power series. By computing the power series accurately to a low degree, and looking at the lowest degree terms of all quartic monomials in ℓ_i, we can try to find a linear combination of these which vanishes.

We only need to find the part of the quartic equation of $\mathcal{K}'$ that is linear in ℓ_3, since this gives the cubic form $\Phi'(z_0, z_1, z_2)$ from which we can read off the curve.

Given a power series $h(s_1, s_2) = \sum_{k=0}^{\infty} \sum_{i+j=k} h_{ij} s_1^i s_2^j \in K[[s_1, s_2]]$, we write $h + \mathcal{O}(\geq n)$ to denote $\sum_{k=0}^{n-1} \sum_{i+j=k} h_{ij} s_1^i s_2^j$. This is the part of h consisting of terms of degree at most $n-1$ in s_1, s_2.

We look for an equation of the form $A(\ell_0, \ell_1, \ell_2)\ell_3^2 + B(\ell_0, \ell_1, \ell_2)\ell_3 + C(\ell_0, \ell_1, \ell_2)$ with A, B, C homogeneous of degree 2, 3, 4, respectively. The lowest degree terms of

the ℓ_i in s_1, s_2 are

$$\ell_0 = s_2^6 \tag{5.55}$$

$$\ell_1 = 2s_1 s_2^5 \tag{5.56}$$

$$\ell_2 = s_1^2 s_2^4 \tag{5.57}$$

$$\ell_3 = s_2^4. \tag{5.58}$$

Note that the leading terms of ℓ_0, ℓ_1, ℓ_2 are degree 6 in s_1, s_2, while the leading term of ℓ_3 is degree 4 in s_1, s_2. Thus the lowest degree terms of A, B, C in terms of s_1, s_2 are at least 20, 22, 24, respectively. To determine B we work modulo $\mathcal{O}(\geq 24)$, which allows us to ignore C.

We consider the vector space spanned by the 12 monomials $\mathcal{M}$ given by $z_1^2 z_3^2, z_0 z_2 z_3$ and $\{z_0^{i_0} z_1^{i_1} z_2^{i_2} z_3 \colon i_0 + i_1 + i_2 = 3, i_j \geq 0\}$. For each monomial $m \in \mathcal{M}$, we compute $m(\ell_0, \ell_1, \ell_2, \ell_3) + \mathcal{O}(\geq 24)$, and compute the space $\mathcal{S}$ of linear relations they satisfy. We have $\dim \mathcal{S} = 4$, but three of those dimensions are spanned by the relations

$$\ell_0^2 \ell_2 \ell_3 - 1/4 \ell_0 \ell_1^2 \ell_3 = \mathcal{O}(\geq 24) \tag{5.59}$$

$$\ell_0 \ell_1 \ell_2 \ell_3 - 1/4 \ell_1^3 \ell_3 = \mathcal{O}(\geq 24) \tag{5.60}$$

$$\ell_0 \ell_2^2 \ell_3 - 1/4 \ell_1^2 \ell_2 \ell_3 = \mathcal{O}(\geq 24), \tag{5.61}$$

which aren't useful. There is then a unique vector in the nullspace that has no terms of the form $\ell_0^2 \ell_2 \ell_3, \ell_0 \ell_1 \ell_2 \ell_3, \ell_0 \ell_2^2 \ell_3$. This gives a putative $B(z_0, z_1, z_2)$. We change variables to $\ell_0, \ell_1, \ell_2, \ell_3 + a_0 \ell_0 + a_1 \ell_1 + a_2 \ell_2$ so that our new $B(z_0, z_1, z_2)$ is of the expected form for the cubic in a Kummer equation; that is, has no terms of the form: $z_i z_2^2$ for $i = 0, 1, 2$. We can now read off from the new $B(z_0, z_1, z_2)$ a putative equation for the isogenous curve, which is a multiple of

$$\tilde{f}(x) = L_1(x) L_2(x) L_3(x), \tag{5.62}$$

as in Theorem 5.7.4.

We now suspect that a change of variables $\ell_0, \ell_1, \ell_2, \ell_3$ satisfies the quartic equation $Q'(z_0, z_1, z_2, z_3)$ for the Kummer surface of $\mathcal{C}' \colon y^2 = \tilde{f}(x)$. We try $\ell_3 = \ell_3 + b_0 \ell_0 + b_1 \ell_1 + b_2 \ell_2$ for some b_i to be determined. We compute $Q'(\ell_0, \ell_1, \ell_2, \ell_3 + b_0 \ell_0 + b_1 \ell_1 + b_2 \ell_2)$ and then solve for b_0, b_1, b_2.

We derive this in detail in `richelot/derive_richelot_on_kummer.m` in [Nic18].

We don't derive the correct twist here, since that is well-known in the literature. But we can now twist the final expression by the correct twist to derive the projective

map on the Kummer surfaces induced by the Richelot isogeny. We give the explicit projective map in `richelot/richelot_on_kummer.m` in [Nic18]. We verify that the image lies on $\mathcal{K}'$ by checking that $Q'(\ell'_0, \ell'_1, \ell'_2, \ell'_3)$ is divisible by $Q(\xi_0, \xi_1, \xi_2, \xi_3)$.

Remark 5.7.7. *In summary, it is too computationally expensive to naively compute the quartic relation satisfied by ℓ_i with general coefficients g_{jk}. Thus we use the power series to find a putative curve $\tilde{f}$ and then try to make a minor change of variables to map into $\mathcal{K}'$. Since we already know the curve $\tilde{f}$, we could have instead skipped this step and computed the projective map on the Kummers slightly more easily. But for the $(5,5)$-isogeny we don't know $\tilde{f}$, so this step is important in that case.*

This proves Theorem 5.7.4, up to the twist. Note that with specialised coefficients g_{jk}, we can compute the twist easily. We will see how to do this in the $(5,5)$-case.

5.7.4 Using the W_T matrices to derive the Richelot isogeny

In this section we give a separate way of deriving the Richelot isogeny, using the W_T matrices, which was originally given in [Fly94]. We use this later to compute the 4-torsion points that double to a given 2-torsion point.

Proposition 5.7.8. *Let $f(x)$ be a degree 5 or 6 polynomial, and let G_1, G_2, G_3 be a Richelot splitting of $f(x)$. Let $L_i(x)$ be defined as above. Let $\mathcal{C}\colon y^2 = f(x)$ and $\mathcal{C}'\colon y^2 = L_1(x)L_2(x)L_3(x)$. The map on the Kummer surfaces is of the form $\xi \mapsto \theta_2^{-1} \circ s \circ \theta_1$, where θ_1, θ_2 are invertible linear transformations and s is the map $s([v_0\colon v_1\colon v_2\colon v_3]) = [v_0^2\colon v_1^2\colon v_2^2\colon v_3^2]$.*

The maps θ_1, θ_2 are in general not defined over the ground field.

Remark 5.7.9. *There are two Richelot isogenies $\mathcal{J} \to \mathcal{J}'$, with composition with $[-1]$ taking one to the other. They are both the same map on the Kummer surfaces $\mathcal{K} \to \mathcal{K}'$.*

Let Σ be the $(2,2)$-subgroup on $\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x)$ corresponding to the 2-torsion points $T_i = \langle G_i(x), 0\rangle$. Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be the corresponding Richelot isogeny.

Our strategy is to change coordinates to simultaneously diagonalise the matrices W_{T_i}. We show that in these coordinates, the coordinate-squaring map $s\colon \mathbb{P}^3 \to \mathbb{P}^3$ restricts to a map from $\mathcal{K}$ to another variety $V \subset \mathbb{P}^3$ whose kernel is $\kappa(\Sigma)$. We finally find an isomorphism $V \to \mathcal{K}'$, where $\mathcal{K}'$ is the Kummer surface of the isogenous Jacobian.

Recall an $n \times n$ matrix M is diagonalisable over K if and only if its minimal polynomial is a product of distinct linear factors over K. Direct computation shows that $W_T^2 = c_T I$, where I is the 4×4 identity matrix. Hence the minimal polynomial m_T of W_T divides $x^2 - c_T$, and since W_T is not a multiple of I, we have $m_T = x^2 - c_T$. Thus W_T is diagonalisable if and only if c_T is square, so is certainly diagonalisable over $K(\sqrt{c_T})$. The eigenvectors of W_T are defined over the same extension.

A set of matrices is simultaneously diagonalisable if and only if they commute. Let W_i denote the translation-by-T_i matrix. Then an explicit computation shows that W_1, W_2, W_3 commute. If S, T are distinct 2-torsion points with overlapping support, then their matrices W_S, W_T anticommute.

Remark 5.7.10. *Eigenvectors for W_T in $\mathbb{A}^4$ need not correspond to points on the Kummer surface. For example, the dimensions of the eigenspaces can be larger than 1, and the Kummer surface does not contain a projective line.*

Lemma 5.7.11. *Let $\mathcal{J}$ be the Jacobian of a genus 2 curve $\mathcal{C}\colon y^2 = f(x)$ over a field K, and let $\mathcal{K}$ be its Kummer surface. Let T be a nonzero element of $\mathcal{J}[2]$ and let W_T be the translation-by-T matrix from Proposition 5.4.2. Let $D \in \mathcal{J}(\overline{K})$ and let $\boldsymbol{v} \in \mathbb{A}^4$ represent the Kummer coordinates $\xi(D)$ of D from Proposition 4.3.7. Then $[2](D) = T$ if and only if $\boldsymbol{v}$ is an eigenvector for W_T.*

Proof. Consider the translation-by-T map on $\mathcal{J}$, which is given on $\mathcal{K}$ by the matrix W_T. Let $\boldsymbol{v} \in \mathbb{A}^4_K$ represent the projective point on the Kummer corresponding to $D \in \mathcal{J}$. If $\boldsymbol{v}$ is an eigenvector for W_T, then there is $\lambda \neq 0$ such that $W_T\boldsymbol{v} = \lambda\boldsymbol{v}$. By Proposition 5.4.2, we know that $W_T\boldsymbol{v} = c_T\boldsymbol{u}$, where $\boldsymbol{u}$ is a vector representing the projective point $\xi(D+T)$, and where c_T is a nonzero constant. Consequently, $\lambda\boldsymbol{v} = c_T\boldsymbol{u}$ in $\mathbb{A}^4$, which implies that $\xi(D) = \xi(D+T)$ on $\mathcal{K}$. Thus one of $D = D+T, D = -(D+T), -D = D+T, -D = -(D+T)$ hold. Since T is assumed nonzero, the only possibility is $2D = -T = T$.

Conversely, if $[2](D) = T$, then we also have $D = -D - T$, so that $\xi(D) = \xi(D+T)$ on $\mathcal{K} \subset \mathbb{P}^3$. Let $\boldsymbol{v}$ be a vector representing $\xi(D)$ and consider $W_T\boldsymbol{v}$. By Proposition 5.4.2, we have $W_T\boldsymbol{v} = \boldsymbol{u}$, where $\boldsymbol{u}$ is a vector representing $\xi(D+T)$. Since $\xi(D) = \xi(D+T)$, there is a nonzero λ such that $\lambda\boldsymbol{u} = \boldsymbol{v}$. Thus $W_T\boldsymbol{v} = \lambda\boldsymbol{v}$. □

Let $L = K(\sqrt{c_1}, \sqrt{c_2})$ be the field extension such that W_1 and W_2 are diagonalisable. Since $W_3 = W_1W_2$, then W_3 is also diagonalisable. Let M be a matrix such that for all $i \in \{1,2,3\}$, we have $M^{-1}W_iM = \Lambda_i$ is diagonal.

Recall $W_T\xi(D) = \alpha_T\xi(D+T)$ for some nonzero α_T. Since $W_T^2 = c_T I$, we have $\alpha_T^2 = c_T$. Transforming to the basis $\eta = M^{-1}\xi$; that is, $\eta_i(D) = \sum_{j=1}^4 M_{ij}^{-1}\xi_j(D)$, we find

$$\eta(D+T) = M^{-1}\xi(D+T) = \frac{1}{\alpha_T}M^{-1}W_T\xi(D) \tag{5.63}$$

$$= \frac{1}{\alpha_T}M^{-1}W_T M\eta(D) = \frac{1}{\alpha_T}\Lambda_T\eta(D). \tag{5.64}$$

Since Λ_T is diagonal with entries $\pm\sqrt{c_T}$, we get $\eta(D+T)_i = \pm\eta(D)_i$ for each $i = 0, 1, 2, 3$. Hence $\eta(D+T)^2$ and $\eta(D)^2$ are projectively equal.

Thus the Richelot map on $\eta(D)$ is $[\eta_0 \colon \eta_1 \colon \eta_2 \colon \eta_3] \mapsto [\eta_0^2 \colon \eta_1^2 \colon \eta_2^2 \colon \eta_3^2]$. More precisely, this map sends D and $D+T$ to the same points for all $D \in \mathcal{K}$ and $T \in \Sigma = \langle T_1, T_2\rangle$. The map $\mathcal{J} \to \mathcal{K} \to \mathcal{K}'$ is exactly taking the quotient by -1 and then Σ.

Remark 5.7.12. *Although it is interesting how we produce the equation of $\tilde{\mathcal{K}}$, in fact it suffices to check that the map $\mathcal{K} \to \tilde{\mathcal{K}}$ is well-defined and Σ-invariant with all coordinates homogeneous of degree 2.*

We can then map back to the standard form of the Kummer as described in Section 5.7.3.1 in order to express the image as the Kummer surface of a genus 2 curve. On doing this, we find the image is the Kummer surface of a twist of $y^2 = L_1(x)L_2(x)L_3(x)$, with the twist being undetectable from the Kummers.

This proves Theorem 5.7.4, apart from finding the correct twist; we don't deal with the twist here as it is well-known. Algorithm 4 summarises the above.

The file `richelot/derive_richelot_on_kummers_using_WT.m` in [Nic18] implements Algorithm 4 in MAGMA, and verifies all the calculations in this section.

Algorithm: Computing the Richelot isogeny on Kummer surfaces
Let W_1, W_2, W_3 be the W_T-matrices for $T = T_1, T_2, T_3$
Compute c_i such that $W_i^2 = c_i I$ for each $i = 1, 2, 3$
Let $L = K(\sqrt{c_1}, \sqrt{c_2}, \sqrt{c_3})$
Compute θ_1 such that $\theta_1^{-1} W_i \theta_1 = \Lambda_i$ is diagonal for each $i = 1, 2, 3$
Let s denote the map $(v_0, v_1, v_2, v_3) \mapsto (v_0^2, v_1^2, v_2^2, v_3^2)$
Compute $\eta = \theta_1^{-1} \xi$
Compute $\ell = s(\eta)$
Apply a linear transformation θ_2 so that $\theta_2(\ell^2)$ have leading terms
$\xi_1\xi_4, \xi_2\xi_4, \xi_3\xi_4, \xi_4\xi_4$
Compute the quartic equation of $\theta_2(\ell^2)$ using Algorithm 3 and using the quartic equation of ξ_i to reduce.
`/* It's important to use a quartic equation that is a quadratic in` ξ_3`, so we can't use the quartic equation that` ℓ_i `satisfy. */`
The map $\mathcal{K}_1 \to \mathcal{K}_2$ is $\xi \mapsto \ell = \theta_2 \circ s \circ \theta_1^{-1} \xi$.

Algorithm 4: The Richelot isogeny on Kummer surfaces.

5.7.5 The dual isogeny

Let $\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x)$ be a genus 2 curve admitting a Richelot isogeny, and let $\mathcal{C}'\colon y^2 = L_1(x)L_2(x)L_3(x)$ be the Richelot isogenous curve. Recall from Theorem 5.7.4 that

$$L_i(x) = [G_{i+1}(x), G_{i+2}(x)]/\Delta. \tag{5.65}$$

Both methods above describe the map $\mathcal{K} \to \mathcal{K}'$ induced by the Richelot isogeny $\varphi\colon \mathcal{J} \to \mathcal{J}'$.

The splitting $(L_1(x), L_2(x), L_3(x))$ now defines a Richelot isogeny from $\mathcal{J}'$. As is well-known classically, and computed in [CF96] and [Smi05], this gives an isogeny $\mathcal{J}' \to \mathcal{J}$, corresponding to the dual isogeny described in Section 5.3. The composition $\varphi' \circ \varphi$ is either $[2]$ or $[-2]$, depending on how we lift the map from the Kummer surfaces.

Proposition 5.7.13. *Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be a Richelot isogeny, and let φ' denote the dual Richelot isogeny. Then*

$$\ker \varphi' = \varphi(\mathcal{J}[2]). \tag{5.66}$$

Proof. If $T \in \mathcal{J}[2]$, then $\varphi'(\varphi(T)) = [2](T) = 0$, so $\varphi(T) \in \ker \varphi'$. This shows that $\varphi(\mathcal{J}[2]) \subseteq \ker \varphi'$. Also, $\varphi\colon \mathcal{J}[2] \to \ker \varphi'$ induces an isomorphism $\mathcal{J}[2]/\ker \varphi \to \varphi(\mathcal{J}[2])$. Since $\#\ker \varphi' = 4 = \#\mathcal{J}[2]/\#\ker \varphi = \#\varphi(\mathcal{J}[2])$, we have $\varphi(\mathcal{J}[2]) = \ker \varphi'$. □

5.7.6 Finding the correct twist

We can compute the twist for any specific curve by using Section 5.5. We just take any point on $\mathcal{J}$, map it through the Kummer surfaces to get its image on $\mathcal{K}'$, and then compute the required twist to lift it to a point on $\mathcal{J}'$. Since we already know the twist in general, this is straightforward.

5.8 The $(5,5)$-isogeny

5.8.1 $(5,5)$-subgroup

In [Fly15], Flynn finds an example of a dimension 2 Jacobian with nontrivial 5-part of Ш. He does this by carrying out descent via a $(5,5)$-isogeny. He first finds a one-parameter family of genus 2 curves $\mathcal{C}$ for which the Jacobian $\mathcal{J}(\mathcal{C})$ contains a copy of $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, rational as a set. Flynn's family consists of a single curve geometrically. In this section, we generalise Flynn's family to an infinite family of curves geometrically.

We construct this as follows, following Flynn (see [Fly15]). Let $\mathcal{C}\colon y^2 = f(x)$, where $f(x) = A_1(x)^2 + B_1(x)^5$, with $\deg A_1 \leq 2$ and $\deg B_1 = 1$. Let α be the root of $B_1(x)$. Then $y - A_1(x)$ meets the curve at $(\alpha, A_1(\alpha))$ with multiplicity 5. Since $\mathcal{C}$ is an odd degree curve, there is a single point at infinity, and so we have $\operatorname{div}(y - A_1(x)) = 5((\alpha, A_1(\alpha)) - \infty)$. We look to write $f(x)$ in two distinct ways so that we get two distinct copies of $\mathbb{Z}/5\mathbb{Z}$. We choose $B_1(x)$ to be rational, but allow solutions for $A_1(x)$ over a quadratic extension. This still ensures that the subgroup $\mathbb{Z}/5\mathbb{Z}$ is rational as a set. We can assume that $f(x)$ is monic with integer coefficients using the coprime degrees trick. We can further assume that $B_1(x) = x$ and $B_2(x) = x - 1$, as in Section 3.2.1. Thus we aim to solve $A_1(x)^2 + x^5 = A_2(x)^2 + (x-1)^5$ for some $A_1(x), A_2(x)$ defined over a possibly quadratic extension of $\mathbb{Q}$ and $d \in \mathbb{Q}^\times$. As in [Fly15], any twist of a solution also admits a $(5,5)$-isogeny.

We use the difference of squares method to write

$$(A_1 + A_2)(A_1 - A_2) = (x-1)^5 - x^5. \tag{5.67}$$

Let ζ_5 be a primitive fifth root of unity. The right hand side of (5.67) is an irreducible quartic over $\mathbb{Q}$ but splits over $\mathbb{Q}(\zeta_5)$. Over the quadratic subfield $\mathbb{Q}(\sqrt{5})$ of $\mathbb{Q}(\zeta_5)$, we have

$$(x-1)^5 - x^5 = -5(x^2 - x + \frac{1}{10}(5 - \sqrt{5}))(x^2 - x + \frac{1}{10}(5 + \sqrt{5})). \tag{5.68}$$

Let w_1 be the first term in parentheses in (5.68) and let w_2 be the second, so that $(A_1+A_2)(A_1-A_2) = -5w_1w_2$. Let $u \in \mathbb{Q}(\sqrt{5})^\times$ and define $A_1+A_2 = -5uw_1, A_1-A_2 = \frac{1}{u}w_2$. Solving for A_1, A_2 gives

$$A_1 = \frac{1}{2}(-5u + \frac{1}{u})x^2 + \frac{1}{2}(5u - \frac{1}{u})x + \frac{1}{4}((\sqrt{5}-5)u + \frac{1}{5}(\sqrt{5}+5)\frac{1}{u}) \tag{5.69}$$

$$A_2 = \frac{1}{2}(-5u - \frac{1}{u})x^2 + \frac{1}{2}(5u + \frac{1}{u})x + \frac{1}{4}((\sqrt{5}-5)u - \frac{1}{5}(\sqrt{5}+5)\frac{1}{u}). \tag{5.70}$$

Let $\mathcal{C}_u$ denote the curve

$$\mathcal{C}_u \colon y^2 = A_1(x)^2 + x^5, \tag{5.71}$$

where $A_1(x)$ is defined in (5.69).

Proposition 5.8.1. *Let $u \in \mathbb{Q}(\sqrt{5})$, and define $A_1(x), A_2(x)$ as above. Then $A_1(x)^2$ and $A_2(x)^2$ are in $\mathbb{Q}[x]$ if and only if $u\bar{u} = \pm 1/5$.*

Proof. Let $\bar{\cdot}$ denote conjugation in $\mathbb{Q}(\sqrt{5})$. Let $A(x) \in K[x]$, where $K = \mathbb{Q}(\sqrt{\Delta})$ is a quadratic extension of $\mathbb{Q}$. Then $A^2 \in \mathbb{Q}[x]$ if and only if $A^2 = \bar{A}^2$, which holds if and only if $(A + \bar{A})(A - \bar{A}) = 0$. Thus $A^2 \in \mathbb{Q}[x]$ if and only if $A = \bar{A}$ or $A = -\bar{A}$. The first is equivalent to $A \in \mathbb{Q}[x]$ and the second is equivalent to $A \in \sqrt{\Delta} \cdot \mathbb{Q}[x]$. Given this, it is straightforward to show that if $u\bar{u} = \pm 1/5$ then $A_1(x)^2, A_2(x)^2 \in \mathbb{Q}[x]$. We are left to show necessity.

We now consider the coefficients of $A_1(x)$. There are two cases.

Case 1: the x^2 coefficient lies in $\mathbb{Q}$. This happens if and only if $A_{12} = \overline{A_{12}}$; that is, $-5u + \frac{1}{u} = -5\bar{u} + \frac{1}{\bar{u}}$. This is equivalent to $(\bar{u} - u)(5u\bar{u} + 1) = 0$. Hence we either have $u - \bar{u} = 0$ or $u\bar{u} = -1/5$. We only have to eliminate this first possibility. If $u \in \mathbb{Q}$, then the constant coefficient of $A_1(x)$ is $\sqrt{5}\left(u + \frac{1}{5u}\right) + \left(\frac{1}{u} - 5u\right)$. This is rational if and only if $u + \frac{1}{5u} = 0$, which is impossible for $u \in \mathbb{Q}$.

Case 2: the x^2 coefficient of $A_1(x)$ lies in $\sqrt{5} \cdot \mathbb{Q}$. This happens if and only if it changes sign under $\bar{\cdot}$. This is equivalent to

$$(u + \bar{u})\left(5 - \frac{1}{u\bar{u}}\right) = 0. \tag{5.72}$$

Hence either $u + \bar{u} = 0$ or $u\bar{u} = 1/5$. Again, we only have to eliminate $u + \bar{u} = 0$. If $u + \bar{u} = 0$, one can show that $A_0 + \overline{A_0} = 0$ only if $5u^2 + 1 = 0$. This is impossible over $\mathbb{Q}(\sqrt{5})$. □

We now investigate the $u \in \mathbb{Q}(\sqrt{5})^\times$ that satisfy $\mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(u) = \pm 1/5$. Since $\mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\sqrt{5}) = -5$ and $\mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}((1+\sqrt{5})/2) = -1$, we have $u = \frac{\beta}{\sqrt{5}}$ or $u = \frac{1+\sqrt{5}}{2}\frac{\beta}{\sqrt{5}}$ for some β of norm 1; that is $\beta \in \ker \mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$.

I am grateful to the external examiner, Tom Fisher, for suggesting the following method to compute $\ker \mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$, which gives considerably more curves than I originally found.

Lemma 5.8.2. *Let L/K be a finite cyclic extension of fields. Then*

$$\ker \mathrm{Norm}_{L/K} = \{\sigma(\alpha)/\alpha \colon \alpha \in L^\times, \sigma \in \mathrm{Gal}(L/K)\}. \tag{5.73}$$

Proof. By definition, L/K is a finite Galois extension with $\mathrm{Gal}(L/K)$ a cyclic group, which we denote by G. Fix a generator σ of G and let n be the order of σ.

First note that $\mathrm{Norm}_{L/K}(\sigma(\alpha)/\alpha) = 1$, since

$$\mathrm{Norm}_{L/K}(\sigma(\alpha)/\alpha) = \prod_{i=0}^{n-1} \sigma^i(\sigma(\alpha)/\alpha) = \sigma^n(\alpha)/\alpha = 1, \tag{5.74}$$

since the product is telescoping, and $\sigma^n = 1$.

It remains to show that elements of $\ker \mathrm{Norm}_{L/K}$ are in the form $\sigma(\alpha)/\alpha$ for some $\alpha \in L^\times$. Suppose $\beta \in L^\times$ has $\mathrm{Norm}_{L/K}(\beta) = 1$.

Hilbert's Theorem 90 implies that $H^1(G, L^\times) = \{0\}$, so that every 1-cocycle is a 1-coboundary. Define the 1-cocycle ξ so that $\xi_\sigma = \beta$. The cocycle condition implies that $\xi_{\sigma^i} = \prod_{j=0}^{i-1} \sigma^j(\beta)$, so that ξ_σ determines ξ. To check that ξ is a 1-cocycle it suffices to verify that $\xi_{\sigma^i\sigma_j} = \xi_{\sigma^i} \cdot \sigma^i(\xi_{\sigma^j})$ for all i, j, which we do not write out explicitly.

Now ξ is a 1-cocycle so by Hilbert's Theorem 90 there is $\alpha \in L^\times$ such that $\xi_\tau = \tau(\alpha)/\alpha$ for all $\tau \in G$. This implies $\beta = \xi_\sigma = \sigma(\alpha)/\alpha$, which completes the proof. □

Thus the solutions $u \in \mathbb{Q}(\sqrt{5})^\times$ to $\mathrm{Norm}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(u) = -1/5$ are precisely $u = \frac{1}{\sqrt{5}}\frac{\bar{\gamma}}{\gamma}$ for $\gamma \in \mathbb{Q}(\sqrt{5})^\times$, where $\bar{\cdot}$ denotes the nontrivial automorphism of $\mathbb{Q}(\sqrt{5})$. Writing $\gamma = t + \sqrt{5}$, for $t \in \mathbb{Q}$, we find

$$u = \frac{1}{\sqrt{5}} \frac{t - \sqrt{5}}{t + \sqrt{5}} \tag{5.75}$$

is a solution for each $t \in \mathbb{Q}$.

Tom Fisher also pointed out that only even powers of u occur in the equation for $\mathcal{C}_u$, so defining

$$u^2 = \frac{1}{5} \cdot \frac{2t - 1 - \sqrt{5}}{2t - 1 + \sqrt{5}} \tag{5.76}$$

gives a more general family of curves, where u is now defined over $\mathbb{Q}(\sqrt{5}, t)(\sqrt{t^2 - t - 1})$. We then twist by $t^2 - t - 1$ to get u again defined over $\mathbb{Q}(\sqrt{5})(t)$. Note that the change to $2t - 1 - \sqrt{5}$ instead of $t - \sqrt{5}$ is to clear denominators later.

We record this in the following proposition.

Proposition 5.8.3. *Define*

$$A_1(x) = 5(x^2 - x) + t + 2 \tag{5.77}$$

$$A_2(x) = \sqrt{5}((2t-1)(x^2 - x) + t) \tag{5.78}$$

in $\mathbb{Q}(\sqrt{5})(t)$*. Then*

$$4(t^2 - t - 1)x^5 + A_1(x)^2 = 4(t^2 - t - 1)(x-1)^5 + A_2(x)^2. \tag{5.79}$$

Let $f(x) = 4(t^2 - t - 1)x^5 + A_1(x)^2$*. Then* $\mathcal{C}_t \colon y^2 = f(x)$ *defines a genus 2 curve over* $\mathbb{Q}$ *with a copy of* $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ *in the Jacobian over* $\mathbb{Q}(\sqrt{5})$*. The subgroup is a* $(5,5)$*-subgroup and is* $\mathbb{Q}$*-rational as a set.*

Proof. Let Σ be the group generated by the two independent order 5 points. It only remains to show that Σ is a $(5,5)$-subgroup. Since $\Sigma \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$, it suffices to show that the Weil pairing restricts to the trivial pairing on Σ. Proposition 5.2.4 implies this, since Σ is defined over $\mathbb{Q}(\sqrt{5})$, which does not contain a primitive 5th root of unity. □

Remark 5.8.4. *The curve for a given* u *is a specialisation of the curve over* $\mathbb{Q}(\sqrt{5})(u)$*. Thus since one is geometrically simple, the generic curve is.*

Proposition 5.8.5. *There are infinitely many pairwise geometrically nonisomorphic curves among the* $\mathcal{C}_t$*.*

Proof. Consider the 1-parameter $\mathcal{C}_t$ in Proposition 5.8.3. We can compute the Igusa invariants of the hyperelliptic curve for general t (defined over $\mathbb{Q}(\sqrt{5})(t)$) using MAGMA. Now consider $(\alpha(t), \beta(t), \gamma(t)) = (I_4/I_2^2, I_6/I_2^3, I_{10}/I_2^5)$. MAGMA shows that $\alpha(t), \beta(t)$ and $\gamma(t)$ are all nontrivial rational functions of t, and so they define a rational map $\mathbb{A}^1 \to \mathbb{A}^3$. The map takes on infinitely many values and so the theory of Igusa invariants from Section 2.1.5 implies that the family contains infinitely many geometrically nonisomorphic curves. □

5.8.2 The $(5,5)$-isogeny

Let $\mathcal{J}_u$ be the Jacobian of the curve $\mathcal{C}_u$ in (5.71). Let Σ denote the copy of $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ that is rational as a set in $\mathcal{J}[5]$. The map $\mathcal{J} \mapsto \mathcal{J}/\Sigma$ induces a map on Kummer surfaces. It is given by quintic forms in the ξ_i that are invariant under translation by points in Σ.

5.8.3 Finding invariant functions for an (n, n)-subgroup

The first step in finding the isogenous curve for the $(2, 2)$-isogeny was to find functions on the Kummer that were invariant by the $(2, 2)$-subgroup. We now discuss this for an (n, n)-isogeny. Let $\mathcal{C}$ be a genus 2 curve with Jacobian $\mathcal{J}$ such that there is an (n, n)-subgroup $\Sigma \subseteq \mathcal{J}[n]$ isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Let T_1, T_2 be generators for Σ. The following method was used in [BFT14] and [Fly15] in the $(3, 3)$ and $(5, 5)$ cases respectively.

5.8.4 The biquadratic forms

Let $\xi_0, \xi_1, \xi_2, \xi_3$ be the Kummer coordinates for a genus 2 curve, as in Proposition 4.3.7. As for the $(2, 2)$-isogeny, we want to find functions η_{ij} that are homogeneous degree n combinations of the ξ_i, that are invariant under translation by Σ (functions of ξ_i are automatically invariant under the -1 map). In the $(2, 2)$ case we were able to spot these easily, but here we will describe a more reliable method using the biquadratic forms from [CF96].

Let $T \in \mathcal{J}[n]$. For any $i \in \{0, 1, 2, 3\}$, the function $\prod_{j=1}^{n} \xi_i(D + jT)$ is a degree n function in the Kummer coordinates that is invariant under translation by T. We can generalise this by allowing more general indices for the ξ_i. Let I be a vector in $\{0, 1, 2, 3\}^n$, with ith entry $I(i)$. We interpret the indices cyclically, so that $I(k) = I(k')$ whenever $k \equiv k' \pmod{n}$. Define the function $q_I(D, T)$ by

$$q_I(D, T) \coloneqq \prod_{j=1}^{n} \xi_{I(j)}(D + (j - 1)T). \tag{5.80}$$

Replacing D by $D+T$ takes the term $\xi_{I(j)}(D+(j-1)T)$ to $\xi_{I(j)}(D+jT)$ in the product. Recall from Section 5.7.3, that the Kummer coordinates ξ_i are projectively equal on linearly equivalent divisors. Thus if $D \in \mathcal{J}$, then there is a constant c, depending on

D, such that $\xi_i(D) = c\xi_i(D + nT)$ for each $i = 0, 1, 2, 3$. Thus

$$q_I(D+T,T) = \prod_{j=1}^{n} \xi_{I(j)}(D+jT) \tag{5.81}$$

$$= \left(\prod_{j=1}^{n-1} \xi_{I(j)}(D+jT)\right) \cdot \xi_{I(n)(D+nT)} \tag{5.82}$$

$$= c\xi_{I(0)}(D) \prod_{j=1}^{n-1} \xi_{I(j)}(D+jT) \tag{5.83}$$

$$= c\prod_{j=1}^{n} \xi_{I(j-1)}(D+(j-1)T) \tag{5.84}$$

$$= cq_{I'}(D,T), \tag{5.85}$$

where $I'(j) = I(j-1)$ for each $j = 1, \ldots, n$. The symmetric group S_n acts on $\{0,1,2,3\}^n$ naturally by permuting the entries of a vector: $\sigma \in S_n$ acts via $({}^{\sigma}I)(j) = I(\sigma(j))$. To get a function symmetric under translation by T, we take the sum of the q_I over the orbit of I under the cyclic subgroup $C_n \subset S_n$.

The only problem is that it's hard to compute $q_I(D,T)$ as defined, since it's hard to compute $\xi(D+jT)$ for an n-torsion point T. For this, we use the biquadratic forms derived by Cassels and Flynn in [CF96].

Proposition 5.8.6 ([CF96, Theorem 3.4.1])**.** *Let $A, B \in \mathcal{J}(K)$. There are polynomials B_{ij}, biquadratic in $\xi_p(A), \xi_q(B)$, such that*

$$(\xi_i(A+B)\xi_j(A-B) + \xi_i(A-B)\xi_j(A+B)) = (2B_{ij}(A,B)), \tag{5.86}$$

as projective matrices.

See [CF96, Theorem 3.4.1] for more details. Crucially, given any points $A, B \in \mathcal{J}$, we can compute $B_{ij}(A,B)$.

We rewrite $q_I(D,T)$ using just the biquadratic forms, addition by a point of order 2, and explicit expressions for multiples of the torsion point T. We split into two cases. If n is odd, then we can partition the integers $1, 2, \ldots, n$ modulo n into $\{0\}, \{1,-1\}, \ldots, \{(n-1)/2, (1-n)/2\}$. The function

$$\eta_I(D,T) \coloneqq \xi_{I(1)}(D) \prod_{j=1}^{(n-1)/2} B_{I(2j),I(2j+1)}(D, jT). \tag{5.87}$$

is a sum of terms of the form $q_I(D,T)$ Taking the sum over the orbit of C_n gives a function symmetric under translation by T.

If n is even, then we can partition $1, 2, \ldots, n$ modulo n into $\{0\}, \{1, -1\}, \ldots, \{n/2-1, 1-n/2\}, \{n/2\}$. The function

$$\eta_I(D,T) \coloneqq \xi_{I(1)}(D)\xi_{I(n)}(D+(n/2)T)\prod_{j=1}^{n/2-1} B_{I(2j)I(2j+1)}(D,jT) \tag{5.88}$$

is also a sum of terms of the form $q_I(D,T)$. The sum over the orbit of S_n is again symmetric under translation by T. Note that $\xi_{I(n)}(D+(n/2)T)$ is computable since $(n/2)T$ is a 2-torsion point.

