Explicit Endomorphisms and Correspondences

Benjamin Smith

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy in Pure Mathematics
at the University of Sydney, December 2005.

Summary

In this work, we investigate methods for computing explicitly with homomorphisms (and particularly endomorphisms) of Jacobian varieties of algebraic curves. Our principal tool is the theory of correspondences, in which homomorphisms of Jacobians are represented by divisors on products of curves. We give families of hyperelliptic curves of genus three, five, six, seven, ten and fifteen whose Jacobians have explicit isogenies (given in terms of correspondences) to other hyperelliptic Jacobians. We describe several families of hyperelliptic curves whose Jacobians have complex or real multiplication; we use correspondences to make the complex and real multiplication explicit, in the form of efficiently computable maps on ideal class representatives. These explicit endomorphisms may be used for efficient integer multiplication on hyperelliptic Jacobians, extending Gallant–Lambert–Vanstone fast multiplication techniques from elliptic curves to higher dimensional Jacobians. We then describe Richelot isogenies for curves of genus two; in contrast to classical treatments of these isogenies, we consider all the Richelot isogenies from a given Jacobian simultaneously. The inter-relationship of Richelot isogenies may be used to deduce information about the endomorphism ring structure of Jacobian surfaces; we conclude with a brief exploration of these techniques.

Statement

This thesis contains no material which has been accepted for the award of any other degree or diploma. All work in this thesis, except where duly attributed to another person, is believed to be original.

Thanks

This work would not have been possible without the support and advice of David Kohel. His patience, insight, and leadership have been a constant source of inspiration to me; it has been a privelege to learn mathematics with him.

Thanks to Sarah Jo Moore, for her patience, inspiration, love, and for bringing me back to earth; my family, especially Michael and Damien Smith, for their support; Martin Bright, Claus Fieker, Martine Girard, and Mike Harrison for answering so many questions; Paul O'Donnell, Dan Lalor, and all my housemates over the years, for giving me a home; Claire d'Este, Paul Hunter, and Holly Swisher for their understanding and postgraduate empathy; my friends, and `listserv@acl.arts.usyd.edu.au` — particularly Tom Murtagh, Gordon Childs, and Mark Wotton — for their trenchant insights (it's true: Richard Touches Creambar Wildly); Lady Jane, Figment, the Never Ends, and all the other bands I've played in over the last four years, for keeping me in time. Finally, thanks to the countless undergraduates of Sydney University I have taught over the last few years, for teaching me.

Contents

Chapter 1

Introduction

In this work, we investigate methods for computing explicitly with homomorphisms (and particularly endomorphisms) of Jacobian varieties of algebraic curves. Our principal tool is the theory of correspondences, in which homomorphisms of Jacobians are represented by divisors on products of curves. We give families of hyperelliptic curves of genus three, five, six, seven, ten and fifteen whose Jacobians have explicit isogenies (given in terms of correspondences) to other hyperelliptic Jacobians. We describe several families of hyperelliptic curves whose Jacobians have complex or real multiplication; we use correspondences to make the real multiplication explicit, in the form of efficiently computable maps on ideal class representatives. These explicit endomorphisms may be used for efficient integer multiplication on hyperelliptic Jacobians, extending the Gallant–Lambert–Vanstone fast multiplication from elliptic curves to higher dimensions. We then describe Richelot isogenies for curves of genus two; in contrast to classical treatments of these isogenies, we consider all the Richelot isogenies from a given Jacobian simultaneously. The inter-relationship of Richelot isogenies may be used to deduce information about the endomorphism ring structure of Jacobian surfaces; we conclude with a brief exploration of these techniques.

1.1 Overview

The remainder of this chapter sets out our basic notation and conventions. In **Chapter 2** we quickly survey the geometry of algebraic curves and their Jacobians. We define divisors and rational equivalence on curves and their products; we then describe abelian varieties and Jacobians, and outline effective arithmetic for hyperelliptic Jacobians, including a brief sketch of Gallant–Lambert–Vanstone (GLV) techniques for efficient integer multiplication on Jacobians. Finally, we describe Dickson polynomials (of the first kind), which will be needed in later chapters.

In **Chapter 3**, we describe the basic theory of correspondences of curves. Given a fixed pair of curves X and Y, a correspondence is defined to be a divisor on the surface $X \times Y$. Every correspondence induces a homomorphism from the Jacobian of X to the Jacobian of Y. The relationship between homomorphisms and correspondences is entirely analogous to the relationship between a morphism of curves and its graph. We describe these induced homomorphisms; the central result is Theorem 3.3.12, which gives an isomorphism between $\mathrm{Hom}(J_X, J_Y)$ and a certain quotient of the divisor group of $X \times Y$. We then define a composition operation for correspondences, which is a geometric realisation of the composition operation on induced homomorphisms. The composition induces a ring structure on the divisor group of $X \times X$, giving a geometric realisation of the endomorphism ring of J_X.