Remark 5.8.7. *We can also take the orbit under S_n.*

Remark 5.8.8. *We can distinguish the two functions by whether the length of I is odd or even.*

Example 5.8.9. *If $n = 2$, we get $\eta_I(D,T) = \xi_{I(1)}(D)\xi_{I(2)}(D, D+T)$. Taking the sum over the orbit of C_2 gives the same functions as in the previous section. If $n = 3$, then we get $\xi_{I(1)}(D)B_{I(2)I(3)}(D,T)$. Suppose $I = (0,1,2)$. Then the orbit under S_3 is*

$$\begin{aligned}&\xi_0(D)B_{12}(D,T) + \xi_0(D)B_{21}(D,T) + \xi_1(D)B_{02}(D,T)\\ &\quad + \xi_1(D)B_{20}(D,T) + \xi_2(D)B_{13}(D,T) + \xi_2(D)B_{31}(D,T).\end{aligned} \tag{5.89}$$

If some of the elements of I had been the same, then there would be fewer terms in the sum.

We now illustrate this for our family of $(5,5)$ curves.

5.8.4.1 Quintics invariant under Σ

We now find the quintics $\ell_0, \ldots, \ell_3$ that are invariant under translation by points in Σ. Let $T_1, T_2 \in \mathcal{J}[5]$ generate Σ and write $\xi(T_1), \xi(T_2)$ for the Kummer coordinates.

Remark 5.8.10. *Flynn's method is to consider the functions*

$$q_{ijklm}(D) = \xi_i(D)B_{jk}(D,T)B_{lm}(D,2T). \tag{5.90}$$

We can compute $B_{ij}(D,T)$ using the Kummer coordinates of D and T. Let

$$\xi_{ijklm}(D) = \xi_i(D-2T)\xi_j(D-T)\xi_k(D)\xi_l(D+T)\xi_m(D+2T). \tag{5.91}$$

Then $q_{ijklm}(D)$ consists of four terms in the form $\xi_{ijklm}(D)$.

We repeat the following process for each of the generators $T = T_1, T = T_2$. We compute a set Λ of S_5-representatives for vectors $I \subset \{0,1,2,3\}^5$. For each $I \in \Lambda$, we compute the function $\eta_I(D,T)$ and take the sum over the orbit of I under S_5. Using MAGMA, we see that the functions $\sum_{\sigma \in S_5} \eta_{\sigma I}(D,T)$ over all $I \in \Lambda$ span a 12-dimensional space of functions invariant by T. We then take the intersection of these spaces for $T = T_1$ and $T = T_2$.

The intersection consists of quintics in ξ_i that are invariant under translation by both T_1 and T_2. The expected dimension of the space of such quintics is 4, which MAGMA verifies is the dimension of our subspace. Thus we have found all such functions.

5.8.4.2 The isogenous curve

Let $\ell_0, \ldots, \ell_3$ denote a basis for the space of quintics that we just found. These are invariant under translation by T_1 and T_2. At this point we have defined the isogeny on the Kummer surfaces. We now want to find the relations between the ℓ_i. This will give us the equation satisfied by the Kummer surface of $\mathcal{J}/\Sigma$, and will let us determine the curve $\mathcal{C}'$ such that $\mathcal{J}/\Sigma = \mathcal{J}(\mathcal{C}')$.

I found it infeasible to use the power series method described in the previous section. This worked with the $(2,2)$-isogeny, but working with quintics is too computationally expensive. I first specialised the ℓ_i to specific curves u_n and computed the equations satisfied by the specialised ℓ_i, which was computationally possible. Flynn suggested trying to find the equation satisfied by the ℓ_i using interpolation. Based on the specialised equations it seemed likely the equation is of the form

$$\ell_3^2(\ell_1^2 - 4\ell_0\ell_2) + \ell_3\Phi(\ell_0,\ell_1,\ell_2) + \Psi(\ell_0,\ell_1,\ell_2), \tag{5.92}$$

where the coefficients of the cubic Φ and the quartic Ψ are rational functions in u of degree at most 4 in the numerator and 2 in the denominator. To start, we restrict to functions where the denominator equals u^2. Multiplying through by u^2, we try to solve the following equation

$$u^2\ell_3^2(\ell_1^2 - 4\ell_0\ell_2) + \ell_3\Phi(\ell_0,\ell_1,\ell_2) + \Psi(\ell_0,\ell_1,\ell_2), \tag{5.93}$$

where the coefficients of Φ, Ψ are polynomials of degree at most 4 in u.

We consider the subspace of quartics in $\ell_0, \ell_1, \ell_2, \ell_3$ generated by

$$\Lambda = \{\ell_3^2(\ell_1^2 - 4\ell_0\ell_2)\} \cup \{\ell_3\ell_0^i\ell_1^j\ell_2^k \colon i+j+k = 3\} \cup \{\ell_0^i\ell_1^j\ell_2^k \colon i+j+k = 4\}. \tag{5.94}$$

For many fixed choices $u_0 \in \mathbb{Q}$ of u, we compute the space of quartics in $\ell_0, \ell_1, \ell_2, \ell_3$ specialised to u_0. We only use u_0 if this space has dimension 1 when using the basis Λ. This gives us many quartics $Q_1, \ldots, Q_r \in \mathbb{Q}(\sqrt{5})[\ell_0, \ell_1, \ell_2, \ell_3]$, each giving conditions on the coefficients of the general quartic. We can then interpolate these conditions to get the general quartic $Q(u) \in \mathbb{Q}(\sqrt{5})(u)[\ell_0, \ell_1, \ell_2, \ell_3]$.

Finally, we can check that the ℓ_i actually satisfy this general quartic equation by substituting in $\ell_0, \ell_1, \ell_2, \ell_3$ and then reducing using the original Kummer equation. Then we linearly transform the ℓ_i so that the quartic equation doesn't contain the monomials $\ell_0\ell_1^2\ell_3, \ell_1^3\ell_3$ and $\ell_1^2\ell_2\ell_3$ monomials. This lets us read off the curve from the Kummer equation, up to twist, as in Section 5.4.1. After moving its Weierstrass point to infinity, we get the degree 5 form

$$\begin{aligned} &-x^5 + \left((10\sqrt{5} - 25)u^2 + \frac{-2\sqrt{5} - 5}{5u^2}\right)x^4 - 8x^3 + \left(-8u^2 - \frac{8}{25u^2}\right)x^2 \\ &- \frac{16}{5}x + \left(\frac{-32\sqrt{5} - 80}{25}u^2 + \frac{32\sqrt{5} - 80}{625u^2}\right) \end{aligned} \tag{5.95}$$

We give the code to verify this in `five_five/five_five_interpolation.m` in [Nic18].

Finding the correct twist The following method was suggested by Flynn to find the correct twist. We take a point $D \in \mathcal{J}(\mathbb{Q}(\sqrt{5})(u))$, compute its Kummer coordinates and then compute its image under the $(5,5)$-isogeny. This gives us Kummer coordinates $(\ell_0, \ell_1, \ell_2, \ell_3) \in \tilde{\mathcal{K}}$. To check if this lifts to a point on $\mathcal{J}'(\mathbb{Q}(\sqrt{5})(u))$, we just have to check if a_9^2 is a square in $\mathbb{Q}(\sqrt{5})(u)$, as in Section 5.5.

Let $K = \mathbb{Q}(\sqrt{5})$. We need to take a point outside the kernel of φ to get a meaningful condition. Since it's hard to find a rational point that works for all u, we actually just choose an arbitrary x-coordinate, $x_0 \in K$, and then twist so that $(x_0, y_0) - \infty$ is rational on $y^2 = df(x)$. We take $D = (1/2, f(1/2)) - \infty$. We have to twist $\mathcal{C}$ by $d = f(1/2)$ to ensure that $D \in \mathcal{J}(K(u))$. We then map this through the $(5,5)$-isogeny on the Kummer and see what twist d' is required on $\mathcal{C}'$ to get a rational lift. Then d/d' is the required twist of $\mathcal{C}'$. We find d/d' is already square, so that we already have the correct twist. Then we rewrite $\mathcal{C}'$ in degree 5 form, to get the above.

We have written $\mathcal{C}'$ in degree 5 form, but we now want to write it in the same form as $\mathcal{C}$, in order to derive the dual isogeny. We can do this by looking for scalars s such that $g(x) - (x - s)^5$ is square, where $g(x)$ is the equation of $\mathcal{C}'$. Flynn suggests

computing the discriminant of $g(x)-(x-s)^5$ as a function of s and finding the roots, since this forces repeated roots. We find that $g(x)-(x-s)^5$ is square with $s=\pm 2/\sqrt{5}$. This shows the following.

Proposition 5.8.11. *Let $u \in \mathbb{Q}(\sqrt{5})$ satisfy $u\bar{u} = \pm 1/5$. Then the curve $y^2 = f(x)$, where $f(x) = A_1(x)^2 + x^5 = A_2(x)^2 + (x-1)^5$, where $A_1(x), A_2(x)$ are as in (5.69) and (5.70), has subgroup $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \subset \mathcal{J}[5](\overline{\mathbb{Q}})$ and is rational as a set. Let*

$$C_1 = x^2 + \frac{(\frac{1}{25}(8\sqrt{5}+20)u^2 + \frac{4}{125}\sqrt{5})}{u^2 + \frac{1}{5}(\sqrt{5}+2)}, \tag{5.96}$$

$$C_2 = x^2 + \frac{(\frac{1}{25}(8\sqrt{5}+20)u^2 - \frac{4}{125}\sqrt{5})}{u^2 - \frac{1}{5}(\sqrt{5}+2)}, \tag{5.97}$$

$$\lambda_1' = (10\sqrt{5}-25)u^2 - 2\sqrt{5} - \frac{5+2\sqrt{5}}{5u^2}, \tag{5.98}$$

$$\lambda_2' = (10\sqrt{5}-25)u^2 + 2\sqrt{5} - \frac{5+2\sqrt{5}}{5u^2}, \tag{5.99}$$

$$s_1' = 2/\sqrt{5}, \tag{5.100}$$

$$s_2' = -2/\sqrt{5}. \tag{5.101}$$

Then $\mathcal{J}/\Sigma$ is the Jacobian of the curve $\mathcal{C}'\colon y^2 = g(x)$, where

$$g(x) = \lambda_1' C_1(x)^2 - (x-s_1')^5 = \lambda_2' C_2(x)^2 - (x-s_2')^5. \tag{5.102}$$

Remark 5.8.12. *Making the same substitution for u^2 in terms of t as in Proposition 5.8.3, and then twisting by t^2-t-1, we derive the isogenous curves for that family.*

The kernel $\mathcal{J}[\varphi]$ is generated by

$$T_1 = (0, A_1(0)) - \infty \tag{5.103}$$

$$T_2 = (1, A_2(1)) - \infty. \tag{5.104}$$

The kernel $\mathcal{J}'[\varphi']$ is generated by

$$T_1' = \left[\left(\frac{2}{\sqrt{5}}, \sqrt{\lambda_1'} C_1\left(\frac{2}{\sqrt{5}}\right)\right) - \infty\right] \tag{5.105}$$

$$T_2' = \left[\left(\frac{-2}{\sqrt{5}}, \sqrt{\lambda_2'} C_2\left(-\frac{2}{\sqrt{5}}\right)\right) - \infty\right]. \tag{5.106}$$

Let K_1, K_2 denote the fields of definition of T_1, T_2, respectively, and let K_1', K_2' denote the fields of definition of T_1', T_2', respectively. One of K_1, K_2 equals $\mathbb{Q}$ and the other equals $\mathbb{Q}(\sqrt{5})$. The fields K_1', K_2' both equal $\mathbb{Q}(\zeta_5)$, since λ_1', λ_2' are both square in $\mathbb{Q}(\zeta_5)(u)$. We can also see this by using the Weil pairing.

5.9 The $(4,4)$-isogeny

Smith studies compositions of Richelot isogenies over finite fields using correspondences ([Smi05]). In this section, we find a family of genus 2 curves whose Jacobians admit a $(4,4)$-isogeny whose kernel is completely defined over $\mathbb{Q}$. We use the theory from Section 5.7 instead of correspondences.

Let $\Sigma \subset \mathcal{J}_1[4]$ be a $(4,4)$-subgroup. Then $\psi\colon \mathcal{J}_1 \to \mathcal{J}_1/\Sigma$ is a $(4,4)$-isogeny. As before, $\mathcal{J}_1/\Sigma$ is a principally polarised abelian variety of dimension 2. Since Jacobians of curves are dense in the space of such abelian varieties, we expect that $\mathcal{J}_1/\Sigma$ is the Jacobian of a curve.

Smith shows in [Smi05] that ψ is a composition of two Richelot isogenies. Firstly, $2\Sigma \subseteq \mathcal{J}_1[2]$ is maximally isotropic under the 2-Weil pairing, so $\varphi_1\colon \mathcal{J}_1 \to \mathcal{J}_1/2\Sigma$ is a Richelot isogeny. Let $\mathcal{J}_2 = \mathcal{J}_1/2\Sigma$ be a Jacobian isomorphic to $\mathcal{J}_1/2\Sigma$. The quotient $\varphi_2\colon \mathcal{J}_2 \to \mathcal{J}_2/(\Sigma/2\Sigma)$ is also a Richelot isogeny. Let $\mathcal{J}_3$ be a Jacobian isomorphic to $\mathcal{J}_2/(\Sigma/2\Sigma)$. Then $\mathcal{J}_3$ is isomorphic to $\mathcal{J}_1/\Sigma$ and so ψ is the composition of the two Richelot isogenies $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$. Thus $(4,4)$-isogenies are compositions of certain Richelot isogenies.

But compositions of Richelot isogenies need not be $(4,4)$-isogenies. Smith analyses this in his thesis, and shows that $\ker\varphi_2 \cap \varphi_1(\mathcal{J}_1[2])$ classifies the composition. The $(4,4)$-isogeny is where $\ker\varphi_2 \cap \varphi_1(\mathcal{J}_1[2]) = \{0\}$. We record this in the proposition below, whose statement is equivalent to results in [Smi05].

Proposition 5.9.1. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a composition of Richelot isogenies. Let $\Sigma = \ker\varphi_2\varphi_1$, and let φ_1' denote the dual Richelot isogeny of φ_1. Then*

(i) $\ker\varphi_2 = \varphi_1(\Sigma)$;

(ii) $\ker\varphi_1' = \varphi_1(\mathcal{J}_1[2])$.

The composition $\varphi_2 \circ \varphi_1$ is a $(4,4)$-isogeny if and only if $\ker\varphi_2 \cap \varphi_1(\mathcal{J}_1[2]) = \{0\}$.

Proof. Note that $\varphi_1(\Sigma) \subseteq \ker\varphi_2$. Also, $\ker\varphi_1 \subset \Sigma$, so $\Sigma/\ker\varphi_1 \cong \varphi_1(\Sigma)$. This shows that $\#\varphi_1(\Sigma) = \#\Sigma/\#\ker\varphi_1 = 4$. Thus $\varphi_1(\Sigma) = \ker\varphi_2$, as they are both order 4. This shows (i). Proposition 5.7.13 shows (ii).

Suppose now that $\varphi_2 \circ \varphi_1$ is a $(4,4)$-isogeny. Let $\Sigma = \ker(\varphi_2 \circ \varphi_1)$; this is a $(4,4)$-subgroup. Since $\ker\varphi_1 \subseteq \Sigma \cap \mathcal{J}_1[2] = 2\Sigma$, we conclude $\ker\varphi_1 = 2\Sigma$.

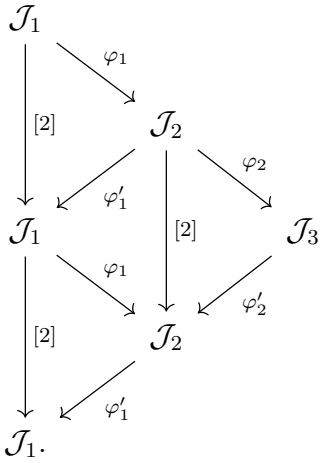
We now show that $\ker\varphi_1' \cap \ker\varphi_2 = \{0\}$. Let $D \in \ker\varphi_1' \cap \ker\varphi_2$. By (i) and (ii), there exists $E \in \Sigma$ and $T \in \mathcal{J}_1[2]$ such that $D = \varphi_1(E) = \varphi_1(T)$. Thus $T - E \in$

$\ker \varphi_1 = 2\Sigma$. Since $E \in \Sigma$, we see that $T \in \Sigma \cap \mathcal{J}_1[2] = 2\Sigma = \ker \varphi_1$. Hence $D = \varphi_1(T) = 0$.

Conversely, suppose $\ker \varphi_2 \cap \varphi_1(\mathcal{J}_1[2]) = \{0\}$. Then let $\Sigma := \varphi_1^{-1}(\ker \varphi_2)$. Then $\#\Sigma = (\deg \varphi_1) \cdot \#\ker \varphi_2 = 16$. Also, if $D \in \Sigma$ then $\varphi_1(D) \in \ker \varphi_2 \subset \mathcal{J}_2[2]$, so that $2D \in \ker \varphi_1$.

Note also that $\Sigma \cap \mathcal{J}_1[2] = \ker \varphi_1$. For, if $D \in \Sigma \cap \mathcal{J}_1[2]$, then $\varphi_1(D) \in \ker \varphi_2 \cap \varphi_1(\mathcal{J}_1[2]) = \{0\}$. Hence $\Sigma \subset \mathcal{J}_1[4]$ and $\Sigma \cap \mathcal{J}_1[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This implies that $\Sigma \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (over $\overline{K}$). □

If $\varphi_2 \circ \varphi_1$ is a $(4,4)$-isogeny, then the isogenies and their duals fit into the following commutative diagram.



(5.107)

5.9.1 A family of curves admitting a $(4,4)$-isogeny

We now give a necessary condition for the Jacobian of a genus 2 curve to have a $(4,4)$-isogeny with kernel completely defined over K. Smith gives a similar condition in his thesis ([Smi05]).

Proposition 5.9.2. *Let $\mathcal{C}_1 \colon y^2 = f(x)$ be a genus 2 curve over a number field K and let $\mathcal{J}_1$ be its Jacobian. Suppose that $\mathcal{J}_1$ admits a $(4,4)$-isogeny φ with kernel Σ completely defined over K. Then $\mathcal{J}_1$ is the image under a Richelot isogeny $\mathcal{J}_2 \to \mathcal{J}_1$ of a Jacobian $\mathcal{J}_2$ such that $\mathcal{J}_2[2](K) \cong (\mathbb{Z}/2\mathbb{Z})^4$.*

Proof. We have seen that $\mathcal{J}_1$ admits a $(4,4)$-isogeny if and only if $\mathcal{J}_1$ admits a Richelot isogeny $\varphi_1 \colon \mathcal{J}_1 \to \mathcal{J}_2$ such that $\mathcal{J}_2$ admits a second Richelot isogeny $\varphi_2 \colon \mathcal{J}_2 \to \mathcal{J}_3$ with $\ker \varphi_2 \cap \varphi_1(\mathcal{J}_1[2]) = \{0\}$. Thus it is necessary that there is a Richelot isogeny $\varphi_1 \colon \mathcal{J}_1 \to \mathcal{J}_2$.

Let $\Sigma = \langle T_1, T_2 \rangle$ be the kernel of the $(4,4)$-isogeny from $\mathcal{J}_1$. Then $\ker \varphi_1 = \langle 2T_1, 2T_2 \rangle$ is also completely defined over K. The kernel of the dual isogeny, $\ker \varphi_1'$, is also completely defined over K.

Proposition 5.9.1 implies that $\ker \varphi_2 = \langle \varphi_1(T_1), \varphi_1(T_2) \rangle$, which is thus also defined completely over K. Moreover, since φ is a $(4,4)$-isogeny, $\ker \varphi_1' \cap \ker \varphi_2 = \{0\}$, which implies that $\mathcal{J}_2[2] = \ker \varphi_1' \oplus \ker \varphi_2$. Since both summands are completely defined over K, the 2-torsion $\mathcal{J}_2[2]$ is also completely defined over K. □

The condition $\mathcal{J}_2[2](K) = \mathcal{J}_2[2](\overline{K})$ is equivalent to saying $\mathcal{J}_2$ is the Jacobian of a hyperelliptic curve $y^2 = G_1(x)G_2(x)G_3(x)$, where $(G_1(x), G_2(x), G_3(x))$ is a Richelot splitting of a degree 5 or 6 polynomial, such that each $G_i(x)$ splits completely over K. Then $\mathcal{J}_1$ is the image under the Richelot isogeny corresponding to $(G_1(x), G_2(x), G_3(x))$, so is the Jacobian of the curve $y^2 = f(x) = L_1(x)L_2(x)L_3(x)$, where $L_i(x)$ are defined as in the Richelot isogeny (Theorem 5.7.4).

Using standard transformations of genus 2 curves, we can assume that $\infty, 0, 1$ are Weierstrass points of the curve $\mathcal{C}_2$. That is, $\mathcal{C}_2 \colon y^2 = dx(x-1)(x-a)(x-b)(x-c)$ for some a, b, c, d. Indeed, since we assume the curve splits, we can transform so that one of the roots is 0, and then use the flip map $(x, y) \mapsto (1/x, y/x^3)$ to get a degree 5 polynomial. Then we can move two of the roots of $f(x)$ to 0, 1.

The possible Richelot isogenies from $\mathcal{J}_2$ are then in bijection with the classes of quadratic splittings of $x(x-1)(x-a)(x-b)(x-c)$. Writing ∞ for the Weierstrass point at infinity, the quadratic splittings are in bijection with partitions of $0, 1, a, b, c, \infty$ into three sets of size 2. There are 15 such partitions. A choice of two partitions determines two Richelot isogenies $\mathcal{J}_1 \xleftarrow{\varphi_1'} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$. The composition $\varphi_2 \circ \varphi_1 \colon \mathcal{J}_1 \to \mathcal{J}_3$ is a $(4,4)$-isogeny precisely when $\ker \varphi_1' \cap \ker \varphi_2 = \{0\}$.

For each choice of $\ker \varphi_1'$, there are 8 available Richelot isogenies φ_2 with this property: 1 partition has exactly three sets in common with the original partition; 6 partitions have exactly one set in common with the original partition (choose which of the three sets, then pair the other two sets differently – two ways each). Thus there are 15 - 7 = 8 partitions with zero sets in common with the original partition.

Remark 5.9.3. *Each quadratic splitting corresponds to two Richelot isogenies in the sense of [Smi05], since we can compose with* $[-1]$ *to get another isogeny with the same kernel.*

Example 5.9.4. *Let* $\mathcal{C}_2$ *be the hyperelliptic curve* $y^2 = x(x-1)(x-a)(x-b)(x-c)$. *Let* $\varphi_1' \colon \mathcal{J}_2 \to \mathcal{J}_1$ *be the Richelot isogeny via the splitting* $(x, (x-1)(x-a), (x-b)(x-c))$.

Thus $\mathcal{J}_1$ is the Jacobian of the curve $\mathcal{C}_1\colon y^2 = L_1(x)L_2(x)L_3(x)$, where

$$L_1(x) = \frac{(-a+b+c-1)x^2 + (2a-2bc)x + abc - ab - ac + bc}{a-bc}, \tag{5.108}$$

$$L_2(x) = \frac{-x^2+bc}{a-bc}, \tag{5.109}$$

$$L_3(x) = \frac{x^2-a}{a-bc}. \tag{5.110}$$

Taking the Richelot isogeny via $\Sigma_2 \coloneqq ((x-1),(x-a)(x-b),x(x-c))$ gives the map $\mathcal{J}_2 \to \mathcal{J}_3$. Here $\mathcal{J}_3$ is the Jacobian of $\mathcal{C}_3\colon y^2 = H_1(x)H_2(x)H_3(x)$, where

$$H_1(x) = \frac{(-a-b+c)x^2 + 2abx - abc}{ab-a-b+c}, \tag{5.111}$$

$$H_2(x) = \frac{-x^2+2x-c}{ab-a-b+c}, \tag{5.112}$$

$$H_3(x) = \frac{x^2-2x-ab+a+b}{ab-a-b+c}. \tag{5.113}$$

Hence $\mathcal{J}_1$ admits the $(4,4)$-isogeny $\mathcal{J}_1 \to \mathcal{J}_2 \to \mathcal{J}_3$ where φ_1 is given by the Richelot isogeny corresponding to $(L_1(x), L_2(x), L_3(x))$ and φ_2 is given by the Richelot isogeny corresponding to Σ_2.

5.9.2 Computing 4-torsion points that double to 2-torsion points

Let $\mathcal{C}_1$ be the curve in Example 5.9.4, and let Σ be the kernel of the $(4,4)$-isogeny. Then Σ is K-rational as a set, but the individual points in Σ need not be defined over K. In this section we show how to compute the 4-torsion points that double to a given 2-torsion point on the Jacobian of a genus 2 curve. We use this in Section 5.9.3 to find conditions under which the invidual points in Σ are defined over K.

Let $\mathcal{J}$ be the Jacobian of a genus 2 curve $\mathcal{C}$. Suppose D is a 4-torsion point on $\mathcal{J}$ such that $[2](D) = T$. Let $\boldsymbol{v} \in \mathbb{A}^4$ be a vector representing the Kummer coordinates $\xi(D)$. Lemma 5.7.11 implies that $\boldsymbol{v}$ is an eigenvector for W_T. After a quadratic extension by $\sqrt{c_T}$, the minimal polynomial of W_T splits, so W_T is diagonalisable over $K(\sqrt{c_T})$. Let Λ_1, Λ_2 be the eigenspaces for W_T, one for each eigenvalue $\sqrt{c_T}, -\sqrt{c_T}$.

We now solve for the eigenvectors that lie on the Kummer surface. Let $\mathbf{v}_1, \mathbf{v}_2$ be a basis for one of the eigenspaces. Then $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2$ lies on the Kummer surface if and only if it satisfies the Kummer equation $Q(z_0, z_1, z_2, z_3)$ (see Theorem 4.3.7). This gives a homogeneous quartic equation in α_1, α_2:

$$Q(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2) = 0. \tag{5.114}$$

Each of the four solutions to the quartic (over $\overline{K}$) gives an eigenvector whose image in projective space lies on the Kummer surface; there are two points on the Jacobian $\mathcal{J}$ above each point, which gives eight 4-torsion points doubling to a given T from one eigenspace. Doing this for both eigenspaces thus gives the 16 4-torsion points D such that $[2](D) = T$.

Algorithm 5 expresses this formally as an algorithm.

Algorithm: Computing four torsion points that double to a K-rational 2-torsion point

Data: Input: f of degree 5 or 6, defined over a field K with a quadratic factor $q(x)$ over K; this factor can be linear if $\deg f = 5$.

Result: Points D in $\mathcal{J}[4](\overline{K})$ such that $[2](D) = T$, where T is the 2-torsion point corresponding to $q(x) = 0$. Here $\mathcal{J}$ is the Jacobian of $y^2 = f(x)$

`FourTorsion`

Compute W, the translation by T matrix

Adjoin a root of its minimal polynomial $x^2 - c$

Compute M such that $MWM^{-1} = \Lambda$ is diagonal

`/* Solve for a solution on the Kummer in each eigenspace. Each eigenspace is dimension 2, generated by` u, v`, say */`

Solve for $Q(\alpha_1 \mathbf{u} + \alpha_2 \mathbf{v}) = 0$, where Q is the Kummer equation of $\mathcal{K}$

`/* Lift each solution on the Kummer to the Jacobian */`

For each $(\xi_0 \cdots \xi_3)$ on the Kummer, adjoin a square root of a_9^2

Then return the points on the Jacobian with these coordinates

end

Algorithm 5: Computing $D \in \mathcal{J}[4]$ such that $2D = T$

5.9.3 A rational $(4, 4)$-kernel

We can now apply this theory to the family from Example 5.9.4. We want to find a curve in the family that admits a $(4, 4)$-subgroup all of whose elements are K-rational. Let T_1, T_2, T_3 be the nontrivial 2-torsion points in the kernel Σ of the Richelot isogeny $\mathcal{J}_1 \to \mathcal{J}_2$. We can show for curves in the family, the minimal polynomials of W_1, W_2, W_3 split in K, and thus the matrices are diagonalisable over K. Moreover, for curves in the family, the homogeneous quartics in α_1, α_2 for each eigenspace of each W_i (from Equation (5.114)) split into quadratics. More precisely, let E_{ij} denote the jth eigenspace of W_i, for $i = 1, 2, 3$ and $j = 1, 2$. Let $\mathbf{v}_1, \mathbf{v}_2$ be a basis for E_{ij}. That is, we have

$$Q(\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2) = U_{ij1}(\alpha_1, \alpha_2) U_{ij2}(\alpha_1, \alpha_2), \tag{5.115}$$

where each U_{ijk} is a homogeneous quadratic in α_1, α_2. These quadratics are important, because if $\mathbf{v}$ is an eigenvector that satisfies the Kummer equation, then it lies in one

i	$\mathrm{disc}(u_{i1})$	$\mathrm{disc}(u_{i2})$	$\mathrm{disc}(u_{i3})$	$\mathrm{disc}(u_{i4})$
1	b	ac	c	ab
2	$(1-b)(a-b)$	$a(1-c)(a-c)$	$(1-c)(a-c)$	$a(1-b)(a-b)$
3	$(a-c)(a-b)$	$bc(1-b)(1-c)$	$(1-b)(1-c)$	$bc(a-b)(a-c)$

Table 5.1: The discriminants of the quadratic factors for the eigenspaces.

of the eigenspaces E_{ij} and thus equals $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2$ for some α_1, α_2 that are a root of one of the U_{ijk}.

We are interested in when the eigenvector is defined over K, and so we are interested in the roots of the U_{ijk}. Let D_1, D_2 be the 4-torsion points in the $(4,4)$-subgroup Σ such that $[2](D_i) = T_i$ for each $i = 1, 2$, and let $D_3 = D_1 + D_2$. In order that D_i has rational coordinates on the Kummer surface, it must be that one of the U_{ijk} has a rational root (for some j, k). Such a rational root exists if and only if the discriminant of U_{ijk} is a square, which is what we now examine.

In the following we group the two eigenspaces for each W_i together, and consider the roots of all four quadratics U_{ijk} for each i. To simplify notation, we now relabel these. Let $u_{ij}(\alpha_1, \alpha_2)$ denote the four quadratics for the eigenspaces of W_i (with $j = 1, 2, 3, 4$).

Table 5.1 shows the discriminants of the quadratics. They are given in terms of the indeterminates a, b, c from Example 5.9.4. The ith row is for the quadratics for the eigenspaces of W_i.

The MAGMA file `four_four/four_four_classification.m` in [Nic18] verifies the discriminants in Table 5.1.

If D_1, D_2, D_3 are K-rational 4-torsion points such that D_1, D_2 generate a $(4,4)$-subgroup, then there is a choice of elements in the table above, one from each row, that are all square in K. This is because D_i is a 4-torsion point lying above the 2-torsion point T_i, and because W_i is the translation-by-T_i matrix.

Remark 5.9.5. *I am grateful to the examiners for suggesting that a more careful study of the eigenspaces from different W_i should make it possible to cut down the number of cases. This would be worth exploring in the future.*

We now find a family of genus 2 curves whose Jacobians have a $(4,4)$-kernel with all the elements defined over the ground field. First we consider a particular combination of discriminants being square, one from each row of Table 5.1. We then compute the 4-torsion points on the Kummer surface corresponding to the eigenvectors. Then we see which pairs of these 4-torsion points generate a $(4,4)$-kernel by mapping across

to the isogenous Kummer surface. Finally, we impose that the 4-torsion points are K-rational by imposing that their a_9^2 are equal modulo squares.

Proposition 5.9.6. *Let $s, t, v \in K$. Define*

$$u = \frac{-s^2(s^2 - t^4 + t^2)v^2 - 2(s^2 - t^4 + t^2)v - 1}{-s^2t(s^2 - t^4 + t^2)v^2 + t}, \tag{5.116}$$

and then define

$$(a, b, c) = \left(\frac{s^2 - t^4 + t^2}{1 - t^2}, \frac{s^2 - t^4 + t^2}{u^2s^2 + 1 - t^2}, t^2 \right). \tag{5.117}$$

Let

$$\begin{aligned} d_2 = &(s^2 - t^4 + t^2)(s^2u^2 + t^4 - 2t^2 + 1) \\ &\cdot (s^4u^2 - s^2t^2u^2 + s^2u^2 - t^6 + 3t^4 - 3t^2 + 1). \end{aligned} \tag{5.118}$$

Let $G_1(x) = x, G_2(x) = (x - 1)(x - a), G_3(x) = (x - b)(x - c)$. Let $f_1(x) = dL_1(x)L_2(x)L_3(x)$ be the isogenous curve via the Richelot isogeny corresponding to (G_1, G_2, G_3), where d is defined to make $f_1(x)$ monic. Let $f_2(x) = d_2dG_1(x)G_2(x)G_3(x)$. Then $\mathcal{C}_1 \colon y^2 = d_2f_1(x)$ admits a $(4, 4)$-isogeny with the kernel K-rational pointwise.

Proof. We try to impose that

$$c, (1 - c)(a - c), bc(a - b)(a - c) \tag{5.119}$$

are all square. This implies that each of W_1, W_2, W_3 has an eigenvector lying on the Kummer surface. If $\boldsymbol{v}$ is an eigenvector for W_T lying on the Kummer surface, then $\boldsymbol{v}$ are the Kummer coordinates of a 4-torsion point D such that $2D = T$. We then hope that we can lift these 4-torsion divisors to points on the Jacobian, and that they form a $(4, 4)$-kernel.

It is necessary that $c = t^2$ for some $t \in K$. Then we look for solutions to

$$(1 - t^2)(a - t^2) = s^2 \tag{5.120}$$

$$b(a - b)(a - t^2) = z^2. \tag{5.121}$$

Equation (5.120) determines a as

$$a = \frac{s^2 - t^4 + t^2}{1 - t^2}. \tag{5.122}$$

We are left to solve equation (5.121), which rearranges to a quadratic in b in terms of s, t, z

$$b^2 - b\left(\frac{s^2 - t^4 + t^2}{1 - t^2} \right) + \frac{z^2(1 - t^2)}{s^2} = 0. \tag{5.123}$$

This is a conic in b, z with the rational point $(0, 0)$. We can parametrise the conic as $(b, z) = (b_0/w_0, z_0/w_0)$, where

$$(b_0 \colon z_0 \colon w_0) = \left(\frac{-s^2 + t^4 - t^2}{s^2} \mu^2 \colon \frac{s^2 - t^4 + t^2}{1 - t^2} \lambda\mu \colon -\lambda^2 + \frac{t^2 - 1}{s^2} \mu^2 \right) \tag{5.124}$$

and $(\lambda \colon \mu) \in \mathbb{P}^1(K(s,t))$. The point $\mu = 0$ gives $b = 0$, which is a degenerate solution to the original equation. Thus we can set $\lambda = u, \mu = 1$, and find the general solution to (5.119) is

$$(a, b, c) = \left(\frac{s^2 - t^4 + t^2}{1 - t^2}, \frac{s^2 - t^4 + t^2}{u^2 s^2 + 1 - t^2}, t^2 \right), \tag{5.125}$$

where $s, t, u \in K$. We thus have a 3-parameter family such that each term in (5.119) is square.

We compute the points on the Kummer surface that are eigenvectors of one of W_1, W_2, W_3 by solving the homogeneous quartic equations for the eigenspaces. For each such $\xi(D)$, we compute the image under the Richelot isogeny using the explicit projective map. In this way we compute all pairs $\xi(D_1), \xi(D_2)$ such that their image on $\mathcal{K}_2$ corresponds to 2-torsion points in $\mathcal{J}_2$ that generates a second Richelot isogeny. In particular, the two points are distinct and have trivial Weil pairing. We require that the kernel $\ker \varphi_2$ of the second Richelot isogeny intersects trivially with the kernel $\ker \varphi_1'$.

This determines all pairs of points on the Kummer surface that are the images of generators of $(4, 4)$-kernels. We now impose that these lift to the Jacobian. This happens if and only if a_9^2 is square in $K(s, t, u)$ (using Section 5.5). We can actually impose that their a_9^2 are equal modulo squares, which means there is a twist of the curve for which both points lift to the Jacobian. The quotient of their a_9^2 equals one of

$$\Delta_1 = (1 - t^2)(s^2 - t^4 + t^2)(s^2 u^2 - s^2 + t^4 - 2t^2 + 1) \tag{5.126}$$

$$\Delta_2 = (s^2 - t^4 + t^2)(s^2 u^2 - t^2 + 1), \tag{5.127}$$

each occurring in 4 of the 8 pairs. The equation $\Delta_i = v_i^2$ is a conic in u, v_i. We can solve the second easily, since it has the point $(u, v_2) = (1/t, t(s^2 - t^4 + t^2))$. Parametrising the conic gives

$$u = \frac{-s^2(s^2 - t^4 + t^2)\lambda^2 - 2(s^2 - t^4 + t^2)\lambda\mu - \mu^2}{-s^2 t(s^2 - t^4 + t^2)\lambda^2 + t\mu^2}. \tag{5.128}$$

ijk	a	b	c
311	$\frac{b-b^2+s^2}{1-b}$	$\frac{-2su+t^2+u^2}{u^2+1}$	t^2
312	$\cdots$	$\frac{1}{u^2(1-t^2)+1}$	$\cdots$
313	$\cdots$	$\frac{1-t^2-u^2}{1-t^2}$	$\cdots$
314	$\cdots$	$u^2 = -b^3 + (t^2+1)b^2 + (s^2-t^2)b$	$\cdots$
321	$\frac{t^2}{(t^2-1)s^2+1}$	$a - \frac{u^2}{a-t^2}$	$\cdots$
322	$\cdots$	$\frac{1}{u^2(1-t^2)+1}$	$\cdots$
323	$\cdots$	$\frac{1-t^2-u^2}{1-t^2}$	$\cdots$
324	$\cdots$	$\frac{a}{u^2(a-t^2)+1}$	$\cdots$
331	$\frac{s^2+t^2-t^4}{1-t^2}$	$a - \frac{u^2}{a-t^2}$	$\cdots$
332	$\cdots$	$\frac{1}{u^2(1-t^2)+1}$	$\cdots$
333	$\cdots$	$\frac{1-t^2-u^2}{1-t^2}$	$\cdots$
334	$\cdots$	$\frac{a}{u^2(a-t^2)+1}$	$\cdots$
341	$\frac{t^2}{(b-1)s^2+1}$	$u^2 = (b-1)(b^2s^2 + (1-s^2)b - t^2)$	$\cdots$
342	$\frac{b}{s^2(b-1)+1}$	$\frac{1}{u^2(1-t^2)+1}$	$\cdots$
343	$\cdots$	$\frac{1-t^2-u^2}{1-t^2}$	$\cdots$
344	$\cdots$	$\frac{u^2(s^2t^2-1)^2+t^2-s^2t^2}{u^2(s^2t^2-1)^2-s^2t^2+1}$	$\cdots$

Table 5.2: The solutions to each condition Λ_{3jk}. An ellipsis means the solution is repeated from above.

The required twist is by $a_9^2(D_1)$, recalling that $a_9^2(D_1)$ and $a_9^2(D_2)$ are equal modulo squares. This can be taken as d_2 as stated in the Proposition. With a, b, c given as in (5.117) with $s, t \in K$ free and u in terms of λ, μ. But $\mu = 0$ implies $u = 1/t$ and then $b = c$, so we can replace $(\lambda\colon \mu)$ with the parameter $v = \lambda/\mu$. This gives the stated 3-parameter family admitting a $(4,4)$-isogeny with rational $(4,4)$-kernel over the twist by d_2. □

Remark 5.9.7. *We haven't yet been able to solve $\Delta_1 = v_1^2$ in general.*

5.9.4 Classifying $(4,4)$-kernels

We denote the condition that $\mathrm{disc}(u_{1i}), \mathrm{disc}(u_{2j}), \mathrm{disc}(u_{3k})$ (see Table 5.1) are all square by Λ_{ijk}. By permuting b and c we can assume that the condition from the first row is either that c is square or that ac is square. Thus we only need to solve Λ_{2jk} and Λ_{3jk} for all j, k.

Proposition 5.9.6 solved Λ_{334}, with the solution given in equation (5.117). We solve the other combinations similarly, and we give their solutions (where parametrisable) in Table 5.2 and Table 5.3.

ijk	a	b	c
211	$\frac{s^2+b-b^2}{1-b}$	$(t^2-1)b^2+(1-t^2)b-s^2t^2+s^2=u^2$	at^2
212	$\cdots$	$u^2=b(b-1)(b^2-b-s^2)(b^2t^2-bt^2-b-s^2t^2+1)$	$\cdots$
213	$\cdots$	$u^2=t^2b^2-(1+t^2)b-s^2t^2+1$	$\cdots$
214	$\cdots$	$\frac{1}{(1-t^2)u^2+1}$	$\cdots$
221	$\frac{t^4-t^2-s^2}{t^4-t^2}$	$\frac{a^2(1-t^2)-u^2}{a(1-t^2)}$	$\cdots$
222	$\cdots$	$\frac{1}{au^2(1-at^2)+1}$	$\cdots$
223	$\cdots$	$\frac{1-at^2-u^2}{1-at^2}$	$\cdots$
224	$\cdots$	$\frac{a}{(1-t^2)u^2+1}$	$\cdots$
231	$\frac{1}{u^2(t^4-t^6)+t^2}$	$\frac{a^2(1-t^2)-u^2}{a(1-t^2)}$	$\cdots$
232	$\cdots$	$\frac{1}{au^2(1-at^2)+1}$	$\cdots$
233	$\cdots$	$\frac{1-at^2-u^2}{1-at^2}$	$\cdots$
234	$\cdots$	$\frac{a}{(1-t^2)u^2+1}$	$\cdots$
241	$\frac{b}{(b-1)s^2+1}$	$\frac{1-t^2-u^2}{1-t^2}$	$\cdots$
242	$\cdots$	$\frac{u^2+s^2-1}{(s^2-t^2)^2u^2+(s^2-t^2)}$	$\cdots$
243	$\cdots$	$u^2=(1-b)(bs^2-s^2+1)(b(s^2-t^2)-s^2+1)$	$\cdots$
244	$\frac{b^2(1-t^2)+u^2}{b(1-t^2)}$	$\frac{u^2s^4(1-t^2)+s^2-1}{s^4(1-t^2)u^2+s^2}$;	$\cdots$

Table 5.3: The solutions to each condition Λ_{2jk}. An ellipsis means the solution is repeated from above.

More detail The condition Λ_{344} is an intersection of conics: $a(1-b)(a-b)=s^2, b(a-b)(a-t^2)=u^2$. The first equation determines a in terms of b, s. Substituting this into the second equation, and ignoring the degenerate solution $b=0$, gives another conic in b, which we can solve similarly.

The condition Λ_{341} is $c=t^2$, $a(1-b)(a-c)=s^2$ and $(a-c)(a-b)=u^2$. The solution to the second equation in a is $a=t^2/((b-1)s^2+1)$. Substituting this into the third equation gives (after removing square factors) $u^2=(b-1)(b^2s^2+b(1-s^2)-t^2)$.

The condition Λ_{241} is an intersection of conics: $a(1-b)(a-b)=s^2, a(a-b)(1-t^2)=u^2$ (once we substitute $c=at^2$). Multiplying the equations and removing square factors gives $(1-b)(1-t^2)=v^2$ for some v, which determines b as $b=\frac{1-t^2-v^2}{1-t^2}$. Then we determine a via the first equation.

For Λ_{243}, we first solve for a in $s^2=a(1-b)(a-b)$ to get $a=b/((b-1)s^2+1)$. Then substitute into $(1-b)(1-at^2)=u^2$ to get the elliptic curve in b, u. Λ_{244} is an intersection of conics: $a(1-b)(a-b)=s^2, a^2t^2b(a-b)(1-t^2)=u^2$ (once we substitute $c=at^2$). Solving $b(a-b)(1-t^2)=u^2$ gives $a=b+\frac{u^2}{b(1-t^2)}$, and substituting into the first equation gives $u^2+b^2(1-t^2))=s^2$ (after removing square factors). Thus $b=\frac{2us}{s^2+t^2-1}$.

We haven't given the general solution for $\Lambda_{314}, \Lambda_{341}, \Lambda_{211}, \Lambda_{212}, \Lambda_{213}, \Lambda_{243}$, but give

a single curve for each that parametrises the solutions. Note that Λ_{314} and Λ_{341} have the same elliptic curve, which suggests we may be able to reduce the number of cases.

Classification For each Λ_{ijk} we have either completely described the space of solutions, or have given the moduli space of genus 2 curves that admit a $(4,4)$-isogeny that have two distinct 4-torsion points whose images on the Kummer surface are K-rational. But the distinct 4-torsion points on the Kummer surface need not be the generators for the $(4,4)$-isogeny. To find a $(4,4)$-isogeny whose kernel is elementwise K-rational on the Jacobian, we further require that the 4-torsion points lift to the Jacobian over the same quadratic extension and also that their 4-Weil pairing is trivial. What we have shown is that any genus 2 curve admitting a $(4,4)$-isogeny whose kernel is defined elementwise over K satisfies one of the equations above.

Proposition 5.9.8. *Let $\mathcal{J}$ be the Jacobian of a genus 2 curve $\mathcal{C}$ over K admitting a $(4,4)$-isogeny φ. Then $\mathcal{C}$ is isomorphic over K to the curve $\mathcal{C}_{abcd}\colon y^2 = df_{abc}(x)$, for some $f_{abc}(x)$ from the $(4,4)$-family and $d \in K^*$. If $\ker\varphi$ is elementwise K-rational, then a, b, c satisfy Λ_{ijk} for some i, j, k and are thus described by Tables 5.3 and 5.2.*

5.9.5 A family of curves where both split

We also found a family of curves that admit a Richelot isogeny such that the curves in the original family have full 2-torsion and their isogenous curves also have full 2-torsion.

Proposition 5.9.9. *Let K be a field and let $K(s,t)$ be the function field in two variables over K. Let $\mathcal{C}\colon y^2 = x(x-1)(x-a)(x-b)(x-c)$, where*

$$\begin{aligned} a &= t^2 \\ b &= (s^2t^2 - s^2 + 3t^2 + 1)/(s^2t^2 + 3s^2 - t^2 + 1) \\ c &= bs^2, \end{aligned} \tag{5.129}$$

and let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. Let

$$(G_1(x), G_2(x), G_3(x)) = (x, (x-1)(x-a), (x-b)(x-c)), \tag{5.130}$$

and let $\mathcal{C}'\colon y^2 = L_1(x)L_2(x)L_3(x)$ be the Richelot isogenous curve for (G_1, G_2, G_3), and let $\mathcal{J}'$ be the Jacobian of $\mathcal{C}'$. Then $\mathcal{J}[2](K(s,t)) \cong (\mathbb{Z}/2\mathbb{Z})^4$ and $\mathcal{J}'[2](K(s,t)) \cong (\mathbb{Z}/2\mathbb{Z})^4$.

Proof. Start with the curve $\mathcal{C}\colon y^2 = x(x-1)(x-a)(x-b)(x-c)$ and consider the Richelot isogeny from the splitting $(G_1(x), G_2(x), G_3(x) = (x, (x-1)(x-a), (x-b)(x-c))$. The Richelot isogenous curve has equation $\mathcal{C}'\colon y^2 = g(x) = L_1(x)L_2(x)L_3(x)$. Then $g(x)$ splits if and only if each $L_i(x)$ splits, which happens if and only if the discriminant of each $L_i(x)$ is square. Recall that $L_i(x) = G_{i+1}(x)G'_{i+2}(x) - G'_{i+1}(x)G_{i+2}(x)$. Victor Flynn pointed out that the discriminant of $L_i(x)$ equals $4\operatorname{Res}(G_{i+1}(x), G_{i+2}(x))$, which can be verified algebraically. Thus $g(x)$ splits if and only if $\operatorname{Res}(G_i(x), G_{i+1}(x))$ is square for each $i = 1, 2, 3$. Recall that $\operatorname{Res}(\prod_{i=1}^n (x-\alpha_i), B(x)) = \prod_{i=1}^n B(\alpha_i)$ and $\operatorname{Res}(A, B) = (-1)^{\deg A \deg B}\operatorname{Res}(B, A)$. Consequently, $g(x)$ splits if and only if the following three quantities are square

$$\operatorname{Res}(G_1, G_2) = a \tag{5.131}$$

$$\operatorname{Res}(G_2, G_3) = (1-b)(1-c)(a-b)(a-c) \tag{5.132}$$

$$\operatorname{Res}(G_3, G_1) = bc. \tag{5.133}$$

Equations (5.131) and (5.133) are equivalent to $a = t^2$ and $c = bs^2$ for $s, t \in K$. Now we look to solve (5.132), which is equivalent to

$$y^2 = (b-1)(bs^2-1)(b-t^2)(bs^2-t^2). \tag{5.134}$$

On changing variables to $b = x + 1$ and further putting $(u, v) = (1/x, y/x^3)$, we transform to a genus 1 curve of the form

$$y^2 = dx^3 + c_2x^2 + c_1x + c_0, \tag{5.135}$$

where $d = (t^2-1)(s^2-1)(t^2-s^2)$. The right hand side isn't monic, so we change variables to $(x, y) = (dX, d^2Y)$, which gives the equation

$$\begin{aligned} Y^2 = X^3 &+ \frac{-2s^4t^2 + 3s^4 + s^2t^4 - s^2t^2 - 2s^2 + t^2}{d^2}X^2 \\ &+ \frac{-s^4t^2 + 3s^4 - s^2t^2 - s^2}{d^3}X + \frac{s^4}{d^4}, \end{aligned} \tag{5.136}$$

which is an elliptic curve. Tracing back the maps, we find that any solution (X, Y) to (5.136) gives a solution $b = 1 + \frac{1}{dX}$ to the original equation (5.134). Since the constant coefficient of the elliptic curve is square, the point $P = (0, \frac{s^2}{d^2})$ lies on the curve. This gives a degenerate solution to (a, b, c), but $2P$ has X-coordinate

$$\frac{s^2t^2 + 3s^2 - t^2 + 1}{4d(t^2 - s^2)}, \tag{5.137}$$

which corresponds to the solution

$$a = t^2 \tag{5.138}$$

$$b = (s^2t^2 - s^2 + 3t^2 + 1)/(s^2t^2 + 3s^2 - t^2 + 1) \tag{5.139}$$

$$c = bs^2. \tag{5.140}$$

□

Remark 5.9.10. *By choosing different multiples of the point P in the proof above, we find different solutions. However, specialising at $(s,t) = (5,11)$ gives a rank 1 curve, generated by the point P with $x(P) = 0$, so generically the elliptic curve has rank 1.*

Remark 5.9.11. *Let $\mathcal{J}$ and $\mathcal{J}'$ be the Jacobians from Proposition 5.9.9. Since $\mathcal{J}'$ has full 2-torsion, $\mathcal{J}$ admits a $(4,4)$-isogeny. Even though $\mathcal{J}$ also has full 2-torsion, this doesn't mean that the $(4,4)$-subgroup is defined over K. It turns out that to find the 4-torsion points lying above the 2-torsion points, which is equivalent to solving for an eigenvector in one of the eigenspaces (for the translation matrix) to lie on the Kummer surface, we need the following product to be square:*

$$(s^2t^2 - s^2 + 3t^2 + 1)(s^2t^2 + 3s^2 - t^2 + 1). \tag{5.141}$$

The other eigenspace has a similar condition. We would then further need these points to lift to the Jacobian, which requires a further element to be square.

Remark 5.9.12. *The family of curves in Proposition 5.9.9 potentially defines an $(8,8)$-isogeny. Let $\varphi_2 \colon \mathcal{J}_2 \to \mathcal{J}_3$ be the Richelot isogeny described in the Proposition. Then define $\varphi_1 \colon \mathcal{J}_1 \to \mathcal{J}_2$ and $\varphi_3 \colon \mathcal{J}_3 \to \mathcal{J}_4$ to be the duals of two Richelot isogenies out of $\mathcal{J}_2$ and $\mathcal{J}_3$, respectively. We need to check that the Weil pairing acts trivially on the kernel.*

5.10 Computing $\mathcal{J}[4](\overline{K})$

Let $\mathcal{J}$ be the Jacobian of a genus 2 hyperelliptic curve $y^2 = f(x)$ over a number field K. The multiplication by n isogeny $[n] \colon \mathcal{J} \to \mathcal{J}$ has kernel $\mathcal{J}[n]$, the n-torsion points. We can also do descent by computing $\mathcal{J}(K)/n\mathcal{J}(K)$, which is called *complete descent*. One way of doing this is to compute the full n-torsion subgroup of $\mathcal{J}(\overline{K})$. If $n = 2$, then $\mathcal{J}[2]$ consists of the 2-torsion points. Assuming $\deg f = 6$, the nontrivial 2-torsion points are precisely $(\alpha_i, 0) + (\alpha_j, 0) - \infty^+ - \infty^-$ where α_i, α_j run over all distinct pairs

of roots of $f(x)$ in $\overline{K}$. Since $f(x)$ has distinct roots in $\overline{K}$, there are 15 such nontrivial 2-torsion points. They are defined over the splitting field of $f(x)$.

Algorithm 5 shows how to compute the 4-torsion points D that double to a given 2-torsion point T on the Jacobian of a genus 2 curve. Since any 4-torsion point $D \in \mathcal{J}[4]$ doubles to $2D \in \mathcal{J}[2]$, applying this process to a basis for $\mathcal{J}[2]$ recovers a basis for $\mathcal{J}[4]$.

We get a basis for $\mathcal{J}[2](\overline{K})$ by first moving to the splitting field K' of $f(x)$, over which all the 2-torsion is defined. Let $\alpha_1, \ldots, \alpha_6$ be the roots of $f(x)$, where we let $\alpha_6 = \infty$ if f is degree 5. Then the nontrivial 2-torsion points are the set $\{T_{ij} : 1 \leq i < j \leq 6\}$, where $T_{ij} = P_i - P_j$. Here $P_i = (\alpha_i, 0)$ if $\alpha_i \neq \infty$ and $P_i = \infty$ if $\alpha_i = \infty$. As discussed in Section 5.2, T_{ij} corresponds to the quadratic $(x - \alpha_i)(x - \alpha_j)$, where we replace $(x - \alpha_i)$ by 1 if $\alpha_i = \infty$.

This gives us an algorithm to compute $\mathcal{J}[4](\overline{K})$.

Chapter 6

Descent methods

6.1 Introduction

Let $\mathcal{J}$ be the Jacobian of a curve $\mathcal{C}$ defined over a field K. A major question in number theory is to determine the set of points $\mathcal{J}(K)$. The Mordell–Weil theorem (Theorem 2.2.2) implies that if K is a number field, and $\mathcal{J}$ is the Jacobian of a smooth curve $\mathcal{C}/K$, then $\mathcal{J}(K)$ is a finitely generated abelian group. Thus there is an integer $r \geq 0$ and a finite group $\mathcal{J}(K)_{\text{tors}}$ such that $\mathcal{J}(K) \cong \mathbb{Z}^r \times \mathcal{J}(K)_{\text{tors}}$. The integer r is called the *rank* of $\mathcal{J}(K)$, and is of great interest.

For any integer $m \geq 2$, we have

$$\mathcal{J}(K)/m\mathcal{J}(K) \cong (\mathbb{Z}/m\mathbb{Z})^r \times J(K)_{\text{tors}}/mJ(K)_{\text{tors}}. \tag{6.1}$$

The torsion subgroup $\mathcal{J}(K)_{\text{tors}}$ is straightforward to compute, and so to compute r it suffices to compute $\mathcal{J}(K)/m\mathcal{J}(K)$ for some integer $m \geq 2$.

More generally, if $\varphi\colon \mathcal{J} \to \mathcal{J}'$ is an isogeny to another Jacobian $\mathcal{J}'$, with φ and $\mathcal{J}'$ also defined over K, then we can try to bound above $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$. If $\varphi'\colon \mathcal{J}' \to \mathcal{J}$ is the dual isogeny (compare Section 2.2.1), which satisfies $\varphi' \circ \varphi = [m]$, we can combine bounds for $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ and $\mathcal{J}(K)/\varphi'\mathcal{J}'(K)$ to get a bound for $\mathcal{J}(K)/m\mathcal{J}(K)$.

In this chapter we introduce Schaefer's method for doing a descent via isogeny ([Sch98]) and then apply it to the $(4,4)$-isogeny computed in Chapter 5. Schaefer originally applied this to Jacobians of superelliptic curves of the form $y^p = f(x)$. Such curves admit the automorphism $\zeta_p\colon (x,y) \mapsto (x, \zeta_p y)$, where ζ_p is a primitive pth root of unity. Let $\mathcal{J}$ denote the Jacobian of such a curve; the map $\varphi = 1 - \zeta_p$ induces an isogeny $\mathcal{J} \to \mathcal{J}$, and Schaefer does a descent via φ-isogeny. Schaefer makes two assumptions to make his method work. The first is to ensure that elements of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ are represented by K-rational divisors on $\mathcal{C}$. The second assumption is

that the map he calls w is injective; we also call this map w, and discuss this problem in Section 6.8.

There are a number of technical difficulties in generalising this approach to other isogenies. Schaefer's approach notably doesn't apply to the case where φ is the multiplication-by-2 isogeny, [2], on the Jacobian. Poonen and Schaefer generalised Schaefer's approach to this case, at the cost that the map w to be defined is no longer injective ([PS97]). More recently, Bruin, Poonen and Stoll generalised the approach further ([BPS14]); they apply their method to a genus 3 nonhyperelliptic curve. We use the original version of Schaefer's method in the following.

Our main contributions are: to use the Richelot descent to generate the local points $\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)$; to use the $(4,4)$-isogeny whose kernel is K-rational in Section 5.9.3, and to explicitly compute it; and to combine the $(4,4)$-descent and Richelot descent on the same diagram.

6.2 Background

Local fields and Galois theory Let s be a place of a number field K. Then we can define the completion K_s, which is a local field. If s is an archimedean place, then K_s is either $\mathbb{R}$ or $\mathbb{C}$; if s is a nonarchimedean place then K_s is a finite extension of $\mathbb{Q}_p$ for some p.

Let $\mathcal{O}_s$ be the ring of integers of K_s. There is a unique prime ideal $\mathfrak{P}$ of $\mathcal{O}_s$. The residue field k_s is the field $\mathcal{O}_s/\mathfrak{P}$. Fix an algebraic closure, $\overline{K}_s$, of K_s. An automorphism $\sigma \in \mathrm{Gal}(\overline{K}_s/K_s)$ fixes $\mathfrak{P}$ (since it's the unique prime ideal) and thus induces an automorphism of $\mathcal{O}_s/\mathfrak{P} = k_s$, fixing $\mathcal{O}_p/p = \mathbb{F}_p$. Thus we have a surjective map $\mathrm{Gal}(\overline{K}_s/K_s) \to \mathrm{Gal}(\overline{k}_s/k_s)$. The inertia group, I_s, is the kernel of this map. We say that a cocycle $\xi \in H^r(K, M)$ is *unramified* at s if it is trivial when restricted to $H^r(I_s, M)$.

The following theorem is key to the proof of the Mordell–Weil theorem, and we will use it later.

Theorem 6.2.1 ([Sil09])**.** *Let K be a number field and let M be a finite abelian $\mathrm{Gal}(\overline{K}/K)$-module. Let S be a finite set of places of K. Then $H^1(K, M; S)$ is finite.*

Fields of definition Let $\mathcal{C}$ be a curve over a number field K. The absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on the group of divisors $\mathrm{Div}(\mathcal{C})$, and if $D \in \mathrm{Div}(\mathcal{C})$, we define the field of definition of D as $K(D) = \overline{K}^{H(D)}$, where $H(D) = \{\sigma \in G_K : {}^{\sigma}D = D\}$

is the subgroup of automorphisms that fix D. By the fundamental theorem of Galois theory in the case of infinite Galois extensions, if $H \subseteq G_K$, we have $\mathrm{Gal}(\overline{K}/K^H) = \bar{H}$, where $\bar{H}$ is the closure of H in G_K. Also, if L is a field intermediate between K and $\overline{K}$, then $\overline{K}^{\mathrm{Gal}(\overline{K}/L)} = L$.

Representing elements of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ The following proposition and proof are from [Sch98], and give a condition under which we can represent points in the quotient $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ by K-rational divisors. In the following sections we define some explicit maps from $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$, assuming that we can represent elements of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ by K-rational divisors.

Proposition 6.2.2 ([Sch98], Proposition 2.7)**.** *Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be an isogeny of degree $q = p^\ell$. Suppose that p is prime to*

$$d = \gcd\{[K'\colon K]\colon K \subseteq K' \subseteq \overline{K}, \mathcal{C}'(K') \neq \emptyset\}. \tag{6.2}$$

Then every element of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ can be represented by a degree zero divisor class that is fixed under G_K.

Proof. Let K' be a degree d' extension of K such that $\mathcal{C}'(K') \neq \emptyset$. By Proposition 2.1.7, $\mathcal{J}'(K)$ equals the $G_{K'}$-fixed divisors of $\mathcal{C}'(K')$ modulo linear equivalence. Let ι denote the inclusion $K \to K'$ and let N denote the norm $K' \to K$. Consider the following commutative diagram

$$\begin{array}{ccccc}
\mathrm{Div}^0(\mathcal{C}')(K) & \longrightarrow & \mathcal{J}'(K) & \longrightarrow & \mathrm{coker} \\
\downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\
\mathrm{Div}^0(\mathcal{C}')(K') & \longrightarrow & \mathcal{J}'(K) & \longrightarrow & 0 \\
\downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\
\mathrm{Div}^0(\mathcal{C}')(K) & \longrightarrow & \mathcal{J}'(K) & \longrightarrow & \mathrm{coker}\,.
\end{array} \tag{6.3}$$

The composition $N \circ \iota$ equals the multiplication by d' map. The right column shows that $d'\colon$ coker $\to$ coker factors through 0, and so multiplication by d' kills the cokernel. Thus d, as defined in the statement, kills the cokernel also. The argument for local fields is similar. See [Sch98]. □

6.3 The Selmer and Tate–Shafarevich groups

We first motivate Schaefer's construction with some abstract maps. At this point we don't need to explicitly compute these maps, but will show how to make this all

more explicit in the next section. We mainly just need to know how to get long exact sequences from short exact sequences in Galois cohomology, and that this is functorial. See Appendix A for an introduction to Galois cohomology.

Let $\mathscr{K}$ be an extension of K, and let $\overline{\mathscr{K}}$ be an algebraic closure. We are mainly interested in when $\mathscr{K}/K$ is a finite extension of number fields, or a completion K_s of K at some place s. Consider the short exact sequence in Galois cohomology

$$0 \to \mathcal{J}[\varphi](\overline{\mathscr{K}}) \xrightarrow{\iota} \mathcal{J}(\overline{\mathscr{K}}) \xrightarrow{\varphi} \mathcal{J}'(\overline{\mathscr{K}}) \to 0. \tag{6.4}$$

Then the associated long exact sequence in Galois cohomology gives the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathcal{J}[\varphi](\mathscr{K}) \xrightarrow{\iota} \mathcal{J}(\mathscr{K}) \xrightarrow{\varphi} \mathcal{J}'(\mathscr{K}) \xrightarrow{\delta} \\ H^1(\mathscr{K}, \mathcal{J}[\varphi]) \xrightarrow{\iota} H^1(\mathscr{K}, \mathcal{J}) \xrightarrow{\varphi} H^1(\mathscr{K}, \mathcal{J}'). \end{aligned} \tag{6.5}$$

This gives the short exact sequence

$$0 \to \mathcal{J}'(\mathscr{K})/\varphi\mathcal{J}(\mathscr{K}) \xrightarrow{\delta} H^1(\mathscr{K}, \mathcal{J}[\varphi]) \xrightarrow{\iota} H^1(\mathscr{K}, \mathcal{J})[\varphi] \to 0. \tag{6.6}$$

To get this, just note that $\ker \iota = \delta(\mathcal{J}'(\mathscr{K}))$, and $\delta(\mathcal{J}'(\mathscr{K})) \cong \mathcal{J}'(\mathscr{K})/\varphi\mathcal{J}'(\mathscr{K})$, since $\ker \delta = \operatorname{im} \varphi$. Finally, the map ι on H^1 is surjective onto its image, which equals the kernel of φ on H^1.

With $\mathscr{K}$ being the completions of K, these sequences fit into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J}'(K)/\varphi\mathcal{J}(K) & \xrightarrow{\delta} & H^1(K, \mathcal{J}[\varphi]) & \xrightarrow{\iota} & H^1(K, \mathcal{J})[\varphi] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \prod_s \alpha_s} & & \downarrow{\scriptstyle \prod_s \beta_s} & & \downarrow{\scriptstyle \prod_s \gamma_s} & & \\ 0 & \longrightarrow & \prod_s \mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s) & \xrightarrow{\prod_s \delta_s} & \prod_s H^1(K_s, \mathcal{J}[\varphi]) & \xrightarrow{\prod_s \iota_s} & \prod_s H^1(K_s, \mathcal{J})[\varphi] & \longrightarrow & 0. \end{array} \tag{6.7}$$

Here α_s is the inclusion of $\mathcal{J}(K)$ into $\mathcal{J}(K_s)$. In general, if $h\colon G' \to G$ is a group homomorphism and $f\colon A \to A'$ is a homomorphism of G-modules, then the map $H^r(G, A) \to H^r(G', A')$ is given by $\xi\colon G^r \to A \mapsto f \circ \xi \circ h\colon G'^r \xrightarrow{h} G^r \xrightarrow{\xi} A \xrightarrow{f} A'$. The maps β_s and γ_s both come from the inclusions $\operatorname{Gal}(\overline{K}_s/K_s) \hookrightarrow \operatorname{Gal}(\overline{K}/K)$ and $\mathcal{J}(\overline{K}) \subset \mathcal{J}(\overline{K}_s)$ for all places s of K.

We can now define the *φ-Selmer group* as

$$\operatorname{Sel}^{\varphi}(\mathcal{J}/K) = \ker \prod_s \iota_s\beta_s, \tag{6.8}$$

and the *Tate–Shafarevich group* as

$$Ш(\mathcal{J}/K) = \ker\left(\prod_s \gamma_s \colon H^1(K,\mathcal{J}) \to H^1(K_s,\mathcal{J})\right). \tag{6.9}$$

The φ-part of the Tate–Shafarevich group is

$$Ш(\mathcal{J}/K)[\varphi] = \ker\left(\prod_s \gamma_s \colon H^1(K,\mathcal{J})[\varphi] \to H^1(K_s,\mathcal{J})[\varphi]\right). \tag{6.10}$$

As can be seen from the diagram above, these fit into the exact sequence

$$0 \to \mathcal{J}'(K)/\varphi\mathcal{J}(K) \xrightarrow{\delta} \mathrm{Sel}^{\varphi}(\mathcal{J}/K) \xrightarrow{\iota} Ш(\mathcal{J}/K)[\varphi] \to 0. \tag{6.11}$$

Let S be a finite set of places of a number field K, and let M be a G_K-module. Then we define $H^1(K, M; S)$ as the subset of $\xi \in H^1(K, M)$ such that ξ is unramified away from S. Milne proves the following proposition in [Mil06], which shows that all of the intersections above can be taken over just the finite set of primes S.

Proposition 6.3.1 ([Mil06])**.** *Let S be the set of archimedean places, the places above $m = \deg\varphi$ and the places of bad reduction for $\mathcal{J}$. The image of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$ lies inside $H^1(K, \mathcal{J}[\varphi]; S)$.*

Remark 6.3.2. *Let $\mathscr{K}$ be an extension of K. We can interpret elements of $H^1(\mathscr{K}, \mathcal{J})$ as torsors of $\mathcal{J}$, which are trivial if and only if they have a $\mathscr{K}$-point. Under this interpretation, elements of $Ш(\mathcal{J}/K)$ correspond to torsors that have a point over every completion K_s of K (we say the torsor has points everywhere locally); nontrivial elements of $Ш(\mathcal{J}/K)$ have points everywhere locally but don't have points over K. Elements of $\mathrm{Sel}^{\varphi}(\mathcal{J}/K)$ correspond to certain torsors that have points everywhere locally.*

6.4 Schaefer's descent method

For Jacobians of curves of genus at least two, it turns out to be difficult to explicitly describe the torsors, and thus to determine whether they have points everywhere locally. In this section, we explain Schaefer's approach to explicitly computing $\mathrm{Sel}^{\varphi}(\mathcal{J}/K)$ ([Sch98]).

Fix an isogeny $\varphi \colon \mathcal{J} \to \mathcal{J}'$ of Jacobians of curves $\mathcal{J}, \mathcal{J}'$. Assume that $\varphi, \mathcal{J}, \mathcal{J}'$ are all defined over a field K. We have the following exact sequence of G_K-modules:

$$0 \to \mathcal{J}'(K)/\varphi\mathcal{J}(K) \to \mathrm{Sel}^{\varphi}(\mathcal{J}/K) \to Ш(\mathcal{J}/K)[\varphi] \to 0. \tag{6.12}$$

The middle term, $\mathrm{Sel}^{\varphi}(\mathcal{J}/K)$ gives an upper bound on $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$, and the sharpness of the bound is measured by $Ш(\mathcal{J}/K)[\varphi]$.

Suppose that $\mathcal{J}[\varphi]$ has exponent m. Then Schaefer constructs the commutative diagram

$$\begin{array}{ccccc} \mathcal{J}'(K)/\varphi\mathcal{J}(K) & \xrightarrow{\delta} & H^1(K,\mathcal{J}[\varphi];S) & \xrightarrow{\rho} & L^*/L^{*m} \\ \downarrow{\scriptstyle \prod_{s\in S}\alpha_s} & & \downarrow{\scriptstyle \prod_{s\in S}\beta_s} & & \downarrow{\scriptstyle \prod_{s\in S}\gamma_s} \\ \prod_{s\in S}\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s) & \xrightarrow{\prod_{s\in S}\delta_s} & \prod_{s\in S}H^1(K_s,\mathcal{J}[\varphi]) & \xrightarrow{\prod_{s\in S}\rho_s} & \prod_{s\in S}L_s^*/L_s^{*m} \end{array} \tag{6.13}$$

where L is an explicitly given K-algebra and ρ is a map defined in terms of $\ker\varphi$; both L and ρ need to be explicitly computed for the given isogeny φ. Let S be the subset of primes of K consisting of primes of bad reduction for $\mathcal{J}$ and $\mathcal{J}'$, together with any primes of K dividing m. The image of the Selmer group in L^*/L^{*m} is

$$\rho\left(\mathrm{Sel}^{\varphi}(\mathcal{J}/K)\right) = L(S,m) \cap \bigcap_{s\in S} \gamma_s^{-1}\left((\rho_s\delta_s)\left(\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)\right)\right), \tag{6.14}$$

where $L(S,m) \subset L^*/L^{*m}$ is the subgroup generated by elements that are unramified away from S. We discuss $L(S,m)$ in more detail in Section 6.9.5.

Definition 6.4.1. *We write $M^{\varphi}(\mathcal{J}/K)$ for $\rho((\mathrm{Sel}^{\varphi}(\mathcal{J}/K))$.*

We will see that the maps ρ, ρ_s are not always injective, but even in that case we can still get information about $\mathrm{Sel}^{\varphi}(\mathcal{J}/K)$.

We now explain Schaefer's construction in [Sch98] in more detail. We first introduce a $\overline{K}$-algebra L', with a specific G_K-action. We then use the Weil pairing to get a map from $\mathcal{J}[\varphi] \to \mu_m(L')$; this induces a map on Galois cohomology $H^1(K,\mathcal{J}[\varphi]) \to H^1(K,\mu_m(L'))$. The Kummer isomorphism gives a map $H^1(K,\mu_m(L')) \xrightarrow{\sim} L^*/L^{*m}$, where L is the subgroup of G_K-invariants of L'. The composition of these maps with the inclusion $\mathcal{J}'(K)/\varphi\mathcal{J}(K) \to H^1(K,\mathcal{J}[\varphi])$ is easy to compute, and we can then work with subgroups of L^*/L^{*m} and their completions, as opposed to elements of Galois cohomology groups.

6.4.1 The $\overline{K}$-algebra L'

Let φ' be the dual isogeny $\mathcal{J}' \to \mathcal{J}$ as in Section 2.2.1; that is, $\varphi' = \lambda^{-1}\varphi^{\vee}\lambda'$, where $\lambda\colon \mathcal{J} \to \mathcal{J}^{\vee}$ and $\lambda'\colon \mathcal{J}' \to \mathcal{J}'^{\vee}$ are the principal polarisations of the Jacobians, and $\varphi^{\vee}$ denotes the dual isogeny of φ in the sense of abelian varieties.

Remark 6.4.2. *If φ is an (n,n)-isogeny as in Chapter 5, then φ' is the isogeny such that $\varphi' \circ \varphi = [n]$.*

Let $D_1, \dots, D_n$ be a G_K-stable spanning set for $\mathcal{J}'[\varphi']$; that is, $\{D_1, \dots, D_n\}$ spans $\mathcal{J}'[\varphi']$ and the action of G_K leaves the set invariant. Define the $\overline{K}$-algebra L' as $\prod_{i=1}^n \overline{K}$, and give L' the following G_K action: if $\sigma \in G_K$, then define $\bar{\sigma} \in S_n$ by $\bar{\sigma}(i) = j$ if and only if ${}^{\sigma}D_i = D_j$. Then for $(a_1, \dots, a_n) \in L'$, define

$$ {}^{\sigma}(a_1, \dots, a_n) = ({}^{\sigma}a_{\bar{\sigma}^{-1}1}, \dots {}^{\sigma}a_{\bar{\sigma}^{-1}n}). \tag{6.15} $$

This is a well-defined G_K-action on L'. Note that ${}^{\sigma}D_i \in \{D_1, \dots, D_n\}$, since the set is G_K-stable.

If E/K is a field extension contained in $\overline{K}$, then define $L_E = {L'}^{\mathrm{Gal}(\overline{K}/E)}$; we write L for L_K when it is clear. Let $E(D_i)$ be the field of definition of D_i over E. We first claim that

$$ L_E \subseteq \prod_{i=1}^{n} E(D_i). \tag{6.16} $$

Since $E(D_i) = \overline{K}^{\mathrm{Gal}(\overline{K}/E(D_i))}$, it suffices to show that ${}^{\tau}(a_i) = (a_i)$ for all $a \in {L'}^{\mathrm{Gal}(\overline{K}/E)}$. But if τ fixes $E(D_i)$, then $\bar{\tau}i = i$. Writing π_i for the ith projection map $L' \to \overline{K}$, we have $\pi_i({}^{\tau}(a_1, \dots, a_n)) = {}^{\tau}a_i$, so that ${}^{\tau}a_i = a_i$ for all $a \in L_E$. Thus $a_i \in E(D_i)$, as required. In general, (6.16) is not an equality, since $E(D_1) \times \cdots \times E(D_n)$ isn't necessarily fixed by $\mathrm{Gal}(L/E)$; in fact, if D_j is in the same G_K-orbit as D_i, then a_i determines a_j via the G_K-action. The following proposition from [Sch98] describes L as a product of some of the $K(D_i)$.

Proposition 6.4.3 ([Sch98])**.** *Let $\Lambda \subseteq \{1, \dots, n\}$ consist of one representative for each G_K-orbit of $\{1, \dots, n\}$ with G_K acting via $\bar{\sigma}$. Let $M = \prod_{j \in \Lambda} K(D_j)$ be the product of the fields of definition of D_j, one for each orbit. For each orbit, $E_1, \dots, E_r$, choose $\sigma_1, \dots, \sigma_r \in \mathrm{Gal}(\overline{K}/K)$ such that $G_K = \coprod_{i=1}^r \sigma_i \,\mathrm{Gal}(\overline{K}/K(E_i))$ and ${}^{\sigma_i}E_1 = E_i$. Define the map $\psi\colon K(E_1) \to \prod_{i=1}^r \overline{K}$ by $\psi(m) = ({}^{\sigma_1}m, \dots, {}^{\sigma_r}m)$. Combine these across all the orbits to define a map $\psi\colon M \to L$. This is an isomorphism of K-algebras.*

Proof. If there is more than one G_K-orbit for $\{D_1, \dots, D_n\}$ then we can combine the maps for each orbit into a single map. The proof below is then applied to each orbit.

We first have to show that if $\sigma \in G_K$, then ${}^{\sigma}(\psi(m)) = \psi(m)$. Let $\sigma \in G_K$ and $m \in M$. Then ${}^{\sigma}\psi(m) = {}^{\sigma}({}^{\sigma_1}m, \dots, {}^{\sigma_n}m)$. It suffices to show the ith elements agree. Temporarily write m_j for ${}^{\sigma_j}m$. We want to show that ${}^{\sigma}m_{\bar{\sigma}^{-1}i} = m_i$. Let $\bar{\sigma}(j) = i$. Then, taking σ_i^{-1} on both sides, it suffices to show ${}^{\sigma_i^{-1}\sigma\sigma_j}m = m$. Thus it suffices to show that $\eta \coloneqq \sigma_i^{-1}\sigma\sigma_j \in \mathrm{Gal}(\overline{K}/K(D_1))$.

Note that if $\sigma \in G_K$ satisfies ${}^{\sigma}D = D$, then $\sigma \in \mathrm{Gal}(\overline{K}/K(D))$. Consider $\overline{\eta}(1)$. Firstly, ${}^{\sigma_j}D_1 = D_j$, so that $\bar{\sigma}_j(1) = j$. Also, we defined j such that $\bar{\sigma}(j) = i$. Hence $\overline{\eta}(1) = 1$. This means that ${}^{\eta}D_1 = D_1$, so that $\eta \in \mathrm{Gal}(\overline{K}/K(D_1))$. Consequently, $\psi(m) \in L$, the G_K-invariants of L'.

The map $M \to L$ is injective, and the map $\mu\colon L \to M$ sending $(\ell_1, \ldots, \ell_n) \mapsto {}^{{\sigma_1}^{-1}}\ell_1$ is an inverse. The image of μ is in $M = K(D_1)$ since $(\ell_1, \ldots, \ell_n) \in L$, so ${}^{\sigma_1}(\ell_1, \ldots, \ell_n) = (\ell_1, \ldots, \ell_n)$; thus, ${}^{\sigma_1}\ell_{\bar{\sigma}_1^{-1}(1)} = \ell_1$. Since ${}^{\sigma_1}D_1 = D_1$, we have $\bar{\sigma}_1(1) = 1$, and thus ${}^{\sigma_1}\ell_1 = \ell_1$. □

Remark 6.4.4. *The map $M \to L$ is not a map of G_K-modules, since M has no G_K-action.*

6.4.2 The cohomology group $H^1(K, \mu_m(L'))$

Recall that we write L for L'^{G_K}. In this section we show

$$H^1(K, \mu_m(L')) \cong L^*/L^{*m}. \tag{6.17}$$

Consider the exact sequence in Galois cohomology

$$1 \to \mu_m(L') \to L'^* \xrightarrow{\cdot^m} L'^* \to 1. \tag{6.18}$$

The long exact sequence in Galois cohomology gives us an exact sequence

$$L^* \xrightarrow{\cdot^m} L^* \xrightarrow{\kappa_m} H^1(K, \mu_m(L')) \to H^1(K, L'^*), \tag{6.19}$$

where κ_m is the connecting homomorphism.

Proposition 6.4.6 shows Hilbert's Theorem 90 holds in our case. This implies that the last term in (6.19) is zero, so the map $\kappa_m\colon L^* \to H^1(K, \mu_m(L'))$ is surjective; its kernel is L^{*m}, so the isomorphism (6.17) follows.

Remark 6.4.5. *Our proof is a modified version of the proof in [Ser79]. The original proof doesn't apply, since the G_K-actions differ.*

Proposition 6.4.6 (Hilbert's Theorem 90)**.** *Let F/K be a Galois extension of infinite fields. Let $L_F = \prod_{i=1}^n F$ be the K-algebra defined on the divisors $D_1, \ldots, D_n$, with the given $\mathrm{Gal}(F/K)$-action. Then $H^1(\mathrm{Gal}(F/K), L_F^{\times}) = \{0\}$.*

Proof. First recall that if G is a profinite group and $\mathcal{U}$ is the collection of open normal subgroups, and if A is a G-module with the discrete topology, then

$$H^1(G, A) = \varinjlim_{N \in \mathcal{U}} H^1(G/N, A^N). \tag{6.20}$$

If G is the Galois group of an infinite Galois extension F/K, then the open subgroups of G are the Galois groups $\mathrm{Gal}(F/E)$ with E/K a finite extension ([Sha]). The open normal subgroups are $\mathrm{Gal}(F/E)$ with E/K finite and normal. Thus $G/N \cong \mathrm{Gal}(E/K)$. Recall $L_E = L_F^{\mathrm{Gal}(F/E)}$. To show that $H^1(\mathrm{Gal}(F/K), L_F^\times)$ is trivial, it suffices to show that each $H^1(\mathrm{Gal}(E/K), L_E^\times)$ is trivial.

We can now slightly modify the proof of Hilbert's Theorem 90. Let ξ be a cocycle in $H^1(\mathrm{Gal}(E/K), L_E^\times)$. We will show that ξ is a coboundary. Consider the map $z\colon L_E^\times \to L_E$ given by

$$z(a) = \sum_{\sigma \in \mathrm{Gal}(E/K)} \xi_\sigma \sigma(a). \tag{6.21}$$

Suppose we can find $a \in L_E^\times$ such that $z(a) \in L_E^\times$; that is, each component of $z(a)$ is nonzero. Then, for any $\tau \in \mathrm{Gal}(E/K)$, we have

$$\begin{aligned} \tau(z(a)) &= \sum_{\sigma \in \mathrm{Gal}(E/K)} \tau(\xi_\sigma)(\tau\sigma)(a) && (6.22)\\ &= \sum_{\sigma \in \mathrm{Gal}(E/K)} \xi_\tau^{-1} \xi_{\tau\sigma} (\tau\sigma)(a) && (6.23)\\ &= \xi_\tau^{-1} \sum_{\sigma \in \mathrm{Gal}(E/K)} \xi_\sigma \sigma(a) && (6.24)\\ &= \xi_\tau^{-1} z(a). && (6.25) \end{aligned}$$

The second line follows from the cocycle condition $\xi_{\tau\sigma} = \xi_\tau \tau(\xi_\sigma)$ and the third line follows by reindexing the sum. Thus we have $\xi_\tau = {}^\tau y / y$ is a coboundary, where $y = 1/z(a)$.

It remains to show that we can find such an $a \in L_E$. In particular, we need each component of $z(a) \in L_E$ to be nonzero. To simplify the $\mathrm{Gal}(E/K)$-action, we consider $\Delta(E) = \{(\alpha, \ldots, \alpha)\colon \alpha \in E\} \subset L_E^\times$, and find $a \in \Delta(E)$ such that $z(a) \in L_E^\times$.

We write E' for $E(D_1, \ldots, D_n)$, the field of definition of all D_i over E. This is a finite extension of E contained in F. First note that $\pi_i \circ \sigma$ is a character $E^\times \to E'^\times$.

We first show that if $\sigma, \tau \in \mathrm{Gal}(E/K)$ and $\pi_i\sigma = \pi_i\tau$ as maps $E^\times \to E'^\times$, then $\sigma = \tau$. Let $a = (\alpha, \ldots, \alpha) \in \Delta(E)$. Then $\pi_i\sigma(a) = {}^\sigma\alpha$, and similarly $\pi_i\tau(a) = {}^\tau\alpha$, so that ${}^\sigma\alpha = {}^\tau\alpha$. This holds for arbitrary $\alpha \in E$, so it follows that $\sigma = \tau$.

Thus the characters $\pi_i \circ \sigma\colon E^\times \to E'^\times$ are distinct and so linearly independent over E'. Thus if $z_i(\alpha) = \sum_{\sigma \in \mathrm{Gal}(E/K)} (\xi_\sigma)_i \sigma(\alpha) = 0$ for all $\alpha \in E$, then $(\xi_\sigma)_i = 0$ for all $\sigma \in \mathrm{Gal}(E/K)$. Consequently, for each i, the kernel of $z_i\colon E \to E'$ is a proper subspace of the K-vector space E.

Over an infinite field, a finite union of proper vector subspaces is a proper subspace. Thus the union of the kernels $\ker z_i$ is a proper subspace of E, so there is $\alpha \in E^\times$ such that for all i, $z_i(\alpha) \neq 0$. That is, with $a = (\alpha, \ldots, \alpha) \in \Delta(E)$, we have

$$z(a) = \sum_{\sigma \in \mathrm{Gal}(E/K)} \xi_\sigma \sigma(a) \neq 0. \tag{6.26}$$

□

6.4.3 The map w

We can now define the map w that was mentioned earlier. Let e_φ denote the Weil pairing with respect to our isogeny $\varphi\colon \mathcal{J} \to \mathcal{J}'$. Since the canonical polarisations λ, λ' are isomorphisms, we have that $\mathcal{J}'^\vee[\varphi^\vee] \cong \mathcal{J}'[\varphi']$, and so we can abuse notation and write the Weil pairing as a pairing

$$e_\varphi\colon \mathcal{J}[\varphi] \times \mathcal{J}'[\varphi'] \to \mu_m(L'). \tag{6.27}$$

Define the map $w\colon \mathcal{J}[\varphi] \to \mu_m(L')$ as

$$w(D) = \left(e_\varphi(D, D_1), \ldots, e_\varphi(D, D_n)\right), \tag{6.28}$$

where $D_1, \ldots, D_n$ are the divisors spanning $\mathcal{J}'[\varphi']$.

Remark 6.4.7. *To compute e_φ in practice, we use the compatibility property (see Section 2.2.2) together with the explicit definition of e_n in Proposition 2.2.7.*

Proposition 6.4.8 ([Sch98])**.** *The map $w\colon J[\varphi] \to \mu_m(L')$ is injective and defined over K. The map $w\colon H^1(K, J[\varphi]) \to H^1(K, \mu_m(L'))$ is thus also defined over K.*

Proof. The map w is injective, since the Weil pairing is nondegenerate. Suppose $w(P) = 1 \in \mu_m(L')$. Then $e_\varphi(P, D_i) = 1$ for each D_i. But the D_i generate $J'[\varphi']$, and so $e_\varphi(P, D) = 1$ for all $D \in J'[\varphi']$, which implies $P = 0$.

We now show that $w\colon J[\varphi] \to \mu_m(L')$ is defined over K. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then

$$w({}^\sigma P) = (e_\varphi({}^\sigma P, D_i))_i, \tag{6.29}$$

while

$$\begin{aligned}
{}^\sigma w(P) &= {}^\sigma(e_\varphi(P, D_i))_i && (6.30)\\
&= ({}^\sigma e_\varphi(P, D_{\bar\sigma^{-1} i}))_i && (6.31)\\
&= (e_\varphi({}^\sigma P, {}^\sigma D_{\bar\sigma^{-1} i}))_i && (6.32)\\
&= (e_\varphi({}^\sigma P, D_i))_i. && (6.33)
\end{aligned}$$

Hence $w({}^\sigma P) = {}^\sigma w(P)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, which implies that w is defined over K. Thus the map $w\colon H^1(K, J[\varphi]) \to H^1(K, \mu_m(L'))$ is also defined over K. □

6.4.4 The Cassels map

We define the *Cassels map* to be the composition

$$\rho_\varphi \colon \mathcal{J}'(K)/\varphi\mathcal{J}(K) \xhookrightarrow{\delta_\varphi} H^1(K, \mathcal{J}[\varphi]) \xrightarrow{w_\varphi} H^1(K, \mu_m(L')) \xrightarrow{\kappa_m^{-1}} L^*/L^{*m}. \tag{6.34}$$

This is the map ρ appearing in the commutative diagram (6.13).

The following proposition and proof are from [Sch98]; we give the proof as it is instructive.

Proposition 6.4.9 ([Sch98])**.** *Let $D_1 \ldots, D_n$ be divisors representing elements of $\mathcal{J}'[\varphi'] \subseteq \mathcal{J}'[m]$ such that $\{D_1, \ldots, D_n\}$ is G_K-stable and spans $\mathcal{J}'[\varphi']$. Let $F_1, \ldots, F_n$ be functions such that* $\operatorname{div} F_i = mD_i$*. Then the map $\kappa_m^{-1} \circ w_\varphi \circ \delta_\varphi$ agrees with the map*

$$\mathcal{J}'(K)/\varphi\mathcal{J}(K) \to L^*/L^{*m} \tag{6.35}$$

$$D \mapsto (F_1(D), \ldots, F_n(D)). \tag{6.36}$$

Proof. We first show that it suffices to use the m-Weil pairing instead of the φ-Weil pairing. Let $D \in \mathcal{J}'[m]$ and $E \in \mathcal{J}'[\varphi'] \subseteq \mathcal{J}'[m]$. Compatibility of the Weil pairing implies that $e_m(D, E) = e_\varphi(\varphi'(D), E)$; that is, the following diagram commutes:

$$\begin{array}{ccc} \mathcal{J}'[m] \times \mathcal{J}'[\varphi'] & & \\ \Big\downarrow{\scriptstyle \varphi' \times \mathrm{id}} & \overset{e_m}{\searrow} & \\ & & \mu_m \\ & \underset{e_\varphi}{\nearrow} & \\ \mathcal{J}[\varphi] \times \mathcal{J}'[\varphi'] & & \end{array} \tag{6.37}$$

Define the map $w_m \colon \mathcal{J}'[m] \to \mu_m(L')$ by $D \mapsto (e_m(D, D_1), \ldots, e_m(D, D_n))$. Thus $w_\varphi(\varphi'(D)) = w_m(D)$ for all $D \in \mathcal{J}'[m]$. Note that $\varphi'(D) \in \mathcal{J}[\varphi]$. Note also that w_m is not necessarily injective, since the $D_1, \ldots, D_n$ only span $\mathcal{J}'[\varphi']$, and not necessarily $\mathcal{J}'[m]$.

We can also apply the long exact sequence in Galois cohomology to the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J}'[m] & \longrightarrow & \mathcal{J}'(\overline{K}) & \xrightarrow{m} & \mathcal{J}(\overline{K}) & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle \varphi'} & & \Big\downarrow{\scriptstyle \varphi'} & & \Big\downarrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & \mathcal{J}[\varphi] & \longrightarrow & \mathcal{J}(\overline{K}) & \xrightarrow{\varphi} & \mathcal{J}(\overline{K}) & \longrightarrow & 0. \end{array} \tag{6.38}$$

The boundary maps of the long exact sequence, together with the commutative triangle that w_φ, w_m induce on cohomology fit into the following commutative diagram:

$$\begin{array}{ccccc} J'(K)/mJ'(K) & \xrightarrow{\delta_m} & H^1(K, J'[m]) & & \\ \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \varphi'} & \overset{w_m}{\searrow} & \\ & & & & H^1(K, \mu_m(L')) \xrightarrow{k} L^*/L^{*m} \\ & & & \underset{w_\varphi}{\nearrow} & \\ J'(K)/\varphi J(K) & \xrightarrow{\delta_\varphi} & H^1(K, J[\varphi]) & & \end{array} \tag{6.39}$$

We want to show that the composition of the lower maps equals the map $D \mapsto (F_1(D), \ldots, F_n(D))$. Since the diagram commutes, it suffices to show that the composition of the top maps also equals $D \mapsto (F_1(D), \ldots, F_n(D))$.

Let $D \in \operatorname{Div}^0 \mathcal{C}'$ represent an element of $\mathcal{J}'(K)/m\mathcal{J}'(K)$. Then $\delta_m(D)$ is the cocycle $\sigma \mapsto {}^\sigma E - E$, where $E \in \operatorname{Div}^0 \mathcal{C}'$ satisfies $mE \sim D$. Then $w_m \circ \delta_m(D)$ is represented by

$$\begin{aligned} \operatorname{Gal}(\bar{K}/K) &\to \mu_m(L') \\ \sigma &\mapsto (e_m({}^\sigma E - E, D_i))_{i=1}^n . \end{aligned} \tag{6.40}$$

By Proposition 2.2.7, we can compute $e_m({}^\sigma E - E, D_i)$ by finding functions with the correct divisors. Let $g \in K(E)(\mathcal{C}')$ have divisor $mE - D$. Then $\operatorname{div}({}^\sigma g/g) = {}^\sigma(mE - D) - (mE - D) = m{}^\sigma E - mE$. We also have $\operatorname{div} F_i = mD_i$ for each $i = 1, \ldots, n$, with $F_i \in K(D_i)(\mathcal{C}')$. Thus

$$e_m({}^\sigma E - E, D_i) = \frac{F_i({}^\sigma E - E)}{{}^\sigma g/g(D_i)}. \tag{6.41}$$

Hence

$$(w_m \circ \delta_m)(D)(\sigma) = \left(\frac{F_i({}^\sigma E - E)}{{}^\sigma g/g(D_i)} \right)_{i=1}^n . \tag{6.42}$$

Let $\beta = (F_i(E)/g(D_i))_{i=1}^n$. Using that ${}^\sigma F_i = F_{\bar{\sigma} i}$ and ${}^\sigma D_i = D_{\bar{\sigma} i}$, we then get

$${}^\sigma \beta = \left(\frac{{}^\sigma F_{\bar{\sigma}^{-1} i}}{{}^\sigma g({}^\sigma D_{\bar{\sigma}^{-1} i})} \right)_{i=1}^n = \left(\frac{F_i}{{}^\sigma g(D_i)} \right)_{i=1}^n \tag{6.43}$$

Hence $(w_m \circ \delta_m)(D)(\sigma) = \frac{\sigma\beta}{\beta}$. The Kummer isomorphism then gives

$$\begin{aligned} k \circ w_m \circ \delta_m(D) &\equiv \beta^m && (6.44)\\ &\equiv (F_i(E)^m / g(D_i)^m)_{i=1}^n && (6.45)\\ &\equiv (F_i(mE)/g(mD_i))_{i=1}^n && (6.46)\\ &\equiv (F_i(mE)/g(\operatorname{div} F_i))_{i=1}^n && (6.47)\\ &\equiv (F_i(mE)/F_i(\operatorname{div} g))_{i=1}^n && (6.48)\\ &\equiv (F_i(mE)/F_i(mE - D))_{i=1}^n && (6.49)\\ &\equiv (F_i(D))_{i=1}^n \pmod{L^{*m}}. && (6.50) \end{aligned}$$

□

Since $\kappa_m^{-1} \circ w_\varphi \circ \delta_\varphi$ agrees with $(F_1, \ldots, F_n)$, we now sometimes write F for the Cassels map.

Note that δ_φ is injective and κ_m is an isomorphism, so the composition $F = \kappa_m^{-1} \circ w_\varphi \circ \delta_\varphi$ is injective if w_φ is injective. Although $w_\varphi \colon J[\varphi] \to \mu_m(L')$ is injective, this does not imply that the induced map $H^1(K, J[\varphi]) \to H^1(K, \mu_m(L'))$ is injective. We investigate this in Section 6.8.

Following Schaefer, we have so far constructed the diagram (6.13). We can compute the group $\rho(\mathrm{Sel}^\varphi(\mathcal{J}/K))$ by computing generators for $\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)$ for each $s \in S$, and then computing the preimage under $\prod_s \beta_s$. Schaefer uses this diagram in [Sch98] to compute the Selmer group for a 2-descent when the curve is of the form $y^2 = f(x)$ with $\deg f = 5$.

We now use this theory to do a descent via $(4,4)$-isogeny, combining this descent with the Richelot isogeny.

6.5 Example: Richelot descent

We now illustrate this in the case of the Richelot descent. Let $f(x) = G_1(x)G_2(x)G_3(x)$ be a Richelot splitting of a degree 5 or 6 polynomial. Let $\mathcal{C} \colon y^2 = f(x)$ be the corresponding hyperelliptic curve, and let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. Let $\varphi \colon \mathcal{J} \to \mathcal{J}'$ be the Richelot isogeny corresponding to the splitting, and let $\varphi' \colon \mathcal{J}' \to \mathcal{J}$ be the dual isogeny. Then the isogenous curve is $\mathcal{C}' \colon y^2 = L_1(x)L_2(x)L_3(x)$, where $L_i(x)$ are defined as in Theorem 5.7.4. Let $D_i = \langle L_i(x), 0\rangle$ for $i = 1, 2$. Then $\{D_1, D_2\}$ is a spanning set for $\mathcal{J}'[\varphi']$.

For each $i = 1, 2$, let $h_i(x) = L_i(x)$. Then $h_i(x)$ satisfies $\operatorname{div} h_i = 2D_i$ for $i = 1, 2$. Since the splittings are defined over K, the field of definition for each D_i is K. Thus $L' = \overline{K} \times \overline{K}$ and $L = K \times K$.

Proposition 6.5.1. *Let φ be the Richelot isogeny described above. Then the map*

$$w_\varphi \colon H^1(K, \mathcal{J}[\varphi](\overline{K}) \to H^1(K, \mu_2(L')) \tag{6.51}$$

is injective.

Proof. In this case w_φ is the map

$$\mathcal{J}[\varphi](\overline{K}) \xrightarrow{w_\varphi} \mu_2(L') \tag{6.52}$$

$$D \mapsto (e_\varphi(D, D_1), e_\varphi(D, D_2)). \tag{6.53}$$

But $\mu_2(L') \cong \mu_2(K)^2$, since D_1, D_2 are both fixed by G_K. Thus $\#\mu_2(L') = 4$. Also $\#\mathcal{J}[\varphi](\overline{K}) = 4$. Since w_φ is an injective map between finite groups of the same size, it is an isomorphism. Thus w_φ induces an isomorphism $H^1(K, \mathcal{J}[\varphi](\overline{K})) \xrightarrow{\sim} H^1(K, \mu_2(L'))$. □

Recall that $M^\varphi(\mathcal{J}/K)$ is defined as the group computed by Schaefer's descent method in Definition 6.4.1. Since w_φ is injective, the φ-Selmer group $\mathrm{Sel}^\varphi(\mathcal{J}/K)$ is isomorphic to $M^\varphi(\mathcal{J}/K)$. We can thus compute $\mathrm{Sel}^\varphi(\mathcal{J}/K)$ using the following diagram

$$\begin{array}{ccc} \mathcal{J}'(K)/\varphi\mathcal{J}(K) & \xrightarrow{h_1 \times h_2} & K(S,2) \times K(S,2) \\ \downarrow{\scriptstyle \prod_{s\in S} \alpha_s} & & \downarrow{\scriptstyle \prod_{s\in S} \gamma_s} \\ \prod_{s\in S} \mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s) & \xrightarrow{h_1 \times h_2} & \prod_{s\in S} \frac{K_s^*}{K_s^{*2}} \times \frac{K_s^*}{K_s^{*2}} \end{array} \tag{6.54}$$

Remark 6.5.2. *Recall we require that $\mathcal{C}(K) \neq \emptyset$ to satisfy the assumption that every point in $\mathcal{J}(K)$ is represented by a G_K-invariant divisor (as in Section 6.2). This holds if $\deg f = 5$ or if $f(x)$ is monic.*

6.6 Higher descents

This section is motivated by the following proposition, which we adapted from the version for elliptic curves given by Silverman in [Sil09, Chapter 10] (compare also [Fis16]).

Proposition 6.6.1. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a sequence of isogenies. The following diagram commutes and has exact rows:*

$$\begin{array}{ccccccccc} \mathcal{J}_1(K) & \xrightarrow{\varphi_2\varphi_1} & \mathcal{J}_3(K) & \xrightarrow{\delta_{21}} & \mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K) & \xrightarrow{\varepsilon_{21}} & Ш(\mathcal{J}_1/K)[\varphi_2\varphi_1] & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_1} & & \\ \mathcal{J}_2(K) & \xrightarrow{\varphi_2} & \mathcal{J}_3(K) & \xrightarrow{\delta_2} & \mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K) & \xrightarrow{\varepsilon_2} & Ш(\mathcal{J}_2/K)[\varphi_2] & \longrightarrow & 0. \end{array} \tag{6.55}$$

Thus the following sequence is exact:

$$0 \to \mathcal{J}_3(K)/\varphi_2\mathcal{J}_2(K) \xrightarrow{\delta_2} \varphi_1\left(\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)\right) \xrightarrow{\varepsilon_2} \varphi_1\left(Ш(\mathcal{J}_1/K)[\varphi_2\varphi_1]\right) \to 0. \tag{6.56}$$

Proof. The previous section applied to the isogenies $\varphi_2\varphi_1$ and φ_2 show that the rows of (6.55) are exact. The columns come by functoriality and because the diagram below commutes:

$$\begin{array}{ccc} \mathcal{J}_1(\overline{K}) & \xrightarrow{\varphi_2\varphi_1} & \mathcal{J}_3(\overline{K}) \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \mathrm{id}} \\ \mathcal{J}_2(\overline{K}) & \xrightarrow{\varphi_2} & \mathcal{J}_3(\overline{K}). \end{array} \tag{6.57}$$

Lemma 6.6.2, below, shows that (6.56) is exact. □

Lemma 6.6.2. *Suppose the following diagram commutes and has exact rows*

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \longrightarrow & 0. \end{array} \tag{6.58}$$

If β is surjective, then the following sequence is exact

$$A' \xrightarrow{f'} B' \xrightarrow{g'} \gamma(C) \xrightarrow{h'} \delta(D) \to 0. \tag{6.59}$$

Proof. First note that the codomains of each map in (6.59) are valid. Indeed, $g'(B') \subseteq \gamma(C)$, since if $b' \in B'$, then $b' = g(b)$ for some $b \in B$, and thus $g'(b') = g'\beta(b) = \gamma g(b) \in \gamma(C)$. Similarly, if $\gamma(c) \in \gamma(C)$, then $h'\gamma(c) = \delta h(c) \in \delta(D)$.

Exactness of (6.59) at B' follows from exactness of the lower row of (6.58).

Consider the sequence

$$\beta(B) \xrightarrow{g'} \gamma(C) \xrightarrow{h'} \delta(D) \to 0. \tag{6.60}$$

We want to show h' is surjective and $\ker h' = \operatorname{im} g'$. Suppose $\delta(d) \in \delta(D)$. Then there is $c \in C$ such that $g(c) = d$. Hence $h'(\gamma(c)) = \delta(g(c))$, so h' is surjective. We still have $h'g' = 0$, so it remains to show that $\ker h' \subseteq \operatorname{im} g'$. If $h'(\gamma(c)) = 0$, then $\gamma(c) = g'(b')$ for some $b' \in B' = \beta(B)$ (since β is surjective). □

The following conjecture is well-known in number theory.

Conjecture 6.6.3. *Let $\mathcal{J}/K$ be the Jacobian of a smooth curve over a number field K. Then $Ш(\mathcal{J}/K)$ is finite.*

If $Ш(\mathcal{J}/K)$ is finite, as conjectured for Jacobians over number fields, then there is a natural number n such that for all $i \geq n$, we have $Ш(\mathcal{J}/K)[m^i] = Ш(\mathcal{J}/K)[m^n]$. With $\varphi_1 = [m^n], \varphi_2 = [m]$, the third term in (6.56) is

$$[m^n]Ш(\mathcal{J}/K)[m^{n+1}] = [m^n]Ш(\mathcal{J}/K)[m^n] = 0. \tag{6.61}$$

In this case, the first map in (6.56) is an isomorphism, so the rank bound from $\varphi_1\left(\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)\right)$ is sharp.

The rank bound from $\varphi_1\left(\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)\right)$ is at least as good as the bound from $\mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K)$; if it is better, then we have found nontrivial elements of $Ш(\mathcal{J}_2/K)[\varphi_2]$.

6.6.1 Technique to find $Ш(\mathcal{J}_2/K)[\varphi_2]$

Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a sequence of isogenies as in the previous section. As usual, let M^φ denote the subgroup of $L(S, m)$ computed by the above algorithm (see Definition 6.4.1), where φ is either $\varphi_2\varphi_1$ or φ_2. We have seen that Sel^φ surjects onto M^φ, but that the kernel can be nontrivial. The following proposition shows how we can still get some information in this case (see [Fis16] for a similar idea in the case of elliptic curves).

Proposition 6.6.4. *Let φ_1, φ_2 be a sequence of isogenies. We have the following commutative diagram with exact rows:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker\rho_{\varphi_2\varphi_1} & \longrightarrow & \mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K) & \xrightarrow{\rho_{\varphi_2\varphi_1}} & M^{\varphi_2\varphi_1} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle q} & & \\ 1 & \longrightarrow & \ker\rho_{\varphi_2} & \longrightarrow & \mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K) & \xrightarrow{\rho_{\varphi_2}} & M^{\varphi_2} & \longrightarrow & 1. \end{array} \tag{6.62}$$

We have

$$\frac{\#\,\mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K)}{\#\varphi_1\,\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)} = \frac{\#Ш(\mathcal{J}_2/K)[\varphi_2]}{\#\varphi_1 Ш(\mathcal{J}_1/K)[\varphi_2\varphi_1]} \geq \frac{\#M^{\varphi_2}}{\#qM^{\varphi_2\varphi_1}}. \tag{6.63}$$

Proof. Recall the exact sequences

$$0 \to \mathcal{J}_3(K)/\varphi_2\mathcal{J}_2(K) \xrightarrow{\delta_2} \mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K) \xrightarrow{\varepsilon_2} Ш(\mathcal{J}_1/K)[\varphi_2] \to 0 \tag{6.64}$$

and

$$0 \to \mathcal{J}_3(K)/\varphi_2\mathcal{J}_2(K) \xrightarrow{\delta_2} \varphi_1\left(\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)\right) \xrightarrow{\varepsilon_2} \varphi_1\left(Ш(\mathcal{J}_1/K)[\varphi_2\varphi_1]\right) \to 0 \quad (6.65)$$

from Proposition 6.6.1. The alternating product of the sizes of the groups is 1 for both sequences. Dividing the two alternating products, we arrive at the first equation.

For the inequality, apply the snake lemma to the diagram, which gives a long exact sequence ending with the terms

$$\frac{\mathrm{Sel}^{\varphi_2}(\mathcal{J}_2/K)}{\varphi_1\,\mathrm{Sel}^{\varphi_2\varphi_1}(\mathcal{J}_1/K)} \to \frac{M^{\varphi_2}}{qM^{\varphi_2\varphi_1}} \to 0. \quad (6.66)$$

Consequently, the first term in (6.66) surjects onto the second, giving the inequality. □

Thus, if $M^{\varphi_2}/qM^{\varphi_2\varphi_1}$ is nontrivial, then so is $Ш(\mathcal{J}_2/K)[\varphi_2]$.

6.7 Comparing $(4,4)$-isogeny and Richelot isogeny

We now combine the $(4,4)$-isogeny descent and Richelot descent on the same diagram, as motivated in Section 6.6. We aim to find examples where a Richelot descent does not give a sharp bound on the rank and a $(4,4)$-descent gives a sharper bound.

Proposition 6.7.1. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a $(4,4)$-isogeny, with $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ and φ_1, φ_2 all defined over a number field K. Suppose that $D_1, \ldots, D_n \in \mathcal{J}_3[\varphi_1'\varphi_2']$ are a G_K-stable set that spans $\mathcal{J}_3[\varphi_1'\varphi_2']$. Let L' be the $\overline{K}$-algebra corresponding to $D_1, \ldots, D_n$ as in Section 6.4.1, and define the maps $w_{\varphi_2\varphi_1}\colon \mathcal{J}_1[\varphi_2\varphi_1](\overline{K}) \to \mu_4(L')$ and $w_{\varphi_2}\colon \mathcal{J}_2[\varphi_2](\overline{K}) \to \mu_2(L')$ as in Section 6.4.3, using $D_1, \ldots, D_n$ and $2D_1, \ldots, 2D_n$, respectively. Then the following diagram of G_K-module homomorphisms commutes and has exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J}_1[\varphi_2\varphi_1](\overline{K}) & \xrightarrow{w_{\varphi_2\varphi_1}} & \mu_4(L') & \xrightarrow{q_4} & \mathrm{coker}_4 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle .2} & & \downarrow{\scriptstyle .2} & & \\ 0 & \longrightarrow & \mathcal{J}_2[\varphi_2](\overline{K}) & \xrightarrow{w_{\varphi_2}} & \mu_2(L') & \xrightarrow{q_2} & \mathrm{coker}_2 & \longrightarrow & 1 \end{array} \quad (6.67)$$

where q_4 and q_2 are the cokernels of the first maps.

Proof. We take the G_K-action on L' corresponding to $D_1, \ldots, D_n$ as explained in Section 6.4.1. This defines the G_K-action on $\mu_4(L')$, $\mu_2(L')$ and the cokernels.

Since $D_1, \ldots, D_n$ spans $\mathcal{J}_3[\varphi_1'\varphi_2']$ and is G_K invariant as a set, then $2D_1, \ldots, 2D_n$ spans $\mathcal{J}_3[\varphi_2']$ and is G_K invariant as a set also. Indeed, $2\mathcal{J}_3[\varphi_1'\varphi_2'] \subseteq \mathcal{J}_3[\varphi_2']$ and they are both order 4, so $\mathcal{J}_3[\varphi_2'] = 2\mathcal{J}_3[\varphi_1'\varphi_2']$.

The maps $w_{\varphi_2\varphi_1}$ and w_{φ_2} are G_K-equivariant: if $D \in \mathcal{J}_1[\varphi_2\varphi_1](\overline{K})$ and $\sigma \in G_K$, then ${}^{\sigma}w_{\varphi_2\varphi_1}(D) = w_{\varphi_2\varphi_1}({}^{\sigma}D)$ by Proposition 6.4.8. If $D \in \mathcal{J}_2[\varphi_2](\overline{K})$ and $\sigma \in G_K$, then we have

$$\begin{aligned}
{}^{\sigma}w_{\varphi_2}(D) &= {}^{\sigma}\left(e_{\varphi_2}(D, 2D_i)\right)_{i=1}^{4} && (6.68)\\
&= \left({}^{\sigma}e_{\varphi_2}(D, 2D_{\bar{\sigma}^{-1}i})\right)_{i=1}^{4} && (6.69)\\
&= \left(e_{\varphi_2}({}^{\sigma}D, {}^{\sigma}2D_{\bar{\sigma}^{-1}i})\right)_{i=1}^{4} && (6.70)\\
&= \left(e_{\varphi_2}({}^{\sigma}D, 2D_i)\right)_{i=1}^{4} && (6.71)\\
&= w_{\varphi_2}({}^{\sigma}D). && (6.72)
\end{aligned}$$

Compatibility of the Weil pairing shows that the left square commutes:

$$e_{\varphi_2}(\varphi_1(D), 2D_i) = e_{\varphi_2\varphi_1}(D, 2D_i) = e_{\varphi_2\varphi_1}(D, D_i)^2. \tag{6.73}$$

The vertical map $\cdot^2 \colon \mu_4(L') \to \mu_2(L')$ is a G_K-module homomorphism since we used the same G_K-action on both modules.

The maps $w_{\varphi_2\varphi_1}$ and w_{φ_2} are both injective, since the Weil pairing is nondegenerate and since $D_1, \ldots D_n$ spans $\mathcal{J}_3[\varphi_1'\varphi_2']$ and $2D_1, \ldots 2D_n$ spans $\mathcal{J}_3[\varphi_2']$. Taking cokernels thus makes the rows exact. The whole diagram commutes since the left square commutes and cokernels are functorial. □

Remark 6.7.2. *We use the same G_K-action on L' in the bottom row of the diagram as for the top row. That is, we use the G_K-action from $D_1, \ldots, D_n$ rather than $2D_1, \ldots, 2D_n$. The field of definition $K(2D_i)$ can be a strict subfield of $K(D_i)$, but using the same L' makes the homomorphisms in the diagram G_K-equivariant. Unfortunately, using the same L' can mean that the lower row of the commutative diagram is not injective, even when it would have been injective with the L' defined for $2D_1, \ldots, 2D_n$.*

The long exact sequence attached to this commutative diagram gives the following diagram with exact rows

$$\begin{array}{ccccc}
\operatorname{coker}_4^{G_K} & \xrightarrow{\delta_{\varphi_2\varphi_1}} & H^1(K, \mathcal{J}_1[\varphi_2\varphi_1](\overline{K})) & \xrightarrow{w_{\varphi_2\varphi_1}} & H^1(K, \mu_4(L')) \\
\downarrow{\scriptstyle \cdot^2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \cdot^2} \\
\operatorname{coker}_2^{G_K} & \xrightarrow{\delta_{\varphi_2}} & H^1(K, \mathcal{J}_2[\varphi_2](\overline{K})) & \xrightarrow{w_{\varphi_2}} & H^1(K, \mu_2(L'))
\end{array} \tag{6.74}$$

Proposition 6.7.3. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be two Richelot isogenies whose composition is a $(4,4)$-isogeny. The following diagram commutes:*

$$\begin{array}{ccccccc} \frac{\mathcal{J}_3(K)}{\varphi_2\varphi_1\mathcal{J}_1(K)} & \xhookrightarrow{\delta_4} & H^1(K, \mathcal{J}_1[\varphi_2\varphi_1]) & \xrightarrow{w_{\varphi_2\varphi_1}} & H^1(K, \mu_4(L')) & \xrightarrow{\kappa_4} & L^*/L^{*4} \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle .2} & & \downarrow{\scriptstyle \mathrm{id}} \\ \frac{\mathcal{J}_3(K)}{\varphi_2\mathcal{J}_2(K)} & \xhookrightarrow{\delta_2} & H^1(K, \mathcal{J}_2[\varphi_2]) & \xrightarrow{w_{\varphi_2}} & H^1(K, \mu_2(L')) & \xrightarrow{\kappa_2} & L^*/L^{*2} \end{array} \tag{6.75}$$

Proof. Recall the definition of L' and its G_K-action from Proposition 6.7.1. We have already shown that the middle square commutes. It remains to show that the left and right hand squares commute.

The left hand square comes from the following diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J}_1[\varphi_2\varphi_1] & \longrightarrow & \mathcal{J}_1(\overline{K}) & \xrightarrow{\varphi_2\varphi_1} & \mathcal{J}_3(\overline{K}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathcal{J}_2[\varphi_2] & \longrightarrow & \mathcal{J}_2(\overline{K}) & \xrightarrow{\varphi_2} & \mathcal{J}_3(\overline{K}) & \longrightarrow & 0. \end{array} \tag{6.76}$$

The long exact sequence in Galois cohomology attached to this diagram gives the following commuting square

$$\begin{array}{ccc} \frac{\mathcal{J}_3(K)}{\varphi_2\varphi_1\mathcal{J}_1(K)} & \xhookrightarrow{\delta_4} & H^1(K, \mathcal{J}_1[\varphi_2\varphi_1]) \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi_1} \\ \frac{\mathcal{J}_3(K)}{\varphi_2\mathcal{J}_2(K)} & \xhookrightarrow{\delta_2} & H^1(K, \mathcal{J}_2[\varphi_2]) \end{array} \tag{6.77}$$

where the horizontal rows come from the connecting homomorphism, and we have taken the quotient by the image of the last map on H^0 terms. The G_K-action on all terms here is induced by the G_K-action on the Jacobians and their torsion subgroups, which is not affected by our modified G_K-action on L'.

Let g be the quotient map $L^*/L^{*4} \to L^*/L^{*2}$, given by $\beta L^{*4} \mapsto \beta L^{*2}$. We now show the right hand square commutes:

$$\begin{array}{ccc} H^1(K, \mu_4(L')) & \xrightarrow{\kappa_4} & L^*/L^{*4} \\ \downarrow{\scriptstyle .2} & & \downarrow{\scriptstyle g} \\ H^1(K, \mu_2(L_2')) & \xrightarrow{\kappa_2} & L^*/L^{*2}. \end{array} \tag{6.78}$$

Let $\xi\colon G_K \to \mu_4(L') \in H^1(K, \mu_4(L'))$. Recall that if $\beta \in L^*/L^{*m}$, then $\kappa_m^{-1}(\beta)(\sigma) = \frac{{}^\sigma\gamma}{\gamma}$ where $\gamma \in L'$ satisfies $\gamma^m = \beta$. Consequently, $\kappa_4^{-1}(\beta)(\sigma) = \frac{{}^\sigma\gamma}{\gamma}$ for some $\gamma \in L'$ with $\gamma^4 = \beta$. But also ξ^2 is the map $\xi^2\colon G_K \xrightarrow{\xi} \mu_4(L') \xrightarrow{.^2} \mu_2(L')$. So if $\kappa_4(\xi) = \beta$, then

$$\xi^2(\sigma) = \left(\frac{{}^\sigma\gamma}{\gamma}\right)^2 = \frac{{}^\sigma\gamma^2}{\gamma^2}. \tag{6.79}$$

Thus $\kappa_2(\xi^2) = (\gamma^2)^2 = \beta L^{*2}$, which equals $g(\kappa_4(\xi))$. Thus (6.78) commutes. □

6.8 The kernel of w_φ

The maps $w_{\varphi_2\varphi_1}$ and w_{φ_2} can have nontrivial kernels. Let φ be either $\varphi_2\varphi_1$ or φ_2, and let m be either 4 or 2, respectively. The long exact sequence in Galois cohomology associated to the short exact sequence (6.67) has the terms

$$\mu_m(L')^{G_K} \xrightarrow{q_m} \operatorname{coker}_m^{G_K} \xrightarrow{\delta_\varphi} H^1(K, \mathcal{J}[\varphi]) \xrightarrow{w_\varphi} H^1(K, \mu_m(L')). \tag{6.80}$$

Exactness at $H^1(K, \mathcal{J}[\varphi])$ implies $\ker w_\varphi = \delta_\varphi(\operatorname{coker}_m^{G_K})$. Thus

$$\ker w_\varphi \cong \operatorname{coker}_m^{G_K} / \ker \delta_\varphi \tag{6.81}$$

$$= \operatorname{coker}_m^{G_K} / q_m(\mu_m(L')^{G_K}). \tag{6.82}$$

Hence we can explicitly compute a group isomorphic to $\ker w_\varphi$. Schaefer uses a similar idea in [Sch98].

Let D be a divisor representing an element of a Jacobian $\mathcal{J}/K$. We say D satisfies condition (†) if D is defined over a quadratic extension of K and conjugate to $-D$.

For the next proposition, recall the G_K-action on L' as explained in Remark 6.7.2.

Proposition 6.8.1. *Let D_1, D_2 be generators for $\mathcal{J}_3[\varphi_1'\varphi_2']$.*

(i) If D_1 and D_2 are defined over K, then $\operatorname{coker}_2^{G_K}$ is trivial;

(ii) if D_1 is defined over K, and D_2 satisfies (†), then we use the spanning set $D_1, D_2, -D_2$; in this case, $\#\ker w_{\varphi_2} = 2$;

(iii) if both D_1, D_2 satisfy (†), then we use the spanning set $D_1, -D_1, D_2, -D_2$; in this case $\#\ker w_{\varphi_2} = 4$.

Proof. We first show (i). Suppose that D_1 and D_2 are defined over K. Then we define L' using D_1 and D_2. The Galois action on $\mu_2(L')$ is trivial, since D_1 and D_2 are fixed by G_K, and so $\mu_2(L')$ is also fixed by the Galois action. Moreover, $\operatorname{im} w_{\varphi_2} \colon \mathcal{J}_2[\varphi_2] \to \mu_2(L')$ is an injective map between finite groups of the same size, and so is also surjective. Thus $\operatorname{coker}_2 = \{1\}$, so $\ker w_{\varphi_2}$, which is a quotient of $\operatorname{coker}_2^{G_K}$, is also trivial.

Next consider (ii). Suppose D_1 is K-rational, but D_2 satisfies (†); thus D_2 is defined over a quadratic extension and is conjugate to $-D_2$ over this extension. In this case, we use $D_1, D_2, -D_2$ to define the K-algebra L' and $w_{\varphi_2\varphi_1}$ and we use $2D_1, 2D_2, -2D_2$ to define w_{φ_2}.

If $D \in \mathcal{J}_2[\varphi_2]$, then $w_{\varphi_2}(D) = (e_{\varphi_2}(D, 2D_1), e_{\varphi_2}(D, 2D_2), e_{\varphi_2}(D, -2D_2))$. Since $2D_i = -2D_i$, we have $\operatorname{im} w_{\varphi_2} \subseteq \Delta$, where $\Delta = \{(a, b, b) \colon a, b \in \mu_2(L')\}$. Since w_{φ_2} is injective, and $\#\mathcal{J}_2[\varphi_2] = 4 = \#\Delta$, we have $\operatorname{im} w_{\varphi_2} = \Delta$. Also, since $\mu_2(K)$ is fixed by G_K, $\mu_2(L')^{G_K}$ is the subset of elements fixed under all permutations $\bar{\sigma}$ for $\sigma \in G_K$. Thus $\mu_2(L')^{G_K} = \Delta$.

Elements of coker_2 are thus of the form $\alpha\Delta$ for $\alpha \in \mu_2(L')$. Since ${}^{\sigma}\Delta = \Delta$, the G_K-action is ${}^{\sigma}(\alpha\Delta) = {}^{\sigma}\alpha\Delta$. Now consider $\operatorname{coker}^{G_K}$. Let $\alpha\Delta = (a_1, a_2, a_3)\Delta \in \operatorname{coker}_2$. Then $\alpha = (1, 1, a)\Delta$ for some $a \in \mu_2(K)$. Note that G_K fixes $\mu_2(K)$, so the action of $\sigma \in G_K$ on α is by permuting the elements.

Let $\sigma \in G_K$. Then ${}^{\sigma}\alpha\Delta = \alpha\Delta$ if and only if ${}^{\sigma}\alpha/\alpha \in \Delta$. Thus consider when ${}^{\sigma}(1, 1, a)/(1, 1, a) \in \Delta$. There are two cases to consider: ${}^{\sigma}D_2 = D_2$ or ${}^{\sigma}D_2 = -D_2$. In the first case, we have $(1, 1, a)/(1, 1, a) = (1, 1, 1) \in \Delta$. In the second case, we have $(1, 1, a)/(1, a, 1) = (1, a, a) \in \Delta$. Both of these hold with $a = \pm 1$. Hence $\operatorname{coker}_2^{G_K}$ is of order 2, generated by $(1, 1, -1)\Delta$. Note that $\ker w_{\varphi_2} \cong \operatorname{coker}_2^{G_K} / q(\mu_2(L')^{G_K}) = \operatorname{coker}_2^{G_K} / q(\Delta) = \operatorname{coker}_2^{G_K}$, since $q(\Delta)$ maps to zero in $\operatorname{coker}_2^{G_K}$.

Finally we show (iii). Suppose both D_1, D_2 satisfy (†); then we use $D_1, -D_1, D_2, -D_2$ to define L' and $w_{\varphi_2\varphi_1}$ and we use $2D_1, -2D_1, 2D_2, -2D_2$ to define w_{φ_2}. Let $\Delta = \{(a, a, b, b) \colon a, b \in \mu_2(K)\}$. We find similarly that $\operatorname{coker}_2^{G_K}$ is of order 4, generated by $(1, -1, 1, 1)\Delta$ and $(1, 1, 1, -1)\Delta$. □

See Section 5.9.3 for an explicit family of curves admitting a $(4, 4)$-isogeny where both generators are defined over K.

6.9 Explicit explanation of computations

In this section we explain how to perform all the calculations described above.

6.9.1 Some exact sequences

The following lemma is a mild generalisation of Proposition 2.6 in [Sch98]. Recall that if $f \colon A \to B$ is a homomorphism of groups, then we write $A[f]$ to denote the kernel $\ker f$.

Lemma 6.9.1. *Let R be a ring, and let $A \xrightarrow{f} B \xrightarrow{g} C$ be homomorphisms of R-modules. The following is an exact sequence*

$$0 \to \frac{B[g]}{f(A[gf])} \to \frac{B}{f(A)} \xrightarrow{g} \frac{C}{gf(A)} \to \frac{C}{g(B)} \to 0. \tag{6.83}$$

Proof. Consider the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & f(A[gf]) & \longrightarrow & B[g] & \longrightarrow & \frac{B[g]}{f(A[gf])} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & f(A) & \longrightarrow & B & \longrightarrow & \frac{B}{f(A)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \\
0 & \longrightarrow & gf(A) & \longrightarrow & C & \longrightarrow & \frac{C}{gf(A)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & \frac{C}{g(B)} & \longrightarrow & \frac{C}{g(B)} & \longrightarrow & 0
\end{array} \tag{6.84}$$

The middle two rows are exact and commute. Applying the snake lemma gives the top and bottom rows. The top row consists of the kernels of the vertical maps in the middle two rows and the bottom row consists of the cokernels.

We first compute the kernels and cokernels of the vertical maps. The left vertical map, $g\colon f(A) \to gf(A)$, is surjective. Its kernel is $\{f(a)\colon a \in A, gf(a) = 0\} = f(A[gf])$.

The middle vertical map $g\colon B \to C$ is the easiest. Its kernel is $B[g]$ and its cokernel is $C/g(B)$.

Consider now the right vertical map, $g\colon B/f(A) \to C/gf(A)$. Its kernel is $\{b + f(A)\colon g(b) \in gf(A)\} = \frac{B[g]+f(A)}{f(A)}$. Indeed, if $g(b) \in gf(A)$, then $g(b) = gf(a)$ for some $a \in A$, and hence $b = (b - f(a)) + f(a) \in B[g] + f(A)$. By the second isomorphism theorem, $\frac{B[g]+f(A)}{f(A)} = \frac{B[g]}{B[g]\cap f(A)} = \frac{B[g]}{f(A[gf])}$, since $B[g] \cap f(A) = \{f(a)\colon a \in A, gf(a) = 0\} = f(A[gf])$. The cokernel of $B/f(A) \to C/gf(A)$ is by definition $\frac{C/gf(A)}{g(B/f(A))} = \frac{C/gf(A)}{g(B)/gf(A)}$. By the third isomorphism theorem, this is isomorphic to $\frac{C}{g(B)}$.

The snake lemma implies that the right vertical column is exact. Moreover, the first map in the column is injective and the last map in the column is surjective since the first map is the inclusion of the kernel of the middle map and the last map is the map to the cokernel. □

Remark 6.9.2. *Note that $f(A[gf]) \cong \frac{A[gf]}{A[f]}$, using the first isomorphism theorem on the map $f\colon A[gf] \to f(A[gf])$. Its kernel is $\{a \in A[gf]\colon f(a) = 0\} = A[f]$. Thus $\#\frac{B[g]}{f(A[gf])} = \frac{\#B[g]\cdot\#A[f]}{\#A[gf]}$.*

Corollary 6.9.3. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a sequence of isogenies of Jacobians of curves defined over a field K. Then the following sequence is exact:*

$$0 \to \frac{\mathcal{J}_2[\varphi_2](K)}{\varphi_1(\mathcal{J}_1[\varphi_2\varphi_1](K))} \to \frac{\mathcal{J}_2(K)}{\varphi_1\mathcal{J}_1(K)} \xrightarrow{\varphi_2} \frac{\mathcal{J}_3(K)}{\varphi_2\varphi_1\mathcal{J}_1(K)} \to \frac{\mathcal{J}_3(K)}{\varphi_2\mathcal{J}_2(K)} \to 0. \tag{6.85}$$

Suppose further that the isogenies are $\mathcal{J} \xrightarrow{\varphi} \mathcal{J}' \xrightarrow{\varphi'} \mathcal{J}$*, where* $\varphi' \circ \varphi = [m]\colon \mathcal{J} \to \mathcal{J}$*. Then*

$$\#\frac{\mathcal{J}(K)}{m\mathcal{J}(K)} \cdot \frac{\#\mathcal{J}'[\varphi'](K) \cdot \#\mathcal{J}[\varphi](K)}{\#\mathcal{J}[m](K)} = \#\frac{\mathcal{J}'(K)}{\varphi\mathcal{J}(K)} \cdot \#\frac{\mathcal{J}(K)}{\varphi'\mathcal{J}'(K)}. \tag{6.86}$$

Proof. The exact sequence follows from Lemma 6.9.1. The statement about sizes uses Remark 6.9.2, and also that the alternating product of sizes of groups in an exact sequence of finite groups is 1. □

This corollary shows how to combine two descents via isogeny to get a rank bound. Let $\mathcal{J}(K) \cong \mathcal{J}_{\mathrm{tors}}(K) \times \mathbb{Z}^r$, where $\mathcal{J}_{\mathrm{tors}}(K)$ denotes the torsion subgroup of $\mathcal{J}(K)$. Then for any $m \geq 2$, we find

$$\mathcal{J}(K)/m\mathcal{J}(K) \cong \mathcal{J}_{\mathrm{tors}}(K)/m\mathcal{J}_{\mathrm{tors}}(K) \times (\mathbb{Z}/m\mathbb{Z})^r\,. \tag{6.87}$$

A bound $\#\frac{\mathcal{J}(K)}{m\mathcal{J}(K)} \leq N$ thus gives a bound

$$m^r \leq N/\#\frac{\mathcal{J}_{\mathrm{tors}}(K)}{m\mathcal{J}_{\mathrm{tors}}(K)}, \tag{6.88}$$

which bounds the rank, r.

6.9.2 Generating local points

Let $\varphi\colon \mathcal{J} \to \mathcal{J}'$ be an isogeny. To compute the image of the φ-Selmer group in L^*/L^{*m}, we need to compute the preimage under β_s of $F(\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s))$ for each $s \in S$. Thus we need to generate $\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)$. The standard approach is to compute the size of this group and search for local points in $\mathcal{J}'(K_s)$ until we reach this size ([CF96]). In practice we actually compute $\#\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s) \cdot \#\mathcal{J}(K_s)/\varphi'\mathcal{J}'(K_s)$ and search for local points in both groups simultaneously until we reach this size.

The size of $\mathcal{J}'(K)/\varphi\mathcal{J}(K)$

Remark 6.9.4. *If* K *is a local field, then* $J(K)$ *is not finitely generated. For example, if* $K = \mathbb{C}$*, and* $\mathcal{J}$ *is an elliptic curve, then* $\mathcal{J}(K)$ *is isomorphic to a complex torus.*

Proposition 6.9.5 ([CF96], Theorem 7.5.1)**.** *Let* $\mathcal{J}$ *be the Jacobian of a curve of genus* g *over a finite extension* K *of* $\mathbb{Q}_p$*. Let* $\mathfrak{m} = \{x \in \mathcal{O}_K\colon |x| < 1\}$ *be the maximal ideal of* K*. Let* n *be a positive integer. Then*

$$\#\frac{\mathcal{J}(K)}{n\mathcal{J}(K)} = \#\frac{\mathfrak{m}^g}{n\mathfrak{m}^g} \cdot \#\mathcal{J}[n](K). \tag{6.89}$$

Proof. Cassels and Flynn show that if K is a finite extension of $\mathbb{Q}_p$, then $\mathcal{J}(K)$ contains a subgroup H of finite index such that $H \cong \mathfrak{m}^g$ ([CF96, Theorem 7.5.1]). Now consider the snake lemma diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & \longrightarrow & \mathcal{J}[n](K) & \longrightarrow & \ker & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H & \longrightarrow & \mathcal{J}(K) & \longrightarrow & \mathcal{J}(K)/H & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\
0 & \longrightarrow & H & \longrightarrow & \mathcal{J}(K) & \longrightarrow & \mathcal{J}(K)/H & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H/nH & \longrightarrow & \mathcal{J}(K)/n\mathcal{J}(K) & \longrightarrow & \operatorname{coker} & & \\
 & & & & & & \downarrow & & \\
 & & & & & & 0 & &
\end{array} \tag{6.90}$$

where ker and coker are the kernel and cokernel of the vertical map $\mathcal{J}(K)/H \to \mathcal{J}(K)/H$ induced by multiplication by n on the Jacobian. Note that $[n]\colon H \to H$ is injective, since $H \cong \mathfrak{m}^g$. Since H is finite index in $\mathcal{J}(K)$, the right column is an exact sequence of finite groups; thus the alternating product of their sizes is 1, which shows that $\#\ker = \#\operatorname{coker}$. The snake lemma shows the sequence of finite groups

$$0 \to \mathcal{J}[n](K) \to \ker \to H/nH \to \mathcal{J}(K)/n\mathcal{J}(K) \to \operatorname{coker} \to 0 \tag{6.91}$$

is exact. The alternating product of their sizes is thus also 1, which gives the statement in the proposition. □

The following lemma is a standard fact about $\mathbb{Q}_p$, but we give it for completeness.

Lemma 6.9.6. *Let $K = \mathbb{Q}_p$ and let $\mathfrak{m}$ be its maximal ideal. Let n be a positive integer. Then*

$$\#\frac{\mathfrak{m}^g}{n\mathfrak{m}^g} = |n|_p^{-g}. \tag{6.92}$$

Proof. Since $\mathfrak{m}^g/n\mathfrak{m}^g = (\mathfrak{m}/n\mathfrak{m})^g$, it suffices to prove that $\#\mathfrak{m}/n\mathfrak{m} = |n|_p^{-1}$. Write $n = ap^r$ for some $r \geq 0$ and a with $p \nmid a$. Let $x \in \mathfrak{m} = p\mathbb{Z}_p$, so we can write

$$x = a_1 p + \cdots + a_r p^r + x' p^{r+1} \tag{6.93}$$

where each $a_i \in \{0, \dots, p-1\}$ and $x' \in \mathbb{Z}_p$. Since $p \nmid a$, we have $x'p^{r+1} = \frac{x'}{a}ap^{r+1} = \frac{x'}{a}pn \in pn\mathbb{Z}_p$. Thus

$$x - a_1 p - \cdots - a_r p^r \in np\mathbb{Z}_p = n\mathfrak{m}. \tag{6.94}$$

This shows that $\{a_1 p + \cdots a_r p^r + np\mathbb{Z}_p \colon a_i \in \{0, \dots, p-1\}\}$ is a set of coset representatives for $\mathfrak{m}/n\mathfrak{m}$. Thus $\#\mathfrak{m}/n\mathfrak{m} = p^r = |n|_p^{-1}$. □

Corollary 6.9.7. *Let $\varphi \colon \mathcal{J} \to \mathcal{J}'$ be an m-isogeny between Jacobians over a field K, with φ' defined as usual. Then*

$$\#\frac{\mathcal{J}'(K)}{\varphi\mathcal{J}(K)} \cdot \#\frac{\mathcal{J}(K)}{\varphi'\mathcal{J}'(K)} = \#\frac{\mathcal{J}(K)}{m\mathcal{J}(K)} \cdot \frac{\#\mathcal{J}'[\varphi'](K) \cdot \#\mathcal{J}[\varphi](K)}{\#\mathcal{J}[m](K)}. \tag{6.95}$$

If $K = \mathbb{Q}_p$ and the curves have genus g, then

$$\#\mathcal{J}(\mathbb{Q}_p)/\varphi'\mathcal{J}'(\mathbb{Q}_p) \cdot \#\mathcal{J}'(\mathbb{Q}_p)/\varphi\mathcal{J}(\mathbb{Q}_p) = \#\mathcal{J}(\mathbb{Q}_p)[\varphi] \cdot \#\mathcal{J}'(\mathbb{Q}_p)[\varphi'] \cdot |m|_p^{-g}. \tag{6.96}$$

Proof. The first follows from Corollary 6.9.3. The second follows by combining Proposition 6.9.5 with Lemma 6.9.6. □

Generators for Richelot isogenies Let $\varphi \colon \mathcal{J} \to \mathcal{J}'$ be a Richelot isogeny defined over a local field K_s. Cassels and Flynn give the following method to find generators for $\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)$ and $\mathcal{J}(K_s)/\varphi'\mathcal{J}'(K_s)$. Equation (6.96) gives the expected size of the product when $K_s = \mathbb{Q}_p$. We then simultaneously search for points in $\mathcal{J}'(K_s)/\varphi\mathcal{J}(K_s)$ and $\mathcal{J}(K_s)/\varphi'\mathcal{J}'(K_s)$ until we reach this expected size. It is easier to check whether points are independent in L_s^*/L_s^{*2} than in the quotient of Jacobians. Given points $P_1, \dots, P_m \in \mathcal{J}(K_s)$ and $Q_1, \dots, Q_n \in \mathcal{J}'(K_s)$, we thus compute

$$\#\langle F_s(P_1), \dots, F_s(P_m)\rangle \cdot \#\langle F_s'(Q_1), \dots, F_s'(Q_n)\rangle, \tag{6.97}$$

and, since the Richelot Cassels maps F_s, F_s' are injective, we can check if this equals the expected size.

Searching for local points For the Jacobian of a genus 2 curve, a simple method of searching for points is to first search for points on the Kummer surface and then check if the points lift to the Jacobian using Section 5.5. To search on the Kummer surface, we iterate over values z_0, z_1, z_2 of bounded height and check whether the Kummer equation $Q(z_0, z_1, z_2, \xi_3)$ is soluble for ξ_3 (where Q is the Kummer quartic from equation (4.36)).

Remark 6.9.8. *This is the method currently implemented in* MAGMA *for searching for points on a Jacobian of a genus 2 curve over $\mathbb{Q}$; we implement our own version in [Nic18] for $\mathbb{Q}_p$, since the version for local points in* MAGMA *doesn't appear to be accessible to the user.*

Generating local points for $(4,4)$-isogenies The above approach works well when the Cassels map $F\colon \mathcal{J}'(K)/\varphi\mathcal{J}(K) \to L^*/L^{*m}$ is injective. But when F is not injective, we can't compare sizes. If φ is a $(4,4)$-isogeny, then even when the kernel of φ is elementwise K-rational, the kernel of φ' won't be. We now explain our approach to generating $\mathcal{J}_3(K_s)/\varphi_2\varphi_1\mathcal{J}_1(K_s)$, which is one of our main contributions to make $(4,4)$-descent practical. The basic idea is to use the Richelot isogeny to generate enough points in $\mathcal{J}_3(K_s)/\varphi_2\mathcal{J}_2(K_s)$.

We first prove a lemma relating generators of groups in a short exact sequence.

Lemma 6.9.9. *Let $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of groups. Suppose that $c_1, \dots, c_n$ generate C and suppose that $a_1, \dots, a_m$ generate A. Let $c_1', \dots, c_n' \in B$ be such that $g(c_i') = c_i$ for each $i = 1, \dots, n$. Then $\{f(a_1), \dots, f(a_m), c_1', \dots, c_n'\}$ generates B.*

Proof. Let $b \in B$. Choose n_i such that $g(b) = \prod_i c_i^{n_i}$. Then $b\prod_i {c_i'}^{-n_i} \in \ker g = \operatorname{im} f$. Hence there are m_j such that $b\prod_i {c_i'}^{-n_i} = \prod_j a_j^{m_j}$. □

Proposition 6.9.10. *Let $\mathcal{J}_1 \xrightarrow{\varphi_1} \mathcal{J}_2 \xrightarrow{\varphi_2} \mathcal{J}_3$ be a composition of Richelot isogenies. The group $\mathcal{J}_3(K)/\varphi_2\varphi_1\mathcal{J}_1(K)$ is generated by $\mathcal{J}_3(K)/\varphi_2\mathcal{J}_2(K)$ and $\varphi_2\left(\mathcal{J}_2(K)/\varphi_1\mathcal{J}_1(K)\right)$.*

Proof. Apply Lemma 6.9.9 to the exact sequence in (6.85). We don't need to find preimages for the generators of $\mathcal{J}_3(K)/\varphi_2\mathcal{J}_2(K)$, since representatives for these already lie in $\mathcal{J}_3(K)$. □

We set up the diagram for Schaefer's descent with divisors E_1, E_2 that are K-rational and span $\mathcal{J}'[\varphi_2']$. The corresponding Cassels map is injective, as discussed in Section 6.5. Algorithm 6 computes generators for $\mathcal{J}_3(K)/\varphi_2\varphi_1\mathcal{J}_1(K)$.

Algorithm: Computing generators for $J_3(K)/\varphi_2\varphi_1 J(K)$
Data: Richelot isogenies φ_1, φ_2 such that $\varphi_2 \circ \varphi_1$ is a $(4,4)$-isogeny.
Result: Divisors that generate $J_3(K)/\varphi_2\varphi_1 J(K)$.
`LocalGeneratorsFourFour`
    Compute local generators D_i for $J_3(K)/\varphi_2 J_2(K)$
    Compute local generators E_j for $J_2(K)/\varphi_1 J(K)$
    Compute the images $\varphi_2(E_j)$ for each E_j
    return $D_i, \varphi_2(E_j)$
end

Algorithm 6: Computing generators for the $(4,4)$-isogeny

Remark 6.9.11. *In fact we compute each $\varphi_2(E_j)$ using the map induced by the Richelot isogeny on the Kummer surface, rather than the Richelot isogeny on Jacobians. Thus we find the image of each $\varphi_2(E_j)$ on the Kummer surface $\mathcal{K}_3$, and then lift it to the Jacobian $\mathcal{J}_3$. This gives two points on the Jacobian, of which one is $\varphi_2(E_j)$; since the two lifts are related by negation on $\mathcal{J}_3$, we can just choose one of them to be a generator.*

Generating local points for complete 4-descent We don't carry out a complete 4-descent in this thesis, but we note here that we can find generators for $\mathcal{J}(K)/4\mathcal{J}(K)$ given generators for $\mathcal{J}(K)/2\mathcal{J}(K)$. This would be useful for doing a complete 4-descent as we could generate all the local points just using a complete 2-descent, analogously to the idea above for generating the local points for a $(4,4)$-isogeny just using Richelot isogenies.

The following lemma shows that generators for $\mathcal{J}(K)/2\mathcal{J}(K)$ are also generators for $\mathcal{J}(K)/4\mathcal{J}(K)$.

Lemma 6.9.12. *Let A be an abelian group. Suppose that $a_1, \ldots, a_r$ generate A/mA for some integer $m \geq 2$. Then also $a_1, \ldots, a_r$ generate $A/m^n A$ for all $n \geq 1$.*

Proof. We prove this by induction, with the case $n = 1$ holding trivially. Let $n \geq 2$, and assume that $a_1, \ldots, a_r \in A$ generate $A/m^{n-1}A$. We want to show that $a_1, \ldots, a_r$ generate $A/m^n A$.

Let $b \in A$, and write $b \equiv u_1 a_1 + \cdots + u_r a_r \pmod{m^{n-1}A}$ for some $u_1, \ldots, u_r \in \mathbb{Z}$. Thus there exists $c \in A$ such that $b = u_1 a_1 + \cdots + u_r a_r + m^{n-1}c$. Then $c \equiv v_1 a_1 + \cdots v_r a_r \pmod{m^{n-1}A}$ for some $v_1, \ldots, v_r \in \mathbb{Z}$. Hence $mc \equiv mv_1 a_1 + \cdots + mv_r a_r \pmod{m^n A}$, and thus $b = (u_1 + mv_1)a_1 + \cdots + (u_r + mv_r)a_r + m^n d$, for some $d \in A$. Thus $a_1, \ldots, a_m$ still generate $A/m^n A$. □

6.9.3 Computing the functions h_i for 4-torsion points

Let $\mathcal{C}$ be the hyperelliptic curve $y^2 = f(x)$ over a field K where $\deg f = 6$ and let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. Let K' be an extension field of K; let D be a divisor on $\mathrm{Div}^0\,\mathcal{C}(K')$ representing a point in $\mathcal{J}[4](K')$. We now compute a function $h \in K'(\mathcal{C})$ such that $\mathrm{div}\, h = 4D$, where D is a 4-torsion point. When D is one of the generators D_1, D_2 of the kernel of a $(4,4)$-isogeny, the corresponding functions h_1, h_2 define the Cassels map (compare with Proposition 6.4.9).

In this section we use the notation $\langle a(x), b(x), d\rangle$ from Section 2.1.4.

We first need the following lemma, which we prove in Appendix C.

Lemma 6.9.13. *Let $D = \langle a(x), b(x), d\rangle$ be a nontrivial divisor on the genus 2 curve $y^2 = f(x)$ such that $2D \sim 0$. Then $b(x) \equiv 0 \pmod{a(x)}$ and $f(x) \equiv 0 \pmod{a(x)}$.*

Proposition 6.9.14. *Let $D = \langle a(x), b(x)\rangle$ represent an element of $\mathcal{J}[4](K')$, where $\deg a = 2$, and let T be a divisor representing the class $[2D]$. Write $T = \langle t(x), 0\rangle$ for some polynomial $t(x)$. Solve $e(x)b(x) \equiv 1 \pmod{a(x)^2}$. Let $H(x)$ be a representative for $\frac{1}{2}(b(x)+e(x)f(x)) \pmod{a(x)^2}$ of degree at most 3. Then $\mathrm{div}((y-H(x))^2/t(x)) = 4D$.*

Proof. Since $D = \langle a(x), b(x)\rangle$, we have $b(x)^2 - f(x) = \lambda a(x)g(x)$ for some $g(x)$.

Since $2[D] = [T]$, we have $2D + T \sim 0$. Riemann-Roch shows that $2D + T = \mathrm{div}\,\varphi(x,y)$ where φ is in the K'-vector space spanned by $\{1, x, y, x^2, x^3\}$; thus $\varphi = y - H(x)$ for some $H(x)$ of degree at most 3. Taking the resultant of φ and $y^2 - f(x)$, we find $H(x)^2 - f(x) = \lambda a(x)^2 t(x)$ for some nonzero $\lambda \in K'$.

Moreover, $H(x) \equiv b(x) \pmod{a(x)}$, since $y - H(x)$ passes through the points in D. Thus we can write $H(x) = b(x) + a(x)c(x)$, for some polynomial $c(x)$ satisfying $\deg c(x) \leq 1$. We first derive this $c(x)$, and then simplify $H(x)$.

Substituting $H(x) = b(x) + a(x)c(x)$ into $H(x)^2 - f(x) = \lambda a(x)^2 t(x)$, we find

$$b(x)^2 - f(x) + 2a(x)b(x)c(x) + a(x)^2c(x)^2 = \lambda a(x)^2 t(x). \tag{6.98}$$

Taking Equation (6.98) modulo $a(x)^2$, we can determine $a(x)c(x)$ modulo $a(x)^2$, and thus $H(x)$ modulo $a(x)^2$. We have to solve

$$a(x)b(x)c(x) \equiv \frac{1}{2}(f(x) - b(x)^2) \pmod{a(x)^2}. \tag{6.99}$$

At this point we want to find a multiplicative inverse for $b(x)$ modulo $a(x)^2$. Note that $a(x)$ and $b(x)$ are coprime: if $\ell(x)$ is a common factor, then $\ell(x)$ divides $H(x)$, so

that $\ell(x)^2$ divides $H(x)^2 - \lambda a(x)^2 t(x) = f(x)$. Since $f(x)$ is square-free, this means $\ell(x)$ is a constant. Thus also $a(x)$ and $b(x)^2$ are coprime. Thus there exists a multiplicative inverse $e(x)$ for $b(x)$ modulo $a(x)^2$, satisfying $b(x)e(x) \equiv 1 \pmod{a(x)^2}$, which we can find using the extended Euclidean algorithm.

Multiplying by $e(x)$ we find that $a(x)c(x) \equiv \frac{1}{2}(f - b(x)^2)e(x) \pmod{a(x)^2}$. Thus

$$\begin{aligned} H(x) &\equiv b(x) + a(x)c(x) \pmod{a(x)^2} && (6.100)\\ &\equiv b(x) + \frac{1}{2}(f(x) - b(x)^2)e(x) \pmod{a(x)^2} && (6.101)\\ &\equiv \frac{1}{2}(b(x) + e(x)f(x)) \pmod{a(x)^2}, && (6.102) \end{aligned}$$

where we used that $b(x)^2 e(x) \equiv b(x) \pmod{a(x)^2}$.

Now define $H(x) \in K[x]$ as the unique representative of degree at most 3 for $\frac{1}{2}(b(x)+e(x)f(x)) \pmod{a(x)^2}$; the above implies that $H(x)^2 - f(x) \equiv 0 \pmod{a(x)^2}$. Thus $H(x)^2 - f(x) = a(x)^2 s(x)$ for some $s(x)$. This equation corresponds to the relation between divisors

$$\operatorname{div}(y - H(x)) = 2\langle a(x), H(x)\rangle + \langle s(x), H(x)\rangle. \tag{6.103}$$

Since $H(x) \equiv b(x) \pmod{a(x)}$, we see that $\langle a(x), H(x)\rangle = D$. Thus $\operatorname{div}((y-H(x))^2) = 4D + 2\langle s(x), H(x)\rangle$. Consequently, $S = \langle s(x), H(x)\rangle$ is 2-torsion, so by Lemma 6.9.13 we must have $s(x) \mid H(x)$. Thus $S = \langle s(x), 0\rangle$ and $2D = S = T$, so $s(x)$ and $t(x)$ are associates. Since $\operatorname{div} t(x) = 2T$, we finally have

$$\operatorname{div}\left(\frac{(y - H(x))^2}{t(x)}\right) = 4D. \tag{6.104}$$

□

Remark 6.9.15. *If $a(x)$ is an irreducible quadratic, then the equations modulo $a(x)$ make sense in the field $K[x]/a(x)$. Otherwise, $a(x)$ is a product of two linear polynomials, say $a(x) = \ell_1(x)\ell_2(x)$. In this case we treat expressions modulo $a(x)$ as expressions modulo $\ell_1(x)$ and $\ell_2(x)$ separately, and solve them separately.*

Divisors of other forms Let $\mathcal{C}$ be the genus 2 curve $y^2 = f(x)$, and let $D = \langle a(x), b(x), d\rangle$ be a divisor on $\mathcal{C}$. Proposition 6.9.14 deals with the case that $\deg f = 6$ and $\deg a(x) = 2$. If $\deg f = 5$, then we can first transform to a degree 6 form (see Section 2.1), compute the function, and then transform back. Thus the only remaining case is $\deg a = 1$ and $\deg f = 6$. In this case, we have $D = P - Q$ for some points

$P, Q \in \mathcal{C}$. If both P and Q are affine points on $\mathcal{C}$, then there is a function φ such that $4(P-Q) = \operatorname{div}\varphi$. This implies $4(P-Q)+4(Q+\bar{Q}-\infty^+-\infty^-) = \operatorname{div}(\psi \cdot (x - x(Q))^4)$. Hence we can first find ψ such that $\operatorname{div}\psi = 4(P + \bar{Q} - \infty^+ - \infty^-)$ and then we have $\operatorname{div}\psi/(x - x(Q))^4 = 4(P - Q)$. This also deals with $D = P - Q$ where one or both of the points is at infinity. Indeed, first translate by x so that neither of P, Q is an affine point with x-coordinate 0, and then transform using $(u, v) = (1/x, y/x^3)$. This results in $P' - Q'$ where P', Q' are both affine points.

6.9.4 Computing in K^*/K^{*m}

We have to compute in K^*/K^{*m} where K is either a number field or the completion of a number field. We discuss the number field case in Section 6.9.5.

Suppose K is a finite extension of $\mathbb{Q}_p$, and let π be a uniformiser (element with valuation 1). Let $\mathfrak{o} = \{x \in K : v(x) \geq 0\}$ denote the ring of integers of K; let $\mathfrak{p} = \{x \in K : v(x) > 0\}$ denote the maximal ideal. Let $k_K = \mathfrak{o}/\mathfrak{p}$ denote the residue field. The group of principal units of K is $U^{(1)} = 1 + \mathfrak{p}$.

Proposition 6.9.16 ([Neu99])**.** *The multiplicative group of a p-adic field K is of the form*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d, \tag{6.105}$$

where $d = [K : \mathbb{Q}_p]$, $q = \#k_K$ and $a \geq 0$. The torsion submodule of $U^{(1)}$ is isomorphic to μ_{p^a}, which determines a.

Remark 6.9.17. MAGMA *can compute the multiplicative group K^* of a p-adic field K using* `UnitGroup(K)`*, and can also compute the quotient K^*/K^{*m} for an integer $m \geq 2$ using* `quo<U | m * U>`*.*

Remark 6.9.18. MAGMA *can construct a finite extension of $\mathbb{Q}_p$ as follows. First define* `Qp := pAdicField(5, 20)`*, say, and then take an irreducible polynomial $m(T)$ and use the function* `LocalField(Qp, m)`*. This returns a* `RngLocA`*, and we can convert it to a* `FldPad` *by using* `RamifiedRepresentation` *(for which more functions are available).*

6.9.5 Computing in $K(S, m)$

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers.

Definition 6.9.19. *Let Q be a prime ideal of $\mathcal{O}_K$ and let $x \in \mathcal{O}_K$. Then we define $v_Q(x)$ as the maximal integer v such that $x \in Q^v$. We extend this to K by letting $v_Q(x/y) = v_Q(x) - v_Q(y)$ for all $x, y \in \mathcal{O}_K$.*

The ideal $(x) = x\mathcal{O}_K$ factors uniquely as a product of prime ideals $(x) = Q_1^{e_1} \cdots Q_n^{e_n}$, and in fact $v_{Q_i}(x) = e_i$ for each Q_i in the factorisation. For Q not appearing in the factorisation we have $v_Q(x) = 0$.

If R is an integral domain with field of fractions K, then a fractional ideal of R is an R-submodule I of K such that there is a nonzero $r \in R$ such that $rI \subseteq R$. The ring R is a Dedekind domain if and only if every nonzero fractional ideal of R is invertible; this holds when R is the ring of integers of a number field.

Let S be a finite set of primes of K and let $m \geq 2$ be an integer. Then we define $K(S, m)$ as the following group:

$$K(S,m) = \{x \in K^*/K^{*m} \colon v_Q(x) \equiv 0 \pmod{m} \text{ for all prime ideals } Q \notin S\}. \tag{6.106}$$

We first describe $K(S, m)$ in the simpler case when $\mathcal{O}_K$ is a principal ideal domain.

The case when $\mathcal{O}_K$ is a principal ideal domain Suppose $\mathcal{O}_K$ is a principal ideal domain. Let $S = \{P_1, \ldots, P_r\}$ be the finite set of primes, and let $P_i = (\alpha_i)$. Then $x \in K(S, m)$ generates the fractional ideal $(x) = x\mathcal{O}_K$, and unique factorisation of ideals implies that $(x) = \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s Q_j^{f_j}$ for some unique ideals Q_j and unique exponents e_i, f_j. Since $x \in K(S, m)$, we have $f_j = mf_j'$ for some $f_j' \in \mathbb{Z}$, for each j. Write $Q_j = (\beta_j)$ for each j. Then $(x) = \prod_{i=1}^r (\alpha_i^{e_i}) \prod_{j=1}^s (\beta_j^{f_j})$. Let $\alpha = \prod_{i=1}^r \alpha_i^{e_i}$ and $\beta = \prod_{j=1}^s \beta_j^{f_j'}$. Then there is a unit u such that $x = u\alpha\beta^m$. This shows the following proposition.

Proposition 6.9.20. *Let K be a number field and suppose that $\mathcal{O}_K$ is a principal ideal domain. Let $S = \{P_1, \ldots, P_r\}$ be a finite set of prime ideals of $\mathcal{O}_K$, and let $P_i = (\alpha_i)$. Then the map*

$$\begin{aligned} K(S,m) &\to \frac{\mathcal{O}_K^*}{\mathcal{O}_K^{*m}} \times \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^r, \\ x &\mapsto \left(\frac{x}{\alpha\beta^m}, e_1, \ldots, e_r\right), \end{aligned} \tag{6.107}$$

is an isomorphism, where α, β, e_i are as above.

Proof. The map is an isomorphism, since the inverse is $(u, e_1, \ldots, e_r) \mapsto u\alpha_1^{e_1} \cdots \alpha_r^{e_r} K^{*m}$, which has kernel $\mathcal{O}_K^{*m} \times (\mathbb{Z}/m\mathbb{Z})^r$. □

Dirichlet's unit theorem describes the units in $\mathcal{O}_K$ (see [Neu99] for a good reference), and we can then compute the quotient $\mathcal{O}_K^*/\mathcal{O}_K^{*m}$.

Theorem 6.9.21 (Dirichlet's unit theorem)**.** *Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Suppose there are r real embeddings $K \hookrightarrow \mathbb{R}$ and s pairs of complex embeddings $K \hookrightarrow \mathbb{C}$. Let $t = r + s - 1$. Then the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is isomorphic to*

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^t, \tag{6.108}$$

where $\mu(K)$ is the group of roots of unity of K.

There are *fundamental units* $\eta_1, \ldots, \eta_t$ such that the isomorphism $\mu(K) \times \mathbb{Z}^t$ is explicitly given by $(\zeta, e_1, \ldots, e_t) \mapsto \zeta\eta_1^{e_1} \cdots \eta_t^{e_t}$.

We can compute the roots of unity $\mu(K)$ in K as follows. Suppose ζ is a primitive nth root of unity in K. Then ζ satisfies the irreducible polynomial $\Phi_n(T) \in \mathbb{Q}[T]$. Hence $\Phi_n(T)$ has a root in K. In particular, we must have $\varphi(n) \leq [K\colon \mathbb{Q}]$. This gives only finitely many $\Phi_n(T)$ to check.

Remark 6.9.22. MAGMA *can compute the unit group of the ring of integers $\mathcal{O}_K$ of a number field using* `UnitGroup(K)`*. We can compute the valuations $e_i = v_{P_i}(x)$ using* `Valuation(x, P_i)`*.*

The general case If $\mathcal{O}_K$ is not a principal ideal domain, the problem is harder. Siksek and Smart give an algorithm to compute generators for $K(S, m)$ when m is prime in [SS97]. We generalise this here to the case where m is not prime, but the proofs mostly follow the same structure.

Let J_K denote the group of nonzero fractional ideals of $\mathcal{O}_K$. Let C_K denote the class group of K, which is the multiplicative group J_K modulo the following equivalence relation: $I \sim J$ if and only if there is $\alpha \in K^*$ such that $I = (\alpha)J$. Write $[I]$ for the equivalence class containing the ideal $I \subseteq \mathcal{O}_K$. We denote the m-torsion of C_K by $C_K[m]$; this consists of ideal classes $[I]$ such that I^m is principal.

Consider the map $\theta\colon K(S, m) \to J_K/J_K^m$ given by $\alpha \mapsto (\alpha)J_K^m$. We trivially have an exact sequence

$$1 \to \ker\theta \to K(S, m) \xrightarrow{\theta} \operatorname{im}\theta \to 1, \tag{6.109}$$

where $\operatorname{im}\theta \subseteq J_K/J_K^m$. We will show this exact sequence splits, and describe $\ker\theta$ and $\operatorname{im}\theta$ separately, which describes $K(S, m)$ as the direct product.

Proposition 6.9.23. *We have*

$$\ker\theta \cong \frac{\mathcal{O}_K^*}{\mathcal{O}_K^{*m}} \times C_K[m]. \tag{6.110}$$

Proof. Let $I_1, \ldots, I_r \in J_K$ be representatives for a basis of $C_K[m]$, and let $I_i^m = (\beta_i)$ for each $i = 1, \ldots, r$. Suppose $x \in K^*$ represents an element of $\ker\theta \subseteq K(S,m) \subset K^*/K^{*m}$. Then $(x) = I^m$ for some ideal I. This implies $[I] \in C_K[m]$, so that $[I] = \prod_{i=1}^r [I_i]^{\mathbf{e}_i}$ for some vector $\mathbf{e}$ with entries in $\mathbb{Z}$. The ideal classes are equal, so there is $\gamma \in K^*$ such that $I = (\gamma)\prod_{i=1}^r I_i^{\mathbf{e}_i}$. Thus

$$(x) = I^m = (\gamma^m)\prod_{i=1}^r I_i^{m\mathbf{e}_i} = (\gamma^m)\prod_{i=1}^r (\beta_i^{\mathbf{e}_i}). \tag{6.111}$$

Thus there is a unit $u \in \mathcal{O}_K^*$ such that $x = u\gamma^m \prod_{i=1}^r \beta_i^{\mathbf{e}_i}$. Let g be the map

$$\begin{aligned} g\colon \ker\theta &\to \mathcal{O}_K^*/\mathcal{O}_K^{*m} \times C_K[m] \\ g(x) &= (u, [I]). \end{aligned} \tag{6.112}$$

We now define an inverse to g. Consider the map $h\colon \mathcal{O}_K^*/\mathcal{O}_K^{*m} \times C_K[m] \to \ker\theta$ given by $(u,[I]) \mapsto u \cdot \prod_{i=1}^r \beta_i^{\mathbf{e}_i}$, where $[I] = \prod_{i=1}^r [I_i]^{\mathbf{e}_i}$. This is well-defined, since the ideal generated by $u \cdot \prod_i \beta_i^{\mathbf{e}_i}$ is $\prod_{i=1}^r I_i^{m\mathbf{e}_i} \in J_K^m$. Moreover g and h are mutually inverse. □

Next we describe $\operatorname{im}\theta$.

In the following, if $\mathbf{v} \in \mathbb{Z}^n$ is a vector and $d \in \mathbb{Z}$ we write $\gcd(\mathbf{v}, d)$ for the vector whose ith element is $\gcd(\mathbf{v}_i, d)$. If $\mathbf{u} \in \mathbb{Z}^n_{>0}$, we write $\mathbf{v} \pmod{\mathbf{u}}$ for the vector whose ith element is $\mathbf{v}_i \pmod{\mathbf{u}_i}$. For $M \in M_{n_1\times n_2}(\mathbb{Z})$ and $a \in \mathbb{Z}$, define $\Lambda(M,a)$ as

$$\Lambda(M,a) = \{\mathbf{v} \in \mathbb{Z}^{n_1} \colon \mathbf{e}M \equiv 0 \pmod{a}\}; \tag{6.113}$$

for a vector of integers $\mathbf{a} \in \mathbb{Z}^{n_2}$, we extend the definition to

$$\Lambda(M,\mathbf{a}) = \{\mathbf{e} \in \mathbb{Z}^{n_1} \colon \mathbf{e}M \equiv 0 \pmod{\mathbf{a}}\}. \tag{6.114}$$

Both of $\Lambda(M,a)$ and $\Lambda(M,\mathbf{a})$ are finitely generated $\mathbb{Z}$-modules, so admit a finite basis according to the main theorem on finitely generated modules over principal ideal domains.

The following proof is based on the proof in [SS97], but we generalise to the case where m is not necessarily prime.

Proposition 6.9.24. *Let $C_1, \dots, C_g$ be representatives for a basis of C_K, and define $\mathbf{s} \in \mathbb{Z}^g$ by $\mathbf{s}_i = \operatorname{ord}[C_i]$. Suppose $S = \{P_1, \dots, P_n\}$ is a finite set of primes of K, and let M be the matrix defined by $[P_i] = \prod_{j=1}^g [C_j]^{M_{ij}}$. For $\mathbf{e} \in \Lambda(M, \gcd(\mathbf{s}, m))$, we define $\mathbf{t} \in (\mathbb{Z}/m\mathbb{Z})^{n_1}$ such that $t \equiv \mathbf{e}M \pmod m$. The ideal $\prod_{i=1}^n P_i^{\mathbf{e}_i} \prod_{j=1}^g C_j^{-\mathbf{t}_j}$ is principal, equal to $(\alpha_{\mathbf{e}})$, say, and these $(\alpha_{\mathbf{e}})$ generate $\operatorname{im}\theta$. Let $\mathbf{e}^{(1)}, \dots, \mathbf{e}^{(h)}$ be a basis for $\Lambda(M, \mathbf{a})$. Then*

$$\operatorname{im}\theta \cong \bigoplus_{i=1}^{h} \mathbb{Z}/b_i\mathbb{Z}, \tag{6.115}$$

where b_i is the order of $\mathbf{e}^{(i)}$ in $(\mathbb{Z}/m\mathbb{Z})^{n_1}$.

Proof. Let J be a fractional ideal representing an element of $\operatorname{im}\theta$. Then $J = (\alpha)I^m$ for some $I \in J_K$, so that $[J] = [I]^m$ in the class group. Let $J = \prod_{i=1}^n P_i^{\mathbf{e}_i}$ be its unique prime factorisation, where we assume without loss of generality that $0 \le \mathbf{e}_i < m$ for each i; if any other prime ideals occur in the factorisation, then their exponents are divisible by m since $x \in K(S, m)$ and thus we can absorb them into I. Then

$$[J] = \prod_{i=1}^n [P_i]^{\mathbf{e}_i} = \prod_{i=1}^n \prod_{j=1}^g [C_j]^{\mathbf{e}_i M_{ij}} \tag{6.116}$$

$$= \prod_{j=1}^g [C_j]^{\mathbf{t}_j}, \tag{6.117}$$

where $\mathbf{t}_j = \sum_{i=1}^n \mathbf{e}_i M_{ij}$. The fact that $[J] = [I]^m$ implies that for each j, we have $[C_j]^{\mathbf{t}_j} = [C_j]^{m\mathbf{x}_j}$ for some $\mathbf{x}_j$. This holds if and only if $\mathbf{t}_j = m\mathbf{x}_j + \mathbf{s}_j\mathbf{y}_j$, which is soluble if and only if $\gcd(\mathbf{s}_j, m)$ divides $\mathbf{t}_j$. Thus we have the congruences

$$\mathbf{t}_j \equiv 0 \pmod{\gcd(\mathbf{s}_j, m)} \tag{6.118}$$

for each $j = 1, \dots, g$. Equivalently, $\mathbf{e}M \equiv 0 \pmod{\gcd(\mathbf{s}, m)}$; that is,

$$\mathbf{e} \in \Lambda(M, \gcd(\mathbf{s}, m). \tag{6.119}$$

For each solution $\mathbf{e} = (e_1, \dots, e_n)$ to the congruences (6.119), we have $\prod_{j=1}^g C_j^{\mathbf{t}_j} \in J_K^m$. Let $J_{\mathbf{e}}$ be the ideal $\prod_{i=1}^n P_i^{\mathbf{e}_i}$. Then $J_{\mathbf{e}}$ satisfies $[J_{\mathbf{e}}] \equiv \prod_{j=1}^g [C_j]^{\mathbf{t}_j}$, so that $J_{\mathbf{e}} \prod_{j=1}^g C_j^{-\mathbf{t}_j} = (\alpha_{\mathbf{e}})$ is principal. Thus $J_{\mathbf{e}} J_K^m = (\alpha_{\mathbf{e}})$. There are finitely many solutions $\mathbf{e}$ to the congruences in $(\mathbb{Z}/m\mathbb{Z})^n$. Thus $\operatorname{im}\theta$ is generated by all the $\alpha_{\mathbf{e}} \in K^*/K^{*m}$ corresponding to the solutions $\mathbf{e}$ to the congruences (6.119).

If $\mathbf{e}^{(1)}, \dots, \mathbf{e}^{(n)}$ is a basis for $\Lambda(M, \gcd(\mathbf{s}, m)) \subset (\mathbb{Z}/m\mathbb{Z})^n$, and $\alpha_i = \alpha_{\mathbf{e}^{(i)}}$, then $\theta(\alpha_1), \dots, \theta(\alpha_n)$ is a basis for $\operatorname{im}\theta$. □

We can compute $\Lambda(M, \mathbf{a})$ as the intersection

$$\Lambda(M, \mathbf{a}) = \bigcap_{j=1}^{n_2} \Lambda(M[:, j], \mathbf{a}_j), \tag{6.120}$$

where $M[:, j]$ denotes the jth column of M. Thus, given an algorithm that can compute $\Lambda(M, a)$ for an arbitrary matrix $M \in M_{n_1 \times n_2}(\mathbb{Z})$ and integer a, we can also compute $\Lambda(M, \mathbf{a})$. MAGMA can compute the kernel of a matrix M over $\mathbb{Z}/a\mathbb{Z}$ using `Kernel`.

Corollary 6.9.25. *Let K be a number field and let S be a finite set of primes. Let $\alpha_1, \ldots, \alpha_h$ be as in Proposition 6.9.24; let $\beta_1, \ldots, \beta_r$ be as in Proposition 6.9.23. Let $\eta_1, \ldots, \eta_r$ be a system of fundamental units for K and let ζ be a generator for the roots of unity. Then $K(S, m)$ is isomorphic to the abelian group $\ker\theta \times \operatorname{im}\theta$, with basis*

$$\beta_1, \ldots, \beta_r, \eta_1, \ldots, \eta_r, \zeta, \alpha_1, \ldots, \alpha_h. \tag{6.121}$$

Proof. The elements $\theta(\alpha_1), \ldots, \theta(\alpha_h)$ are a basis for $\operatorname{im}\theta$. Thus we can define the map $\operatorname{im}\theta \to K(S, m)$ by $\theta(\alpha_i) \mapsto \alpha_i$. This splits the exact sequence

$$1 \to \ker\theta \to K(S, m) \to \operatorname{im}\theta \to 1. \tag{6.122}$$

□

Algorithm 7 expresses this more formally.

Algorithm: Computing in $K(S, m)$
Data: Number field K, finite set of primes $S = \{P_1, \ldots, P_n\}$ of K, integer $m \geq 2$.
Compute the class group C_K of K
Compute the m-torsion $C_K[m]$; let $J_1, \ldots, J_r$ be the generators
Compute a principal generator β_i for J_i^m for each i
Compute the unit group U of $\mathcal{O}_K$
Compute the matrix M such that $[P_i] = \prod_j [C_j]^{M_{ij}}$
Compute a basis $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(h)}$ for $\Lambda(M, \gcd(\mathbf{s}, m))$
Compute α_i for $\mathbf{e}^{(i)}$ for each $i = 1, \ldots, h$
return the group generated by α_i, β_j and generators for U

Algorithm 7: Computing in $K(S, m)$.

Given $x \in K^*/K^{*m}$, we compute its image in $K(S, m)$ as follows. First compute $\mathbf{e}(x)$ by factoring $(x) = \prod_{i=1}^n P_i^{\mathbf{e}_i} I'^m$, where I' absorbs any prime factors not in S. Then $\theta(x) = \theta(\alpha_{\mathbf{e}})$. Write $\mathbf{e} = \sum_{j=1}^h a_i \mathbf{e}^{(i)}$ for some $a_i \in \mathbb{Z}$. Let $\beta = \prod_{j=1}^h \alpha_j^{a_j}$; then $\gamma = x/\beta \in \ker\theta$. The image of x in $\operatorname{im}\theta$ is $(a_1, \ldots, a_h)$. The image in $\ker\theta$ is the image of γ, as in the proof of Proposition 6.9.23.

Example 6.9.26. *In the case that $m = p$ is prime, we can compute a basis for the Selmer congruences more simply, as in [SS97]. First choose a basis $[C_1], \dots [C_g]$ for $C_K[p]$ such that $p \nmid \mathbf{s}_i$ for $i = 1, \dots, k$ and $p \mid \mathbf{s}_i$ for $i = k+1, \dots, g$. Compute M_{ij} as above for P_i. Then the congruences are*

$$\mathbf{t}_j = \sum_{i=1}^{n} \mathbf{e}_i M_{ij} \equiv 0 \pmod{p} \tag{6.123}$$

for $j = k+1, \dots, g$. Then the space of solutions $\mathbf{e}$ is the left nullspace of $M[:, k+1:g]$ over $\mathbb{F}_p$.

We give a program to compute this in `four_four/selmer_groups_general.m` in [Nic18].

6.10 Computing the $(4,4)$-descent

The file `descent/four_four_descent.m` in [Nic18] contains the code to carry out a $(4,4)$-descent and a Richelot descent simultaneously. The program outputs whether the image of the $(4,4)$-Selmer group in the Richelot Selmer group is smaller than the Richelot Selmer group. We attempted to find an example of a genus 2 curve admitting a $(4,4)$-isogeny with rational kernel such that the bound from a $(4,4)$-descent improves upon a bound from a Richelot descent. Unfortunately we have not yet been able to find such an example, and this remains a work in progress. In the rest of this section we discuss some technical details involved with the computations.

Bad primes for the $(4,4)$-isogeny The bad primes for the $(4,4)$-isogeny are the union of the bad primes for the two Richelot isogenies. We also have to worry about the $(4,4)$-isogeny degenerating into a different type of composition of Richelot isogenies. We know that $D_1, D_2 \in \mathcal{J}[4]$ generate the kernel of the $(4,4)$-isogeny. We have $\langle D_1, D_2 \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, which is preserved under reduction modulo any odd prime p. This is because the prime-to-p part of $\mathcal{J}_{\text{tors}}$ injects into the reduction $\tilde{\mathcal{J}}(\mathbb{F}_p)$. The property $e_4(D_1, D_2) = 1$ is also preserved under reduction modulo any odd prime p.

The $(4,4)$ diagram Let $L = K \times K$. Let γ_4 be the $(4,4)$-Cassels map $\mathcal{J}_1(K) \to L^*/L^{*4}$, given on points by $\gamma_4((x,y)) = (F_1(x,y), F_2(x,y))$, where $F_i(x,y) = (y - H_i(x))^2/t_i(x)$ as in Section 6.9.3. Let γ_2 be the Richelot Cassels map $\mathcal{J}_1(K) \to L^*/L^{*2}$, given on points by $\gamma_2((x,y)) = (t_1(x,y), t_2(x,y))$ where t_1, t_2 are as in the $(4,4)$ section. In particular, since $F_i(x,y) \equiv t_i(x,y) \pmod{K^{*2}}$, the following diagram commutes:

$$\begin{array}{ccc} \frac{\mathcal{J}_3(K)}{\varphi_2\varphi_1\mathcal{J}_3(K)} & \xrightarrow{\gamma_4} & L^*/L^{*4} \\ \downarrow & & \downarrow q \\ \frac{\mathcal{J}_3(K)}{\varphi_2\mathcal{J}_2(K)} & \xrightarrow{\gamma_2} & L^*/L^{*2} \end{array} \tag{6.124}$$

The vertical maps are induced by the quotients.

Let s be a prime of K. Let $L_s = \prod_{\mathfrak{s}|s} L_{\mathfrak{s}}$. Since s is a prime of K, and $L = K \times K$, we have $L_s = K_s \times K_s$. Write $\gamma_{4,s}$ and $\gamma_{2,s}$ for the corresponding local maps, as in the diagram (6.13). For $i = 2, 3$, and for a prime s of K, let $\beta_{i,s} \colon L^*/L^{*i} \to L_{i,s}^*/L_{i,s}^{*i}$ be the localisation maps. We also have the localised commutative diagram:

$$\begin{array}{ccc} \frac{\mathcal{J}_3(K_s)}{\varphi_2\varphi_1\mathcal{J}_3(K_s)} & \xrightarrow{\gamma_{4,s}} & L_s^*/L_s^{*4} \\ \downarrow & & \downarrow q_s \\ \frac{\mathcal{J}_3(K_s)}{\varphi_2\mathcal{J}_2(K_s)} & \xrightarrow{\gamma_{2,s}} & L_s^*/L_s^{*2} \end{array} \tag{6.125}$$

Each term in (6.124) maps down to the corresponding term in (6.125) by the obvious localisation map, and the resulting cube commutes.

Intersecting at $p = \infty$ Suppose $K = \mathbb{Q}$. Here we explain how to intersect at $p = \infty$; that is, the completion $\mathbb{R}$ of $\mathbb{Q}$.

We first have to generate the real points for the Richelot isogeny.

Let $\varphi \colon \mathcal{J} \to \mathcal{J}'$ be a Richelot isogeny. Cassels and Flynn show (see [CF96, Chapter 7])

$$\#\frac{\mathcal{J}(\mathbb{R})}{\varphi'\mathcal{J}'(\mathbb{R})} \cdot \#\frac{\mathcal{J}'(\mathbb{R})}{\varphi\mathcal{J}(\mathbb{R})} = 4. \tag{6.126}$$

We can generate points on $\mathcal{J}(\mathbb{R})$ by first generating points on $\mathcal{K}(\mathbb{Q})$ and then checking if $a_9^2 \geq 0$. If so, then the Kummer point lifts to the Jacobian over $\mathbb{R}$. We can then compute the image under the Richelot Cassels map just using the Kummer coordinates.

If S is a given finite set of rational primes, we have $\mathbb{Q}(S, m) = \langle -1 \rangle \times \langle S \rangle \subset \mathbb{Q}^*/\mathbb{Q}^{*m}$. We have

$$\mathbb{R}^*/\mathbb{R}^{*m} = \begin{cases} \{\pm 1\}, \text{ if } m \text{ even} \\ \{1\}, \text{ if } m \text{ odd} . \end{cases} \tag{6.127}$$

This is because the image of $\cdot^m \colon \mathbb{R}^* \to \mathbb{R}^*$ is $\mathbb{R}_{>0}$ if m is even and $\mathbb{R}^*$ if m is odd.

The inclusion map $\mathbb{Q}(S, m) \subset \mathbb{Q}^*/\mathbb{Q}^{*m} \to \mathbb{R}^*/\mathbb{R}^{*m}$ is given by $\alpha \mapsto \text{sign}(\alpha)$ if m is even, and is the constant map 1 if m is odd.

Computing the image of the $(4,4)$-Selmer group in the Richelot Selmer group. If S is a finite set of primes, let

$$\begin{aligned} H_4(S) &= \beta_{4,s}^{-1}(\cap_{s\in S}\gamma_{4,s}(\mathcal{J}_1(\mathbb{Q}_s))), \\ H_2(S) &= \beta_{2,s}^{-1}(\cap_{s\in S}\gamma_{2,s}(\mathcal{J}_1(\mathbb{Q}_s))) \end{aligned} \tag{6.128}$$

be the $(4,4)$-Selmer group and Richelot-Selmer group, respectively. Let

$$q\colon L^*/L^{*4} \to L^*/L^{*2} \tag{6.129}$$

be the quotient map that reduces an element modulo squares. Since (6.124) and (6.125) commute, we have $q(H_4(S)) \subseteq H_2(S)$.

The image of $H_4(S)$ in $H_2(S)$ is the quotient $H_4(S)/(H_4(S)\cap L^{*2})$.

Remark 6.10.1. *We caution that $q(H_4(S))$ is not equal to $H_4(S)/H_4(S)^2$. For example, if $G = \langle 2,3,5\rangle \subseteq \mathbb{Q}^*/\mathbb{Q}^{*4}$ and $H = \langle 2^2, 3\rangle$, then $H\cap G^2 = \langle 2^2, 3^2\rangle$, while $H^2 = \langle 3^2\rangle$.*

Remark 6.10.2. *For the Richelot Cassels map we can replace one of the components by the product of the other two, since the product of all three is square. This is no longer possible for the $(4,4)$-Cassels map as the product of all three components is not guaranteed to be in K^{*4}.*

6.10.1 Computing Cassels maps

Consider the Richelot Cassels map. Suppose $\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x)$ is a genus 2 curve admitting a Richelot isogeny, and let $\mathcal{C}'\colon y^2 = L_1(x)L_2(x)L_3(x)$ be the isogenous curve, where $L_i(x) = [G_{i+1}(x), G_{i+2}(x)]/\Delta$ (see Theorem 5.7.4). Then the Cassels map is

$$\begin{aligned} \mathcal{J}(K)/\varphi'\mathcal{J}'(K) &\to K^*/K^{*2}\times K^*/K^{*2}\times K^*/K^{*2} \\ (x,y) &\mapsto (G_1(x), G_2(x), G_3(x)), \end{aligned} \tag{6.130}$$

extended linearly to divisors.

Evaluating at points at infinity Lemma 6.10.3 lets us efficiently compute the Richelot Cassels map using the Kummer coordinates of the point.

Lemma 6.10.3. *Let $f(x) = G_1(x)G_2(x)G_3(x)$ be a Richelot splitting with $\deg f$ either 5 or 6. Let $D \neq 0 \in \mathcal{J}(K)$ and let $\xi \in \mathbb{A}^4$ be a representative vector for the Kummer*

coordinates of D. Let $c_0 \in K$ be defined such that $a_\xi(x) = c_0(\xi_0 x^2 - \xi_1 x + \xi_2)$ is monic. Then the image of D under the Richelot Cassels map is

$$\begin{cases} (\operatorname{Res}(G_1, a_\xi), \operatorname{Res}(G_2, a_\xi), \operatorname{Res}(G_3, a_\xi)), & \text{if } \deg a_\xi \text{ is even} \\ (c_1 \operatorname{Res}(G_1, a_\xi), c_2 \operatorname{Res}(G_2, a_\xi), c_3 \operatorname{Res}(G_3, a_\xi)), & \text{if } \deg a_\xi \text{ is odd,} \end{cases} \tag{6.131}$$

where c_i is the x^2 coefficient of G_i.

Proof. Let $\mathfrak{m} = \infty^+ + \infty^-$ if $\deg f = 6$ and $\mathfrak{m} = 2\infty$ if $\deg f = 5$. Consider the point $D = P_1 + P_2 - \mathfrak{m}$ on $\mathcal{J}$. Let $a(x)$ be the polynomial for the x-coordinates of D in Mumford notation. Then $a(x)$ is proportional to $\xi_0 x^2 - \xi_1 x + \xi_2$, where ξ are the Kummer coordinates of D. Our choice of $a_\xi(x)$ above is the unique monic polynomial proportional to this.

We can compute the map at points at infinity as follows. Let $G(x)$ be a polynomial and let $d = \lceil \deg G/2 \rceil$; thus $G(x) = G_{2d}x^{2d} + G_{2d+1}x^{2d+1} + \cdots + G_0$ with at least one of G_{2d} and G_{2d+1} being nonzero. Then

$$\begin{aligned} G(x) &= G(1/u) && (6.132) \\ &= \frac{G_{2d} + uG_{2d+1} + \cdots + u^{2d}G_0}{u^{2d}} && (6.133) \\ &\equiv \tilde{G}(u) \pmod{K^{*2}}, && (6.134) \end{aligned}$$

where $\tilde{G} = u^{2d}G(1/u)$ is the 'flip' polynomial. Let P_∞ be a point at infinity. Then $G(P_\infty) \equiv \tilde{G}(0) \pmod{K^{*2}}$. In particular, $G(P_\infty) \equiv G_{2d}$, the coefficient of x^{2d} in $G(x)$.

In this case, each $G_i(x)$ has degree 1 or 2, so $d = 1$. Thus $G_i(P_\infty) \equiv c_i \pmod{K^{*2}}$, where c_i is the x^2 coefficient of $G_i(x)$. In particular, $G(\mathfrak{m}) = G_{2d}^2$ is square. So we are reduced to computing $G(P_1 + P_2)$.

If neither of P_1, P_2 is at infinity, then $\deg a_\xi = 2$, and the Cassels map is just $(G_1(x_1)G_1(x_2), G_2(x_1)G_2(x_2), G_3(x_1)G_3(x_2))$. If both of P_1, P_2 are at infinity, then $a_\xi(x) = 1$ and the Cassels map is $(1, 1, 1)$.

If exactly one of P_1, P_2 is at infinity, then $D = P - P_\infty$ for an affine point P and point at infinity P_∞, and the Cassels map is $(G_1(x(P))/G_{2d}, G_2(x(P))/G_{2d}, G_3(x(P))/G_{2d})$.

In all cases, our definition agrees with the Cassels map modulo squares. □

Example 6.10.4. *Let $(G_1(x), G_2(x), G_3(x)) = (x^2 + x + 1, x^2 - 1, x^2 - 5)$. Consider $\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x)$. The Jacobian $\mathcal{J}$ of $\mathcal{C}$ has the points*

$$\begin{aligned} P_1 &= (1, 0) + (-1, 0) - \infty^+ - \infty^- && (6.135) \\ P_2 &= \infty^+ - \infty^- && (6.136) \\ P_3 &= (1, 0) - \infty^+ && (6.137) \\ P_4 &= \langle x^2 - 5x - 4, 29x + 19, 2 \rangle, && (6.138) \end{aligned}$$

where P_4 is given in Mumford notation. We compute the Cassels map for each of these below. Let ρ denote the Cassels map $\mathcal{J}(\mathbb{Q})/\varphi'\mathcal{J}'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$. For P_1, we have

$$(G_1(1)G_1(-1), G_2(1)G_2(-1), G_3(1)G_3(-1)) = (3, 0, 16); \tag{6.139}$$

we can ignore $G_i(\infty^+ + \infty^-)$, since the proof above shows that $G_i(\infty^+) \equiv G_i(\infty^-) \pmod{\mathbb{Q}^{*2}}$. Using that the product of the components is square, and replacing the components modulo squares, we find $\rho(P_1) = (3, 1, 1)$. For P_2, we have $\rho(P_2)_i = G_i(\infty^+)/G_i(\infty^-) \equiv 1 \pmod{\mathbb{Q}^{*2}}$. For P_3, we have

$$(G_1((1,0)), G_2((1,0)), G_3((1,0))) = (3, 0, -4) \tag{6.140}$$

$$\big(G_1(\infty^+), G_2(\infty^+), G_3(\infty^+)\big) = (1, 1, 1), \tag{6.141}$$

since the x^{2d} coefficient of each of $G_1(x), G_2(x)$ and $G_3(x)$ is the x^2 coefficient, which is 1. Thus $\rho(P_3) = (3, \alpha, -4)$, where $3 \cdot \alpha \cdot -4 \equiv 1 \pmod{\mathbb{Q}^{*2}}$. Thus $\rho(P_3) = (3, -3, -1)$.

For P_4 we use the method described by Lemma 6.10.3. We have $a_\xi(x)$ is $x^2 - 5x - 4$. The resultants $\operatorname{Res}(G_i, a_\xi)$ for $i = 1, 2, 3$ are $31, -16, -124$, respectively. Thus $\rho(P_4) = (31, -1, -31)$.

Remark 6.10.5. *The bad primes for the splitting above: (x^2+x+1, x^2-1, x^2-5) are those dividing the discriminant of $G_1(x)G_2(x)G_3(x)$, together with those dividing the Δ from the Richelot isogeny, together with 2. These are $2, 3, 5, 31$. As expected, these are the only prime factors occurring modulo squares in the images under the Cassels map.*

The next example highlights the importance of using the x^2 coefficient of each $G_i(x)$, rather than just the leading coefficient.

Example 6.10.6. *Let $(G_1(x), G_2(x), G_3(x)) = (x, 2x^2 + x + 1, x^2 - 3)$. In particular, $G_1(x)$ is linear. Consider $\mathcal{C}\colon y^2 = G_1(x)G_2(x)G_3(x)$. Then $P = \langle x + 1, 2, 1\rangle \in \mathcal{J}$. Then $\rho(P)_i = \operatorname{Res}(G_i, x + 1)/c_i$, where c_i is the x^2 coefficient of $G_i(x)$. Since $c_1 = 0$, the first component is undefined, but we have $G_2(-1)/c_2 = 2/2 = 1$ and $G_3(-1)/c_3 = -2/1 = -2$, respectively. Thus, replacing the first component by the product of the other two, we have*

$$\rho(P) \equiv (-2, 1, -2). \tag{6.142}$$

Remark 6.10.7. *We use the definition of the resultant such that*

$$\mathrm{Res}(p(x), x - \alpha) = p(\alpha). \tag{6.143}$$

This implies that

$$\mathrm{Res}(p(x), q(x)) = c^{\deg q} \prod_{i=1}^{n} p(\alpha_i), \tag{6.144}$$

where $q(x) = c\prod_{i=1}^{n}(x - \alpha_i)$. *However,* MAGMA *uses a different convention.*

Evaluating the $(4, 4)$**-Cassels map at points at infinity** Let $D \in \mathcal{J}[4](K)$, where $\mathcal{J}$ is the Jacobian of $\mathcal{C}\colon y^2 = f(x)$. We have seen that if $\deg f = 6$, then $\operatorname{div} F = 4D$, where $F = (y - H(x))^2/t(x)$ for some polynomials $H(x)$ and $t(x)$. We can evaluate F at the affine point (x, y) as usual. We can write F in terms of (u, v)-coordinates as

$$\begin{aligned} F(x, y) &= F(1/u, v/u^3) && (6.145)\\ &= \frac{(v - u^3 H(1/u))^2}{u^4 \cdot u^2 t(1/u)} && (6.146)\\ &\equiv \frac{(v - \tilde{H}(u))^2}{\tilde{t}(u)} \pmod{K^{*4}}, && (6.147) \end{aligned}$$

where $\tilde{H}(u) = u^3 H(1/u)$ and $\tilde{t}(u) = u^2 t(1/u)$. If P_∞ is a point at infinity, then it has (u, v)-coordinates $(0, v_0)$ for some v_0, and so $F(P_\infty) = \frac{(v_0 - H_3)^2}{t_2}$, where H_3, t_2 are the degree 3 and 2 terms of $H(x), t(x)$, respectively.

In particular, $F(\mathfrak{m}) = \frac{(v_0^2 - H_3^2)^2}{t_2^2}$, where $v_0 = \sqrt{f_6}$.

Remark 6.10.8. *Often when computing Cassels maps we find one of the components evaluates to zero. To get around this we try computing* $h(D + E) - h(E)$ *for various points* E. *Since* h *is a homomorphism, this gives the same result, but may have both components defined.*

Chapter 7

Conclusion

In this chapter we summarise our results and give some ideas for further work.

Torsion Tables 3.1, 3.2 and 3.3 list the torsion orders we found using the methods discussed in Chapter 3. Of particular note is Example 3.1.7, which provides the first known example of a geometrically simple Jacobian of a genus 2 curve with a point of order 25. The previous torsion record for a geometrically simple Jacobian of a hyperelliptic curve of genus 3 was 41, due to Kronberg ([Kro15]). We found new examples of such Jacobians containing a point of order $N > 41$ for N in the set

$$\{42, 43, 44, 48, 49, 50, 52, 54, 56, 64, 65, 72, 91\}, \tag{7.1}$$

as well as many for smaller N (see Table 3.2). The previous torsion record for a geometrically simple Jacobian of a hyperelliptic curve of genus 4 was 72, due to Leprévost ([Lep97]). We found new examples of such Jacobians containing a point of order $N > 72$ for N in the set

$$\{74, 82, 88\}, \tag{7.2}$$

as well as many new examples for smaller N. Tables F.1, F.2 and F.3 in Appendix F list more of the curves we found.

For further work, one idea is to analyse other torsion orders known to occur in the literature that we didn't manage to recover. We may be able to find generalisations of our methods that we missed. We don't currently focus on even degree hyperelliptic curves where ∞^+, ∞^- are defined over a quadratic extension, or on finding points on the Jacobian of the form $\langle a(x), b(x), d\rangle$ with $\deg a(x) > 1$.

We could improve the point searching routines so that we can find more curves with the same methods. For example, we sometimes don't find rational points on the

varieties when one of the equations is a conic, which we could sometimes parametrise. Many of our examples of curves seem to come from 1-parameter families, but we don't currently try too hard to find these families.

Another idea is to search for Jacobians where there is a subgroup rational as a set. This could let us recover Jacobians with a $(7,7)$-subgroup. The Gröbner basis approach can do this in theory.

Kummer coordinates In Chapter 4, we found an embedding of the Kummer varieties of superelliptic curves of genus 3 into projective space. We saw in Chapter 5, while computing isogenies between Jacobians of curves of genus 2, how useful an explicit embedding Kummer variety of a curve can be. We hope that the Kummer embedding in the superelliptic genus 3 case will be similarly helpful.

One future direction with this work is to compute a theory of heights for the Jacobians of genus 3 superelliptic curves using the Kummer embedding, analogously to [Sto17]. We could also try and extend the Kummer embedding to all genus 3 nonhyperelliptic curves.

We also don't currently have a practical proof of why the Kummer coordinates are invariant under negation. Although this holds for all examples we checked, it seems computationally tricky to prove this in general.

Jacobian coordinates We found an explicit basis for the Jacobian coordinates of superelliptic genus 3 curves in Section 4.4.5, but were unable to compute the quadratic relations between them. This would give an embedding of the Jacobians of superelliptic genus 3 curves. We could potentially do the same for the Jacobian coordinates of genus 3 hyperelliptic curves. However, the computations may not currently be computationally feasible.

Isogenies In Chapter 5, we classified the genus 2 curves whose Jacobians admit a $(4,4)$-isogeny. We further provided an infinite family of such Jacobians such that the kernel of the $(4,4)$-isogeny was completely defined over the ground field, and gave explicit conditions under which this can occur. One future direction is to complete this classification. Our current classification only guarantees that there are 4-torsion points whose images on the Kummer surface are distinct and K-rational, while we also need that these 4-torsion points generate a $(4,4)$-isogeny and lift to rational points on the Jacobian.

We also extended Flynn's example of genus 2 curves whose Jacobians admit a $(5,5)$-isogeny to find infinitely many pairwise geometrically nonisomorphic such Jacobians. A future direction here is to completely classify such curves.

Descent In Chapter 6 we extended Schaefer's algorithm for computing the Selmer group of a Jacobian to carry out a $(4,4)$-descent on the Jacobians of curves that admit a $(4,4)$-isogeny. We were able to carry out a descent via $(4,4)$-isogeny for the Jacobians of the curves in our family of Jacobians with a rational $(4,4)$-kernel, but haven't yet been able to find an example where the rank from the $(4,4)$-descent improves upon the bound from the Richelot descent. The main issue we encountered is that the curves in our family have large bad primes, which means the calculations take a long time.

Bibliography

[And17] Andrea, 2017. `https://math.stackexchange.com/questions/2371991/classification-of-principally-polarized-abelian-surface` (accessed 14-06-2018).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD11] Nils Bruin and Kevin Doerksen. The arithmetic of genus two curves with (4,4)-split Jacobians. *Canadian Journal of Mathematics*, 63(5):992–1024, 2011.

[BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa. Descent via (3, 3)-isogeny on Jacobians of genus 2 curves. *Acta Arithmetica*, 165(3):201–223, 2014.

[BJF88] Jean-Benoit Bost and Mestre Jean-Francois. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.*, 38:36–64, 1988.

[BL04] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2004.

[BLP09] Nicolas Bernard, Franck Leprévost, and Michael Pohst. Jacobians of genus-2 curves with a rational point of order 11. *Experimental Mathematics*, 18(1):65–70, 2009.

[BPS14] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. 2014.

[Can87] David G Cantor. Computing in the Jacobian of a Hyperelliptique Curve. *Mathematics of Computation*, 48(177):95–101, 1987.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Cambridge University Press, 1996.

[CM96] Daniel Coray and Constantin Manoil. On large Picard groups and the Hasse principle for curves and K3 surfaces. *Acta Arithmetica*, 76(2):165–189, 1996.

[Col84] Alberto Collino. A New Proof of the Ran-Matsusaka Criterion for Jacobians. *American Mathematical Society*, 92(3):329–331, 1984.

[CS86] G. Cornell and J.H. Silverman. *Arithmetic geometry*. Springer-Verlag, 1986.

[DS18] Katthaleeya Daowsud and Thomas A. Schmidt. Continued fractions for rational torsion. *Journal of Number Theory*, 189:115–130, 2018.

[Elk18] Noam Elkies. Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order. `http://www.math.harvard.edu/~elkies/g2_tors.html`, 2002 (accessed 14-06-2018).

[Fis16] Tom Fisher. Higher descents on an elliptic curve with a rational 2-torsion point. *Mathematics of Computation*, 86(307):2493–2518, 2016.

[Fly90a] E. V. Flynn. Large rational torsion on Abelian varieties. *Journal of Number Theory*, 36(3):257–265, 1990.

[Fly90b] Eugene Victor Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Mathematical Proceedings of the Cambridge Philosophical Society*, 107(3):425–441, 1990.

[Fly91] E. V. Flynn. Sequences of rational torsion on abelian varieties. *Inventiones mathematicae*, 106:433–442, 1991.

[Fly94] E. V. Flynn. Descent via isogeny in dimension 2. *Acta Arithmetica*, 66(1):23–43, 1994.

[Fly95] E. V. Flynn. An Explicit Theory of Heights. *Transactions of the American Mathematical Society*, 347(8):3003–3015, 1995.

[Fly15] E. V. Flynn. Descent via (5, 5)-isogeny on Jacobians of genus 2 curves. *Journal of Number Theory*, 153:270–282, 2015.

[FS97] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arithmetica*, 79(4):333–352, 1997.

[GPS00] S. D. Galbraith, S. M. Paulus, and N. P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–406, 2000.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag New York, 1977.

[HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12(3):315–364, 2000.

[How96] Everett W. Howe. The Weil pairing and the Hilbert symbol. *Math. Ann.*, 305:387–392, 1996.

[How14] Everett W. Howe. Genus-2 Jacobians with torsion points of large order. *Bulletin of the London Mathematical Society*, 47(1):127–135, 2014.

[HZ02] Everett W Howe and Hui June Zhu. On the Existence of Absolutely Simple Abelian Varieties of a Given Dimension over an Arbitrary Field. *Journal of Number Theory*, 92:139–163, 2002.

[Igu60] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.

[Iit82] S. Iitaka. *Algebraic Geometry: An Introduction to Birational Geometry of Algebraic Varieties*. Springer-Verlag New York, 1982.

[Kro15] Max Kronberg. *Explicit Construction of Rational Torsion Divisors on Jacobians of Curves*. PhD thesis, Universität Oldenburg, 2015.

[Kro17] Max Kronberg. Constructing Superelliptic Curves with non-trivial rational torsion on their Jacobians. 2017. arXiv, `http://arxiv.org/abs/1707.04042`.

[Len82] Lenstra, A. K. and Lenstra, H. W. and Lovász, L. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, Dec 1982.

[Lep92] Franck Leprévost. Torsion sur des familles de courbes de genre g. *manuscripta mathematica*, 75:303–326, 1992.

[Lep95] Franck Leprévost. Jacobiennes de certaines courbes de genre 2: torsion et simplicité. *Journal de Theorie des Nombres de Bordeaux*, 7(1):283–306, 1995.

[Lep97] Franck Leprévost. Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$. *manuscripta mathematica*, 92:47–63, 1997.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186, 1977.

[Mes09] Jean-Francois Mestre. Couples de Jacobiennes isogénes de courbes hyperelliptiques de genre arbitraire. 2009. arXiv, `http://arxiv.org/abs/0902.3470`.

[Mil] J. S. Milne. Abelian Varieties. Lecture notes `http://www.jmilne.org/math/CourseNotes/av.html` (accessed 8/7/2018).

[Mil06] J. S. Milne. *Arithmetic Duality Theorems*. Booksurge Publishing, 2006.

[Mor22] Louis Joel Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[Mül14] J. Steffen Müller. Explicit Kummer varieties of hyperelliptic Jacobian threefolds. *LMS Journal of Computation and Mathematics*, 17(1):496–508, 2014.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Inventiones Mathematicae*, 1(4):287–354, 1966.

[Mum70] David Mumford. *Abelian Varieties*. Tata Institute of Fundamental Research Publications, 1970.

[Mum07] David Mumford. *Tata Lectures on Theta II*. Birkhäuser Basel, 2007.

[MZ13] Daniel Miller and David Zywina. Arithmetic of curves, 2013. Lecture Notes Math 7390 (Cornell University) `https://github.com/dkmiller/arith-curve` (accessed 8/7/2018).

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.

[Nic18] Chris Nicholls. Accompanying code for the thesis. Research Thesis Digital Submission, 2018.

[Oga94] Hiroyuki Ogawa. Curves of Genus 2 with a Rational Torsion Divisor of Order 23. *Proc. Japan Acad.*, 70(9):295–298, 1994.

[Pla14] V. P. Platonov. Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field. *Russian Mathematical Surveys*, 69(1):1–34, 2014.

[PP12a] V. P. Platonov and M. M. Petrunin. New orders of torsion points in Jacobians of curves of genus 2 over the rational number field. *Doklady Mathematics*, 85(2):286–288, 2012.

[PP12b] V. P. Platonov and M. M. Petrunin. On the Torsion Problem in Jacobians of Curves of Genus 2 over the Rational Number Field. *Doklady Mathematics*, 86(2):642–643, 2012.

[PS97] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *Journal fur die Reine und Angewandte Mathematik*, 488:141–188, 1997.

[PZP13] V. P. Platonov, V. S. Zhgun, and M. M. Petrunin. On the simplicity of Jacobians for hyperelliptic curves of genus 2 over the field of rational numbers with torsion points of high order. *Doklady Mathematics*, 87(3):318–321, 2013.

[Ric37] F. Richelot. De transformatione integralium abelianorum primi ordinis commentatio. *J. Reine Angew. Math.*, 16:221–341, 1837.

[Sch98] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Mathematische Annalen*, 471:447–471, 1998.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer-Verlag New York, 1979.

[Sha] Romyar Sharifi. Groups and Galois Cohomology. Lecture Notes `http://math.ucla.edu/~sharifi/lecnotes.html` (accessed 8/7/2018).

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves (Second Edition)*. Springer-Verlag New York, 2009.

[Smi05] Benjamin Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005.

[SS97] N. P. Smart and S. Siksek. On the complexity of computing the 2-Selmer group of an elliptic curve. *Glasgow Mathematics Journal*, 39(1997):251–257, 1997.

[Sto95] Michael Stoll. Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil group of rank at least 19. *C. R. Acad. Sci. Paris, Série I*, 321(10):1341–1345, 1995.

[Sto17] Michael Stoll. An Explicit Theory of Heights for Hyperelliptic Jacobians of Genus Three. In *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*, pages 665–715. Springer-Verlag, 2017.

[Stu00] Andrew Stubbs. *Hyperelliptic Curves*. PhD thesis, University of Liverpool, 2000.

[Tat66] John Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones Mathematicae*, (2):134–144, 1966.

[VA] Anthony Várilly-Alvarado. Arithmetic of del Pezzo Surfaces. Lecture notes from Arithmetic of Surfaces, Leiden 2010. `http://math.rice.edu/~av15/Files/LeidenLectures.pdf` (accessed 8/7/2018).

[Vac05] Francesco Vaccarino. The ring of multisymmetric functions. *Annales de l'Institut Fourier*, 55(3):717–731, 2005.

[Vak17] Ravi Vakil. The Rising Sea: Foundations Of Algebraic Geometry Notes, 2017. Lecture Notes `http://math.stanford.edu/~vakil/216blog/` (November 18 2017 version, accessed 8/7/2018).

[Wam98] Paul van Wamelen. Equations for the Jacobian of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 350(8):3083–3106, 1998.

[Wei29] Andre Weil. L'arithmétique sur les courbes algébriques. *Acta Arithmetica*, 52:281–315, 1929.

Appendix A

Group cohomology

Galois cohomology is defined as (profinite) group cohomology with respect to the Galois group. We define group cohomology and refer to Sharifi's excellent notes for the definition of Galois cohomology ([Sha]).

Let G be a group, and let M be a G-module. In this section, we write the group action multiplicatively: if $m \in M$ and $g \in G$, we write $g \cdot m$ for the action of g on m. For each $n \geq 0$, we define the *n-cochains* $C^n(G, M)$ as functions $\varphi\colon G^n \to M$. The *cochain operator* $d^n\colon C^n \to C^{n+1}$ is given by

$$\begin{aligned} d^n(\varphi)(g_1, \ldots, g_{n+1}) &= g_1 \cdot \varphi(g_2, \ldots, g_{n+1}) \\ + \sum_{i=1}^{n} (-1)^i \varphi(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) & \\ + (-1)^{n+1} \varphi(g_1, \ldots, g_n). & \end{aligned} \tag{A.1}$$

Remark A.0.1. *Only the cases $n = 0$ and $n = 1$ are relevant for us.*

In particular, $C^0(G, M) = M$, where we interpret elements of M as functions from the empty product G^0 to M. To be clear, the 0th cochain map is given by $d^0(\varphi)(g_1) = g_1 \cdot \varphi - \varphi$. Since $\varphi \in C^0(G, M) = M$ is just an element of M, this implies $d^0(m)$ is the map

$$\begin{aligned} d^0(m)\colon G &\to M \\ g &\mapsto g \cdot m - m. \end{aligned} \tag{A.2}$$

The sequence

$$C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \to \cdots \tag{A.3}$$

forms a cochain complex; that is, $d^{i+1} \circ d^i = 0$ for each $i \geq 0$. We define the *cohomology group* $H^i(G, M)$ as the cohomology group in the usual way for this cochain complex.

Definition A.0.2. *We define the ith cohomology group $H^i(G, M)$ as $\ker d^i / \operatorname{im} d^{i-1}$ for each $i \geq 0$.*

The groups $H^0(G, M)$ and $H^1(G, M)$ The important cohomology groups to understand for descent are H^0 and H^1.

We have $H^0(G, M) = \ker d^0 / \operatorname{im} d^{-1}$. Since $d^{-1} = 0$, an element of $H^0(G, M)$ is represented by a 0-cochain $\varphi \in C^0(G, M)$ such that $d^0(\varphi) = 0$. This is an element $m \in M$ such that $g \cdot m = m$ for all $g \in G$. In other words, $H^0(G, M) = M^G$: the elements of M that are fixed under the action of G.

An element of $H^1(G, M)$ is represented by a 1-cochain $\varphi\colon G \to M$ such that $d^1(\varphi) = 0$. Using the explicit description of the cochain differential, we see that

$$d^1(\varphi)(g_1, g_2) = g_1\varphi(g_2) - \varphi(g_1 g_2) + \varphi(g_1). \tag{A.4}$$

Thus, $d^1(\varphi) = 0$ exactly when $\varphi(g_1 g_2) = \varphi(g_1) + g_1\varphi(g_2)$ for all $g_1, g_2 \in G$. Moreover, given $m \in C^0(G, M) = M$, we have $d^0(m)(g) = g \cdot m - m$. Thus

$$\operatorname{im} d^0 = \{\varphi\colon G \to M \mid \text{ there is } m \in M \text{ such that } \varphi(g) = g \cdot m - m\}. \tag{A.5}$$

It follows that

$$H^1(G, M) = \frac{\{\varphi\colon G \to M \mid \varphi(g_1 g_2) = \varphi(g_1) + g_1\varphi(g_2)\}}{\{\varphi\colon G \to M \mid \text{ there is } m \in M \text{ such that } \varphi(g) = g \cdot m - m\}}. \tag{A.6}$$

The connecting homomorphisms Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a short exact sequence in group cohomology. In particular, the maps are homomorphisms of G-modules, so $f(g \cdot x) = g \cdot f(x)$ for all $x \in M$ and $g \in G$.

For each $i \geq 0$, there are natural G-module homomorphisms $C^i(G, L) \to C^i(G, M)$ and $C^i(G, M) \to C^i(G, N)$, induced by f and g, respectively. Indeed, given $\varphi\colon G^i \to L$, we get $f \circ \varphi\colon G^i \to M \in C^i(G, M)$. The map $C^i(G, M) \to C^i(G, N)$ is given by post-composition with g

$$\begin{array}{ccc} G^i & & \\ \downarrow{\scriptstyle \psi} & \searrow^{f\circ\psi} & \\ L & \xrightarrow{f} & M \end{array} \tag{A.7}$$

Proposition A.0.3. *The functor $C^i(G, \cdot)$ is exact from the category of G-modules and G-module homomorphisms to the category of abelian groups and maps of sets.*

Proof. Since $C^i(G, \cdot)$ is simply $\operatorname{Hom}(G^i, \cdot)$, it is a left exact functor. Thus we just have to show that if $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence, then the induced map $C^i(G, B) \xrightarrow{g} C^i(G, C)$ is surjective.

Since the elements of $C^i(G, B)$ are just pointwise maps $G^i \to B$, we can define a map as follows. Let $\varphi\colon G^i \to C$ be an element of $C^i(G, C)$. Then for $(g_1, \ldots, g_i) \in G^i$, define $\psi(g_1, \ldots, g_i)$ as any element of B such that $g(\psi(g_1, \ldots, g_i)) = \varphi(g_1, \ldots, g_i)$; this is possible as g is surjective. □

Consider the short exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0. \tag{A.8}$$

For each $i \geq 0$, Proposition A.0.3 gives the following diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^i(G, A) & \xrightarrow{f} & C^i(G, B) & \xrightarrow{g} & C^i(G, C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & C^{i+1}(G, A) & \xrightarrow{f} & C^{i+1}(G, B) & \xrightarrow{g} & C^{i+1}(G, C) & \longrightarrow & 0 \end{array} \tag{A.9}$$

Applying the snake lemma twice gives a new diagram with exact rows. Explicitly, the bottom row comes from the sequence of kernels from the snake lemma on the above diagram at $i + 1$ instead of i, and the top row comes from the sequence of cokernels from the snake lemma applied to the above diagram at $i - 1$ instead of i.

$$\begin{array}{ccccccccc} & & \frac{C^i(G,A)}{\operatorname{im} d_A^{i-1}} & \xrightarrow{f} & \frac{C^i(G,B)}{\operatorname{im} d_B^{i-1}} & \xrightarrow{g} & \frac{C^i(G,C)}{\operatorname{im} d_C^{i-1}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & \ker d_A^{i+1} & \xrightarrow{f} & \ker d_B^{i+1} & \xrightarrow{g} & \ker d_C^{i+1} & & \end{array} \tag{A.10}$$

Applying the snake lemma once more gives a homomorphism $\delta^i\colon H^i(G, C) \to H^{i+1}(G, A)$, called the connecting homomorphism. This fits into an exact sequence

$$\begin{aligned} &H^i(G, A) \xrightarrow{f} H^i(G, B) \xrightarrow{g} H^i(G, C) \\ &\xrightarrow{\delta^i} H^{i+1}(G, A) \xrightarrow{f} H^{i+1}(G, B) \xrightarrow{g} H^{i+1}(G, C). \end{aligned} \tag{A.11}$$

These exact sequences splice together to give a long exact sequence in group cohomology. The coboundary map $\delta^i\colon H^i(G, C) \to H^{i+1}(G, A)$ can be explicitly defined as follows. Let $\varphi \in H^i(G, C)$ be represented by $\varphi\colon G^i \to C$. Choose $\psi\colon G^i \to B$ lifting φ; this is possible by Proposition A.0.3. Then define $\delta^i(\varphi) = f^{-1}(d_B^i(\psi))$. A simple diagram chase shows that this is well-defined.

Appendix B

Addition by a 2-torsion divisor

The following proposition and proof are due to Cassels and Flynn in [CF96].

Proposition B.0.1 ([CF96], Lemma 2.1)**.** *Let $\mathcal{J}$ be the Jacobian of the genus 2 curve $\mathcal{C}\colon y^2 = g(x)h(x)$, where $g(x) = g_2x^2+g_1x+g_0$ is a quadratic and $h(x) = h_4x^4+\cdots+h_0$ is a quartic. Let $D \in \mathcal{J}$ and let T be the 2-torsion divisor corresponding to $g(x)$. Then $\xi(D+T) = W\xi(D)$, where W is the matrix*

$$\begin{pmatrix} g_2^2h_0 + g_0g_2h_2 - g_0^2h_4 & g_0g_2h_3 - g_0g_1h_4 & g_1g_2h_3 - g_1^2h_4 + 2g_0g_2h_4 & g_2 \\ -g_0g_2h_1 - g_0g_1h_2 + g_0^2h_3 & g_2^2h_0 - g_0g_2h_2 + g_0^2h_4 & g_2^2h_1 - g_1g_2h_2 - g_0g_2h_3 & -g_1 \\ -g_1^2h_0 + 2g_0g_2h_0 + g_0g_1h_1 & -g_1g_2h_0 + g_0g_2h_1 & -g_2^2h_0 + g_0g_2h_2 + g_0^2h_4 & g_0 \\ w_1 & w_2 & w_3 & w_4 \end{pmatrix},$$

and

$$\begin{aligned} w_1 &= -g_2(g_0^2h_1h_3 - g_0g_1h_0h_3 + g_0g_1h_1h_2 + 4g_0g_2h_0h_2 - g_0g_2h_1^2 - g_1^2h_0h_2 \\ &\quad + g_1g_2h_0h_1) \\ w_2 &= -2g_0^2g_2h_1h_4 + g_0g_1^2h_1h_4 + 4g_0g_1g_2h_0h_4 - g_0g_1g_2h_1h_3 - 2g_0g_2^2h_0h_3 \\ &\quad - g_1^3h_0h_4 + g_1^2g_2h_0h_3 \\ w_3 &= -g_0(g_0g_1h_3h_4 + 4g_0g_2h_2h_4 - g_0g_2h_3^2 - g_1^2h_2h_4 - g_1g_2h_1h_4 + g_1g_2h_2h_3 \\ &\quad + g_2^2h_1h_3) \\ w_4 &= -g_0^2h_4 - g_0g_2h_2 - g_2^2h_0. \end{aligned} \tag{B.1}$$

Proof. We outline the steps to derive W_T and refer to Lemma 2.1 in [CF96] for more details. Let $f(x) = g(x)h(x)$. Let $\mathfrak{m}_\infty$ be the divisor

$$\mathfrak{m}_\infty = \begin{cases} 2\infty, & \text{if } \deg f = 5, \\ \infty^+ + \infty^-, & \text{if } \deg f = 6, \end{cases} \tag{B.2}$$

as in Equation (2.12). Let $D = (x_1, y_1)+(x_2, y_2)-\mathfrak{m}_\infty$ and let $T = (x_3, 0)+(x_4, 0)-\mathfrak{m}_\infty$. To add points on the Jacobian of a genus 2 curve, we find a cubic through the points

$(x_1, y_1), \ldots, (x_4, y_4)$, which then intersects $\mathcal{C}$ in two further points: $(x_5, -y_5), (x_6, -y_6)$. We then have $D + T = (x_5, y_5) + (x_6, y_6) - \mathfrak{m}_\infty$ (the images of the divisors on the Jacobian are equal).

We first find the quadratic $PX^2 - QX + R$ with roots x_5, x_6. Let $\xi'_0, \ldots, \xi'_3$ denote the Kummer coordinates of $D+T$. Then $(\xi'_0, \xi'_1, \xi'_2) = (P, Q, R)$ as projective matrices, since $\xi'_1/\xi'_0 = x_5 + x_6 = Q/P$ and $\xi'_2/\xi'_0 = x_5 x_6 = R/P$. We will then determine ξ'_3 separately.

We can express the cubic through $(x_1, y_1), (x_2, y_2), (x_3, 0), (x_4, 0)$ as

$$y = g(x)\ell(x), \tag{B.3}$$

where $y = \ell(x)$ is the line through the points $(x_1, \frac{y_1}{g(x_1)}), (x_2, \frac{y_2}{g(x_2)})$. Explicitly,

$$\ell(x) = \frac{x - x_1}{x_2 - x_1}\frac{y_1}{g(x_1)} + \frac{x - x_2}{x_1 - x_2}\frac{y_2}{g(x_2)}. \tag{B.4}$$

Substituting this cubic into the equation $y^2 = g(x)h(x)$ of the curve gives

$$g(x)\left(g(x)\ell(x)^2 - h(x)\right) = 0, \tag{B.5}$$

which is the resultant of the curve with the cubic. The roots of the resultant are precisely the x-coordinates of the intersections, counting multiplicities. We aim to determine the quadratic factor of this expression that has roots x_5, x_6. The factor $g(x)$ is from the points $(x_3, 0), (x_4, 0)$, so we examine the expression in parentheses. This gives the equation

$$\begin{aligned} g(x)\left(\frac{(x - x_1)^2 y_2^2}{(x_2 - x_1)^2 g(x_2)^2} - 2\frac{(x - x_1)(x - x_2)y_1 y_2}{(x_2 - x_1)^2 g(x_1) g(x_2)} + \frac{(x - x_2)^2 y_1^2}{(x_1 - x_2)^2 g(x_1)^2}\right) \\ - h(x) = 0. \end{aligned} \tag{B.6}$$

Replacing y_i^2 with $g(x_i)h(x_i)$ for $i = 1, 2$, and clearing denominators, we have the equation

$$q(x, x_1, x_2) - 2(x - x_1)(x - x_2)g(x)y_1 y_2 = 0, \tag{B.7}$$

where

$$\begin{aligned} q(x, x_1, x_2) = g(x)\left((x - x_1)^2 h(x_2)g(x_1) + (x - x_2)^2 h(x_1)g(x_2)\right) \\ - h(x)(x_2 - x_1)^2 g(x_1)g(x_2). \end{aligned} \tag{B.8}$$

Since $q(x_1, x_1, x_2) = q(x_2, x_1, x_2) = 0$, we can write

$$q(x, x_1, x_2) = (x - x_1)(x - x_2)r(x, x_1, x_2) \tag{B.9}$$

for some polynomial r.

In particular, the x-coordinates of $D + T$ satisfy

$$r(x, x_1, x_2) - 2g(x)y_1y_2 = 0. \tag{B.10}$$

This is the quadratic $PX^2 - QX + R$ from before, but to ensure that P, Q, R are functions in $\mathscr{O}_{\mathcal{J}}(\Theta^+_{\mathcal{J}} + \Theta^-_{\mathcal{J}})$ we scale the equation by $(x_2 - x_1)^2$. Thus, define P, Q, R by the equation

$$PX^2 - QX + R \coloneqq \frac{r(x, x_1, x_2) - 2g(x)y_1y_2}{(x_2 - x_1)^2}, \tag{B.11}$$

which makes sense since r is quadratic in x. Then the coefficients P, Q, R are in $\mathscr{O}_{\mathcal{J}}(\Theta^+_{\mathcal{J}} + \Theta^-_{\mathcal{J}})$, so are linear combinations of $\xi_0(D), \xi_1(D), \xi_2(D), \xi_3(D)$.

We find the coefficients of $\xi_0, \xi_1, \xi_2, \xi_3$ by inspection. First note that the coefficient of ξ_3 is simply the coefficient of $-2y_1y_2$, and then determine the coefficient of $\xi_2 = \frac{x_1x_2(x_2-x_1)^2}{(x_2-x_1)^2}$, and continue in this way.

Now we find the fourth row of W. Since W is an involution, W^2 is a multiple of the identity, say $W^2 = cI$. Squaring the matrix we currently have with fourth row set to w_1, w_2, w_3, w_4 (to be found), we see that the $(2,1), (1,2), (1,3), (1,4)$ entries are linear in w_1, w_2, w_3, w_4 respectively, and so determine the w_i. This gives the fourth row of W as described in the proposition. □

Appendix C

Lemmas

In this appendix we prove some lemmas whose details we did not want to include in the main body of the thesis.

Lemma (Lemma 6.9.13)**.** *Let $D = \langle a(x), b(x), d\rangle$ be a nontrivial divisor on the genus 2 curve $y^2 = f(x)$ such that $2D \sim 0$. Then $b(x) \equiv 0 \pmod{a(x)}$ and $f(x) \equiv 0 \pmod{a(x)}$.*

Proof. We first deal with the case $\deg f = 6$. If $\deg a(x) = 1$, then D is the divisor $\infty^+ - \infty^-$ or its negation.

Then we must have $\deg a(x) = 2$, and the notation $\langle a(x), b(x), 2\rangle$ means the divisor $(\alpha_1, b(\alpha_1)) + (\alpha_2, b(\alpha_2)) - \infty^+ - \infty^-$. If $2D \sim 0$, then there is a function $\varphi \in \mathcal{L}(2(\infty^+ + \infty^-))$ such that $\operatorname{div}\varphi = 2D$ (equality of divisors). The Riemann-Roch theorem shows that φ is in the K-vector space spanned by $\{1, x, x^2\}$. In the affine chart $y^2 = f(x)$, the solution to $\varphi(x) = 0, y^2 = f(x)$ is $\sum_{i=1}^{2}((\gamma_i, \delta_i) + (\gamma_i, -\delta_i))$, where γ_1, γ_2 are the roots of $\varphi(x) = 0$, and $\delta_i^2 = f(\gamma_i)$. Since $\operatorname{div}\varphi = 2D$, the divisors are equal in the affine chart:

$$2(\alpha_1, b(\alpha_1)) + 2(\alpha_2, b(\alpha_2)) = (\gamma_1, \delta_1) + (\gamma_1, -\delta_1) + (\gamma_2, \delta_2) + (\gamma_2, -\delta_2). \tag{C.1}$$

Thus there is a relabelling of the indices such that $(\gamma_1, \delta_1) = (\alpha_1, b(\alpha_1))$, and thus $\delta_1 = -\delta_1$, so $\delta_1 = 0$. Hence $b(\alpha_1) = 0$ also. Similarly, $b(\alpha_2) = 0$. This shows that $a(x)$ divides $b(x)$. But also $0 = \delta_i^2 = f(\alpha_i)$, for $i = 1, 2$, so that $a(x)$ divides $f(x)$ also.

Suppose now that $\deg f$ equals 5. The case $\deg a(x) = 2$ is exactly the same as above. Consider when $\deg a(x) = 1$, say $a(x) = x - \alpha$, without loss of generality. Then $D = (\alpha, \beta) - \infty$. Now $2D \sim 0$ if and only if there is $\varphi \in \mathcal{L}(2\infty)$ such that $\operatorname{div}\varphi = 2(\alpha, \beta) - 2\infty$. Thus up to a constant, $\varphi = x - \gamma$ for some $\gamma \in K$. Then the divisor of φ in the affine chart is $(\gamma, \delta) + (\gamma, -\delta)$, where $\delta^2 = f(\gamma)$. Since this equals $2P$, we have $\delta = -\delta$ and $\alpha = \gamma$. It follows that $a(x)$ divides $f(x)$ and, since $\delta = b(\alpha)$, we have $a(x)$ divides $b(x)$ also. □

Appendix D

Power series

We defined the local power series in Section 5.4.3. They are given as follows.

$$\begin{aligned} s_3 = {} & 4s_1^6f_2f_6 - s_1^6f_3f_5 + 2s_1^6f_4^2 + 8s_1^5s_2f_1f_6 + 18s_1^4s_2^2f_0f_6 + s_1^4s_2^2f_1f_5 \\ & - s_1^4f_4 + 4s_1^3s_2^3f_0f_5 + 2s_1^2s_2^4f_0f_4 + s_1^2 + 2s_2^6f_0f_2 - s_2^4f_0 + \mathcal{O}(\geq 7) \end{aligned} \tag{D.1}$$

$$\begin{aligned} s_4 = {} & s_1^6f_3f_6 + 4s_1^5s_2f_2f_6 + 9s_1^4s_2^2f_1f_6 + s_1^4s_2^2f_2f_5 + 20s_1^3s_2^3f_0f_6 + 3s_1^3s_2^3f_1f_5 \\ & + 9s_1^2s_2^4f_0f_5 + s_1^2s_2^4f_1f_4 + 4s_1s_2^5f_0f_4 + s_1s_2 + s_2^6f_0f_3 + \mathcal{O}(\geq 7) \end{aligned} \tag{D.2}$$

$$\begin{aligned} s_5 = {} & 2s_1^6f_4f_6 + 2s_1^4s_2^2f_2f_6 - s_1^4f_6 + 4s_1^3s_2^3f_1f_6 + 18s_1^2s_2^4f_0f_6 + s_1^2s_2^4f_1f_5 \\ & + 8s_1s_2^5f_0f_5 + 4s_2^6f_0f_4 - s_2^6f_1f_3 + 2s_2^6f_2^2 - s_2^4f_2 + s_2^2 + \mathcal{O}(\geq 7) \end{aligned} \tag{D.3}$$

$$\begin{aligned} s_6 = {} & 6s_1^7f_2f_6 - s_1^7f_3f_5 + 2s_1^7f_4^2 + 13s_1^6s_2f_1f_6 + 2s_1^6s_2f_2f_5 - 2s_1^6s_2f_3f_4 \\ & + 30s_1^5s_2^2f_0f_6 + 7s_1^5s_2^2f_1f_5 - 2s_1^5s_2^2f_2f_4 - s_1^5f_4 + 18s_1^4s_2^3f_0f_5 \\ & + s_1^4s_2^3f_1f_4 + s_1^4s_2f_3 + 10s_1^3s_2^4f_0f_4 + 3s_1^3s_2^4f_1f_3 - 2s_1^3s_2^4f_2^2 \\ & + 2s_1^3s_2^2f_2 + s_1^3 + 6s_1^2s_2^5f_0f_3 - 3s_1^2s_2^5f_1f_2 + 3s_1^2s_2^3f_1 - 4s_1s_2^6f_0f_2 \\ & + s_1s_2^6f_1^2 + 3s_1s_2^4f_0 + s_2^7f_0f_1 + \mathcal{O}(\geq 8) \end{aligned} \tag{D.4}$$

$$\begin{aligned} s_7 = {} & 4s_1^6s_2f_2f_6 - s_1^6s_2f_3f_5 + 2s_1^6s_2f_4^2 + 8s_1^5s_2^2f_1f_6 + 22s_1^4s_2^3f_0f_6 + 2s_1^4s_2^3f_1f_5 \\ & - s_1^4s_2f_4 + 10s_1^3s_2^4f_0f_5 + 6s_1^2s_2^5f_0f_4 + s_1^2s_2 + 2s_1s_2^6f_0f_3 - 2s_1s_2^6f_1f_2 \\ & + s_1s_2^4f_1 - 2s_2^7f_0f_2 + s_2^5f_0 + \mathcal{O}(\geq 8) \end{aligned} \tag{D.5}$$

$$\begin{aligned} s_8 = {} & -2s_1^7f_4f_6 + 2s_1^6s_2f_3f_6 - 2s_1^6s_2f_4f_5 + 6s_1^5s_2^2f_2f_6 + s_1^5f_6 + 10s_1^4s_2^3f_1f_6 \\ & + s_1^4s_2f_5 + 22s_1^3s_2^4f_0f_6 + 2s_1^3s_2^4f_1f_5 + 8s_1^2s_2^5f_0f_5 + 4s_1s_2^6f_0f_4 \\ & - s_1s_2^6f_1f_3 + 2s_1s_2^6f_2^2 - s_1s_2^4f_2 + s_1s_2^2 + \mathcal{O}(\geq 8) \end{aligned} \tag{D.6}$$

$$
\begin{aligned}
s_9 = {} & s_1^7 f_5 f_6 - 4 s_1^6 s_2 f_4 f_6 + s_1^6 s_2 f_5^2 + 6 s_1^5 s_2^2 f_3 f_6 - 3 s_1^5 s_2^2 f_4 f_5 + 10 s_1^4 s_2^3 f_2 f_6 \\
& + 3 s_1^4 s_2^3 f_3 f_5 - 2 s_1^4 s_2^3 f_4^2 + 3 s_1^4 s_2 f_6 + 18 s_1^3 s_2^4 f_1 f_6 + s_1^3 s_2^4 f_2 f_5 \\
& + 3 s_1^3 s_2^2 f_5 + 30 s_1^2 s_2^5 f_0 f_6 + 7 s_1^2 s_2^5 f_1 f_5 - 2 s_1^2 s_2^5 f_2 f_4 + 2 s_1^2 s_2^3 f_4 \\
& + 13 s_1 s_2^6 f_0 f_5 + 2 s_1 s_2^6 f_1 f_4 - 2 s_1 s_2^6 f_2 f_3 + s_1 s_2^4 f_3 + 6 s_2^7 f_0 f_4 - s_2^7 f_1 f_3 \\
& + 2 s_2^7 f_2^2 - s_2^5 f_2 + s_2^3 + \mathcal{O}(\geq 8)
\end{aligned} \tag{D.7}
$$

$$
\begin{aligned}
s_{10} = {} & 8 s_1^8 f_2 f_6 - 2 s_1^8 f_3 f_5 + 5 s_1^8 f_4^2 + 16 s_1^7 s_2 f_1 f_6 + 36 s_1^6 s_2^2 f_0 f_6 + 2 s_1^6 s_2^2 f_1 f_5 \\
& - 2 s_1^6 f_4 + 8 s_1^5 s_2^3 f_0 f_5 + 6 s_1^4 s_2^4 f_0 f_4 + s_1^4 + 4 s_1^2 s_2^6 f_0 f_2 - 2 s_1^2 s_2^4 f_0 \\
& + s_2^8 f_0^2 + \mathcal{O}(\geq 9)
\end{aligned} \tag{D.8}
$$

$$
\begin{aligned}
s_{11} = {} & s_1^8 f_3 f_6 - 3 s_1^8 f_4 f_5 + 16 s_1^7 s_2 f_2 f_6 - 2 s_1^7 s_2 f_3 f_5 + 4 s_1^7 s_2 f_4^2 + 32 s_1^6 s_2^2 f_1 f_6 + \\
& 2 s_1^6 s_2^2 f_2 f_5 - 2 s_1^6 s_2^2 f_3 f_4 + s_1^6 f_5 + 76 s_1^5 s_2^3 f_0 f_6 + 8 s_1^5 s_2^3 f_1 f_5 - 2 s_1^5 s_2 f_4 \\
& + 23 s_1^4 s_2^4 f_0 f_5 + s_1^4 s_2^4 f_1 f_4 - s_1^4 s_2^4 f_2 f_3 + s_1^4 s_2^2 f_3 + 12 s_1^3 s_2^5 f_0 f_4 + 2 s_1^3 s_2 \\
& - 2 s_1^2 s_2^6 f_1 f_2 + s_1^2 s_2^4 f_1 + 4 s_1 s_2^7 f_0 f_2 - 2 s_1 s_2^5 f_0 - s_2^8 f_0 f_1 + \mathcal{O}(\geq 9)
\end{aligned} \tag{D.9}
$$

$$
\begin{aligned}
s_{12} = {} & 3 s_1^8 f_4 f_6 + 6 s_1^6 s_2^2 f_2 f_6 - s_1^6 s_2^2 f_3 f_5 + 2 s_1^6 s_2^2 f_4^2 - s_1^6 f_6 + 12 s_1^5 s_2^3 f_1 f_6 \\
& + 37 s_1^4 s_2^4 f_0 f_6 + 2 s_1^4 s_2^4 f_1 f_5 + s_1^4 s_2^4 f_2 f_4 - s_1^4 s_2^2 f_4 + 12 s_1^3 s_2^5 f_0 f_5 + 6 s_1^2 s_2^6 f_0 f_4 \\
& - s_1^2 s_2^6 f_1 f_3 + 2 s_1^2 s_2^6 f_2^2 - s_1^2 s_2^4 f_2 + s_1^2 s_2^2 + 3 s_2^8 f_0 f_2 - s_2^6 f_0 + \mathcal{O}(\geq 9)
\end{aligned} \tag{D.10}
$$

$$
\begin{aligned}
s_{13} = {} & - s_1^8 f_5 f_6 + 4 s_1^7 s_2 f_4 f_6 - 2 s_1^6 s_2^2 f_4 f_5 + 12 s_1^5 s_2^3 f_2 f_6 - 2 s_1^5 s_2 f_6 + 23 s_1^4 s_2^4 f_1 f_6 \\
& + s_1^4 s_2^4 f_2 f_5 - s_1^4 s_2^4 f_3 f_4 + s_1^4 s_2^2 f_5 + 76 s_1^3 s_2^5 f_0 f_6 + 8 s_1^3 s_2^5 f_1 f_5 + 32 s_1^2 s_2^6 f_0 f_5 \\
& + 2 s_1^2 s_2^6 f_1 f_4 - 2 s_1^2 s_2^6 f_2 f_3 + s_1^2 s_2^4 f_3 + 16 s_1 s_2^7 f_0 f_4 - 2 s_1 s_2^7 f_1 f_3 + 4 s_1 s_2^7 f_2^2 \\
& - 2 s_1 s_2^5 f_2 + 2 s_1 s_2^3 + s_2^8 f_0 f_3 - 3 s_2^8 f_1 f_2 + s_2^6 f_1 + \mathcal{O}(\geq 9)
\end{aligned} \tag{D.11}
$$

$$
\begin{aligned}
s_{14} = {} & s_1^8 f_6^2 + 4 s_1^6 s_2^2 f_4 f_6 + 6 s_1^4 s_2^4 f_2 f_6 - 2 s_1^4 s_2^2 f_6 + 8 s_1^3 s_2^5 f_1 f_6 + 36 s_1^2 s_2^6 f_0 f_6 \\
& + 2 s_1^2 s_2^6 f_1 f_5 + 16 s_1 s_2^7 f_0 f_5 + 8 s_2^8 f_0 f_4 - 2 s_2^8 f_1 f_3 + 5 s_2^8 f_2^2 - 2 s_2^6 f_2 \\
& + s_2^4 + \mathcal{O}(\geq 9)
\end{aligned} \tag{D.12}
$$

$$
\begin{aligned}
s_{15} = {} & - 12 s_1^8 f_4 f_6 + s_1^8 f_5^2 + 4 s_1^7 s_2 f_3 f_6 - 8 s_1^7 s_2 f_4 f_5 + 8 s_1^6 s_2^2 f_2 f_6 + 6 s_1^6 s_2^2 f_3 f_5 \\
& - 8 s_1^6 s_2^2 f_4^2 + 4 s_1^6 f_6 + 16 s_1^5 s_2^3 f_1 f_6 + 8 s_1^5 s_2^3 f_2 f_5 - 4 s_1^5 s_2^3 f_3 f_4 + 4 s_1^5 s_2 f_5 \\
& + 12 s_1^4 s_2^4 f_0 f_6 + 18 s_1^4 s_2^4 f_1 f_5 - 4 s_1^4 s_2^4 f_2 f_4 + s_1^4 s_2^4 f_3^2 + 4 s_1^4 s_2^2 f_4 + 16 s_1^3 s_2^5 f_0 f_5 \\
& + 8 s_1^3 s_2^5 f_1 f_4 - 4 s_1^3 s_2^5 f_2 f_3 + 4 s_1^3 s_2^3 f_3 + 8 s_1^2 s_2^6 f_0 f_4 + 6 s_1^2 s_2^6 f_1 f_3 - 8 s_1^2 s_2^6 f_2^2 \\
& + 4 s_1^2 s_2^4 f_2 + 4 s_1 s_2^7 f_0 f_3 - 8 s_1 s_2^7 f_1 f_2 + 4 s_1 s_2^5 f_1 - 12 s_2^8 f_0 f_2 + s_2^8 f_1^2 + 4 s_2^6 f_0 \\
& + \mathcal{O}(\geq 9).
\end{aligned} \tag{D.13}
$$

Appendix E

The embedding of the Jacobian of a genus 2 curve

Flynn found the following coordinates for the Jacobian of a genus 2 curve, as well as 72 quadratic equations in the coordinates that embed the Jacobian into $\mathbb{P}^{15}$ ([Fly90b]). Let $\mathcal{C}\colon y^2 = f(x)$ be a genus 2 curve. The coordinates are defined for a point on the Jacobian $\mathcal{J}$ of $\mathcal{C}$ of the form $(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$. We take $\infty^+ = \infty^- = \infty$ if $\deg f = 5$. By carefully taking limits, we can also define the coordinates in the case that one of $(x_1, y_1), (x_2, y_2)$ equals ∞^+ or ∞^-. The following coordinates are given in [CF96]. Note that they are only defined projectively. Following Flynn, we give them in reverse order. The functions $a_{15}, \ldots, a_{10}$ are symmetric functions in x_1, x_2:

$$a_{15} = (x_1 - x_2)^2, \tag{E.1}$$

$$a_{14} = 1, \tag{E.2}$$

$$a_{13} = x_1 + x_2, \tag{E.3}$$

$$a_{12} = x_1 x_2, \tag{E.4}$$

$$a_{11} = x_1 x_2 (x_1 + x_2), \tag{E.5}$$

$$a_{10} = (x_1 x_2)^2. \tag{E.6}$$

The functions $a_9, \ldots, a_6$ have the denominator $x_1 - x_2$:

$$a_9 = \frac{y_1 - y_2}{x_1 - x_2}, \tag{E.7}$$

$$a_8 = \frac{x_2 y_1 - x_1 y_2}{x_1 - x_2}, \tag{E.8}$$

$$a_7 = \frac{x_2^2 y_1 - x_1^2 y_2}{x_1 - x_2}, \tag{E.9}$$

$$a_6 = \frac{x_2^3 y_1 - x_1^3 y_2}{x_1 - x_2}. \tag{E.10}$$

The function a_5 is also equal to the Kummer coordinate ξ_3:

$$a_5 = \frac{F_0(x_1, x_2) - 2y_1y_2}{(x_1 - x_2)^2}, \tag{E.11}$$

where

$$\begin{aligned} F_0(x_1, x_2) = 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ + 2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3. \end{aligned} \tag{E.12}$$

We define a_4, a_3 as

$$a_4 = \frac{F_1(x_1, x_2) - (x_1 + x_2)y_1y_2}{(x_1 - x_2)^2}, \tag{E.13}$$

$$a_3 = x_1x_2a_5, \tag{E.14}$$

where

$$\begin{aligned} F_1(x_1, x_2) = f_0(x_1 + x_2) + 2f_1(x_1x_2) + f_2(x_1x_2)(x_1 + x_2) + 2f_3(x_1x_2)^2 \\ + f_4(x_1x_2)^2(x_1 + x_2) + 2f_5(x_1x_2)^3 + f_6(x_1x_2)^3(x_1 + x_2). \end{aligned} \tag{E.15}$$

We define a_2, a_1 as

$$a_2 = \frac{G(x_1, x_2)y_1 - G(x_2, x_1)y_2}{(x_1 - x_2)^3}, \tag{E.16}$$

$$a_1 = \frac{H(x_1, x_2)y_1 - H(x_2, x_1)y_2}{(x_1 - x_2)^3}, \tag{E.17}$$

where

$$\begin{aligned} G(x_1, x_2) = 4f_0 + f_1(x_1 + 3x_2) + f_2(2x_1x_2 + 2x_2^2) + f_3(3x_1x_2^2 + x_2^3) \\ + f_4(4x_1x_2^3) + f_5x_1(x_1x_2^3 + 3x_2^4) + 2f_6x_1(x_1x_2^4 + x_2^5) \end{aligned} \tag{E.18}$$

$$\begin{aligned} H(x_1, x_2) = 2f_0(x_1 + x_2) + f_1x_2(3x_1 + x_2) + 4f_2x_1x_2^2 + f_3x_1x_2^2(x_1 + 3x_2) \\ + 2f_4x_1x_2^3(x_1 + x_2) + f_5x_1x_2^4(3x_1 + x_2) + 4f_6x_1^2x_2^5. \end{aligned} \tag{E.19}$$

Finally,

$$a_0 = a_5^2. \tag{E.20}$$

We say that an expression in the coordinates is *even* if it is invariant under the map $\mathcal{J} \to \mathcal{J}$ given by $D \mapsto -D$, and *odd* if it changes sign. The coordinates a_i are even for $i = 0, 3, 4, 5, 10, 11, 12, 13, 14, 15$, and odd for $i = 1, 2, 6, 7, 8, 9$.

Appendix F

Examples of torsion curves

In this section we provide some examples of the curves we found whose Jacobians have large order torsion points. All of the curves listed here have geometrically simple Jacobians. We also found some torsion orders for which we couldn't verify the Jacobians were simple, but don't list these below.

Each line in the table is a pair $(N, f(x))$. This denotes that the Jacobian of the curve $y^2 = f(x)$ has a point of order N. We write (†) next to N for 1-parameter families of curves. In this case, $f(x)$ is an element of $\mathbb{Q}(t)[x]$ and t is the parameter.

We give one example for each N that we found in the following tables. Table F.1 contains the genus 3 curves and Tables F.2 and F.3 contain the genus 4 curves.

The MAGMA file `torsion/found_torsion_curves.m` in [Nic18] contains all of the curves in the tables.

Table F.1: Equations for genus 3 curves with large torsion

N	$f(x)$
25(†)	$-tx^7+(1/4t^2+7/2t+1/4)x^6+(-9/2t-3/2)x^5$ $+(5/2t+15/4)x^4+(-1/2t-5)x^3+15/4x^2-3/2x+1/4$
26(†)	$-tx^7+(t^2+3t+1/4)x^6+(-7/2t-5/4)x^5+(2t+41/16)x^4$ $+(-1/2t-11/4)x^3+13/8x^2-1/2x+1/16$
27(†)	$-tx^7+(1/4t^2+5/2t+9/4)x^6+(-3t-9)x^5+(2t+15)x^4$ $+(-1/2t-27/2)x^3+7x^2-2x+1/4$
28(†)	$-tx^7+(1/4t^2+2t+4)x^6+(-3t-12)x^5+(2t+17)x^4$ $+(-1/2t-14)x^3+7x^2-2x+1/4$
29	$192x^7-575x^6+612x^5+84x^4-846x^3+900x^2-432x+81$
30	$2000x^7+9129x^6-150x^5-1129x^4+196x^3-49x^2+2x+1$
31	$-648x^7+8521x^6-35304x^5+71928x^4-82404x^3+54432x^2-19440x+2916$
32(†)	$-tx^7+(4t^2+3t+1/4)x^6+(-4t^2-5t-1)x^5+(t^2+5t+7/4)x^4$ $+(-5/2t-7/4)x^3+(1/2t+17/16)x^2-3/8x+1/16$
33	$-32x^7+113x^6-558x^5+1285x^4-1188x^3+572x^2-144x+16$
34	$-12x^7+60x^6-124x^5+145x^4-102x^3+43x^2-10x+1$
35	$128x^7+625x^6-800x^5+556x^4-242x^3+68x^2-12x+1$
36	$-1008x^7+222916x^6-180548x^5+17681x^4+1060x^3+3074x^2+280x+49$
37	$4x^7-16x^6+16x^5+12x^4-32x^3+24x^2-8x+1$
38	$61x^7-112778711/518400x^6+196766153/259200x^5-51613919/51840x^4$ $+228689/1280x^3+3762053/5120x^2-2109807/3200x+301401/1600$
39	$336468610464x^7+1387158244945x^6-3746988201228x^5+2957749220766x^4$ $-626966305196x^3-197416827111x^2+44268024528x+18078415936$
40	$5x^7+4523081161/138384x^6-1452727141/11532x^5+842494611/3844x^4$ $-212383050/961x^3+130569435/961x^2-1509300/31x+8100$
41	$32x^7-23x^6-196x^5+504x^4-560x^3+340x^2-112x+16$
42(†)	$-tx^7+(9t^2+4t+1/4)x^6+(-27t^2-21/2t-1)x^5$ $+(141/4t^2+35/2t+2)x^4+(-51/2t^2-35/2t-5/2)x^3$ $+(43/4t^2+21/2t+2)x^2+(-5/2t^2-7/2t-1)x+1/4t^2+1/2t+1/4$
43	$64x^7-39x^6-10x^5-9x^4+12x^3-x^2-2x+1$
44	$48/25x^7+217/100x^6-41/5x^5+183/25x^4-71/50x^3-17/25x^2$ $+6/25x+9/100$
48	$1152x^7+2692x^6-9768x^5+7764x^4-848x^3-1104x^2+192x+64$
49	$2x^7+1/4x^6-5x^5+5/2x^4+3/2x^3-3/4x^2-1/2x+1/4$
50	$768x^7+34177x^6+3450x^5-1905x^4+364x^3+15x^2-6x+1$
52	$36x^7-11/25x^6+19452/25x^5-26366/25x^4-510x^3+1657x^2-1050x+225$
54	$1512x^7+3514057x^6-4215586x^5-178365x^4+2297474x^3-718955x^2$ $-285012x+142884$
56	$102x^7+1797601/16x^6-2190009/8x^5+4838871/16x^4-751187/4x^3$ $+1092687/16x^2-108129/8x+17689/16$
64	$x^8-8x^7+24x^6-32x^5+18x^4+8x^3-8x^2+1$
65	$x^8-14x^7+55x^6-48x^5+23x^4-14x^3+21x^2-12x+4$
72	$1600x^8-4800x^7+10800x^6-15920x^5+14580x^4-9720x^3$ $+4636x^2-1320x+225$
91	$x^8-6x^6+10x^5-x^4-6x^3+7x^2-2x+1$

Equations for genus 3 curves $y^2=f(x)$ with a point of order N.

Table F.2: Equations for genus 4 curves with large torsion

N	$f(x)$
18(†)	$-tx^9+(9t^2+3t+1/4)x^8+(-36t^2-15/2t-1/4)x^7+(78t^2+10t+1/16)x^6$ $+(-108t^2-15/2t)x^5+(103t^2+3t)x^4+(-68t^2-1/2t)x^3$ $+30t^2x^2-8t^2x+t^2$
28	$12x^9-27x^8+16x^7+34x^6-88x^5+99x^4-68x^3+30x^2-8x+1$
29	$-12x^9+72x^8-184x^7+296x^6-328x^5+253x^4-134x^3+47x^2-10x+1$
30	$-100x^{10}+500x^9-975x^8+700x^7+800x^6-2530x^5+3030x^4-2140x^3$ $+929x^2-230x+25$
31	$-3500x^{10}+14000x^9-17400x^8+10400x^7-1400x^6-1680x^5+1120x^4$ $-420x^3+161x^2-72x+16$
32	$-122500x^{10}+367500x^9-70475x^8-515150x^7+827275x^6-725570x^5$ $+448505x^4-200080x^3+60264x^2-10528x+784$
33	$121x^{10}+242x^8+2200x^7+363x^6+10242x^4-19879x^2+2200x+10000$
34	$121x^{10}+2200x^8-242x^7+10000x^6+121x^4+20000x^3+2200x^2+10000$
35	$-5252187500x^{10}+65055603600x^8-144761853600x^7+174015679600x^6$ $-136905623680x^5+75081959120x^4-29085521920x^3+7678244336x^2$ $-1238608672x+92236816$
40	$x^9-19/4x^8+9x^7-9/2x^6-10x^5+43/2x^4-41/2x^3+23/2x^2$ $-15/4x+9/16$
41(†)	$-tx^9+(1/4t^2+9/2t+1/4)x^8+(-2t^2-8t)x^7+(7t^2+7t)x^6$ $+(-14t^2-3t)x^5+(35/2t^2+1/2t)x^4-14t^2x^3+7t^2x^2$ $-2t^2x+1/4t^2$
42(†)	$-tx^9+(1/4t^2+4t+1)x^8+(-13/2t-7)x^7+(11/2t+85/4)x^6$ $+(-5/2t-73/2)x^5+(1/2t+155/4)x^4-26x^3+43/4x^2-5/2x+1/4$
43(†)	$-tx^9+(1/4t^2+7/2t+9/4)x^8+(-11/2t-27/2)x^7+(5t+141/4)x^6$ $+(-5/2t-105/2)x^5+(1/2t+49)x^4-59/2x^3+45/4x^2-5/2x+1/4$
44(†)	$-tx^9+(1/4t^2+3t+4)x^8+(-5t-20)x^7+(5t+45)x^6$ $+(-5/2t-60)x^5+(1/2t+52)x^4-30x^3+45/4x^2-5/2x+1/4$
45(†)	$-tx^9+(25/4t^2+5/2t+1/4)x^8+(-25t^2-5t)x^7+(50t^2+5t)x^6$ $+(-125/2t^2-5/2t)x^5+(105/2t^2+1/2t)x^4-30t^2x^3+45/4t^2x^2$ $-5/2t^2x+1/4t^2$
46	$-22032x^9+158560x^8-143760x^7+173156x^6-132248x^5+76060x^4$ $-37592x^3+14257x^2-3204x+324$
47	$18101600x^9+44730929x^8+32956830x^7-39627675x^6+13084550x^5$ $-2327500x^4+1016250x^3-231875x^2-18750x+15625$
48(†)	$-tx^9+(4t^2+4t+1/4)x^8+(-4t^2-8t-3/2)x^7$ $+(t^2+10t+4)x^6+(-15/2t-25/4)x^5+(3t+101/16)x^4$ $+(-1/2t-17/4)x^3+15/8x^2-1/2x+1/16$
49	$114688x^9+1358307329x^8-343595896x^7+69229804x^6-11773160x^5$ $+1619926x^4-176008x^3+16268x^2-1176x+49$
50	$3x^9-4x^8+35/4x^6-29/2x^5+13x^4-15/2x^3+45/16x^2-5/8x+1/16$
51	$12939264x^9+13931336779777x^8-1714477822592x^7+63564540820x^6$ $+289626064x^5-26171522x^4+7275424x^3+49348x^2+2704x+169$

Equations for genus 4 curves $y^2=f(x)$ with a point of order N.

Table F.3: Equations for genus 4 curves with large torsion

N	$f(x)$
52	$-81000x^9 + 352561x^8 - 702320x^7 + 893812x^6 - 751940x^5 + 476326x^4$ $-212120x^3 + 59800x^2 - 9500x + 625$
53	$1316551511808x^9 + 648204624757665x^8 - 1367676767024550x^7$ $+1411951052218683x^6 - 821802862194162x^5 + 276730856522437x^4$ $-42969861545628x^3 - 46817938620x^2 + 578238694272x + 21828289536$
54(†)	$-tx^9 + (9t^2 + 4t + 1/4)x^8 + (-36t^2 - 21/2t - 3/4)x^7$ $+(78t^2 + 35/2t + 13/16)x^6 + (-108t^2 - 35/2t - 3/8)x^5$ $+(103t^2 + 21/2t + 1/16)x^4 + (-68t^2 - 7/2t)x^3$ $+(30t^2 + 1/2t)x^2 - 8t^2x + t^2$
55	$36x^9 - 8x^8 - 412x^7 + 1488x^6 - 2752x^5 + 2992x^4 - 1752x^3$ $+588x^2 - 108x + 9$
57	$-32x^9 + 217x^8 - 316x^7 + 176x^6 + 4x^5 - 58x^4 + 28x^3 - 4x + 1$
58(†)	$-tx^9 + (9t^2 + 4t + 1/4)x^8 + (-18t^2 - 21/2t - 5/4)x^7$ $+(27t^2 + 35/2t + 131/48)x^6 + (-18t^2 - 35/2t - 41/12)x^5$ $+(9t^2 + 21/2t + 97/36)x^4 + (-7/2t - 11/8)x^3$ $+(1/2t + 4/9)x^2 - 1/12x + 1/144$
59	$32x^9 - 31x^8 - 94x^7 + 167x^6 - 34x^5 - 99x^4 + 68x^3 + 4x^2 - 16x + 4$
60	$64x^9 - 124x^8 - 4x^7 + 357x^6 - 606x^5 + 531x^4 - 272x^3 + 83x^2 - 14x + 1$
61	$42875000x^9 - 198879975x^8 + 379237950x^7 - 317077325x^6 - 56637680x^5$ $+423452755x^4 - 473231690x^3 + 275449309x^2 - 86799580x + 11764900$
62	$285768x^9 - 281655x^8 - 464724x^7 + 560274x^6 + 288312x^5 - 406811x^4$ $-157780x^3 + 289296x^2 - 96040x + 9604$
63	$-1500625000x^9 + 7061881225x^8 - 13627115600x^7 + 15374111600x^6$ $-11587219280x^5 + 6190389520x^4 - 2374328320x^3 + 626795456x^2$ $-101110912x + 7529536$
65	$4608x^9 + 9769x^8 - 30332x^7 + 8620x^6 + 23440x^5 - 18128x^4 - 704x^3$ $+5248x^2 - 2048x + 256$
66	$4608x^9 - 5180x^8 - 81372x^7 + 345417x^6 - 655244x^5 + 721812x^4$ $-493008x^3 + 207328x^2 - 49536x + 5184$
67	$16x^9 + 57x^8 - 158x^7 + 87x^6 + 38x^5 - 37x^4 - 14x^3 + 22x^2 - 8x + 1$
68	$105840x^9 + 61070164x^8 - 198101120x^7 + 390170548x^6 - 479406200x^5$ $+404864209x^4 - 226283960x^3 + 75818680x^2 - 13445600x + 960400$
72(†)	$-tx^9 + (16t^2 + 4t + 1/4)x^8 + (-48t^2 - 14t - 1)x^7$ $+(68t^2 + 28t + 5/2)x^6 + (-56t^2 - 35t - 4)x^5 + (28t^2 + 28t + 9/2)x^4$ $+(-8t^2 - 14t - 7/2)x^3 + (t^2 + 4t + 7/4)x^2 + (-1/2t - 1/2)x + 1/16$
74	$33012672x^9 - 33274127x^8 - 39094086x^7 + 120073119x^6 - 91425812x^5$ $+16264575x^4 + 18739482x^3 - 9702767x^2 - 2870304x + 1937664$
82	$-840x^9 + 7345x^8 - 26592x^7 + 54392x^6 - 70856x^5 + 61780x^4$ $-36320x^3 + 13936x^2 - 3168x + 324$
82	$-696x^9 + 4777x^8 - 11360x^7 + 14184x^6 - 10104x^5 + 3868x^4$ $-480x^3 - 144x^2 + 32x + 4$
88	$104448x^9 - 45884x^8 + 153912x^7 - 331572x^6 - 352236x^5$ $+1012380x^4 - 892728x^3 + 462645x^2 - 131418x + 21609$

Equations for genus 4 curves $y^2 = f(x)$ with a point of order N.