The principal tool for the analysis of the divisor group of a surface is intersection theory. **Chapter 4** surveys basic intersection theory on products of curves; the principal results are the definition of the intersection number (Theorem 4.1.1) and the *adjunction formula* (Theorem 4.2.1). Throughout, we apply the results to examples from the theory of correspondences.

The intersection number has a serious limitation, however: it is not well-defined on equivalence classes of correspondences inducing the same homomorphism. In **Chapter 5**, we construct a pairing on divisors on $X \times Y$ that is posititive definite on these equivalence classes (Definition 5.1.1). The key result is the Adjoint Theorem (Theorem 5.2.2), which implies that the pairing is equivalent to a twisted trace pairing on the space of homomorphisms

(Theorem 5.3.3). This gives a useful and explicit connection between the purely geometric intersection theory on $X \times Y$ and the arithmetic theory of $\mathrm{Hom}(J_X, J_Y)$. In the context of endomorphisms, this pairing was used by Weil as a foundational tool in his proof of the Riemann hypothesis for curves. We show how to use the pairing to determine when correspondences are $\mathbb{Z}$-linearly dependent (Proposition 5.4.1), and to express a correspondence in terms of a known basis (Algorithm 5.4.2).

We then turn our attention to correspondences of hyperelliptic curves, in **Chapter 6**. Hyperelliptic curves are double covers of projective lines, so we consider the relationship between correspondences of hyperelliptic curves and the induced correspondences of the covered lines. We also consider some cases of the inverse problem: which correspondences of projective lines lift to interesting correspondences of hyperelliptic curves? As an example, we exhibit hyperelliptic curves with cyclotomic complex multiplication in §6.3.1, and show how correspondences on these curves may be used to conduct efficient integer multiplication in their Jacobians. We also describe correspondences arising from the work of Cassou–Noguès and Couveignes [12] in §7.4. For each correspondence, we identify the induced isogeny.

We continue our investigation of hyperelliptic curves in **Chapter 7**, where we construct a number of families of hyperelliptic curves whose Jacobians have real multiplication. We make these real multiplications completely explicit, by providing correspondences representing the endomorphisms and constructing efficiently evaluable maps on the ideal class representation of the Jacobians in §7.2. In §7.3, we consider a class of curves originally described by Tautz, Top and Verberkmoes in [62], which have real multiplications derived from cyclotomic covers. In §7.4, we describe a family of curves over finite fields, with real multiplication induced by Artin–Schreier covers. Finally, in §7.5 we examine families of curves with real multiplication described by Mestre in [44]. To our knowledge, this work provides the first explicit realisations of the induced homomorphisms. These effective endomorphisms may be used to give efficient integer multiplications on the Jacobians.

In **Chapter 8**, we specialise to the case of curves of genus two. In particular, we consider Richelot isogenies, which split multiplication by two

on Jacobian surfaces. The explicit construction of these isogenies, due to Richelot, is classical. We extend the treatments of Flynn and Cassels [11] and of Bost and Mestre [5] to give a complete description of Richelot isogenies in terms of *quadratic splittings* (Definition 8.2.1), a new data structure which considerably simplifies the treatment of sets of Richelot isogenies and the correspondences that induce them.

We conclude our investigation in **Chapter 9** by examining graphs of Richelot isogenies, with a view to determining the endomorphism ring structure of a Jacobian surface. We give an algorithm for detecting certain cycles in the graph of k-rational Richelot isogenies (Algorithm 9.3.1), and give several examples of its application. This generalises the work of Kohel [35] and others from elliptic curves to Jacobian surfaces.

1.2 Notation and conventions

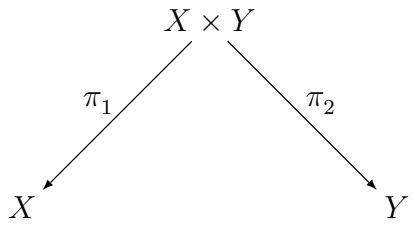
We fix the following notations and conventions:

- We denote the base field by k, its multiplicative group by $k^\times$, and its algebraic closure by $\overline{k}$. Unless otherwise stated, all schemes are k-schemes.

- Throughout, X, Y and Z will always denote reduced, irreducible, nonsingular projective algebraic curves over k. The (geometric) genus of X is denoted g_X. Note that the properties we assume of the curves X and Y imply that their geometric and arithmetic genera coincide. The *Jacobian variety* (hereafter *Jacobian*) of X is denoted J_X. The ring of endomorphisms of J_X is denoted by $\mathrm{End}(J_X)$.

- The product of X and Y (over $\mathrm{Spec}(k)$) is a surface, denoted by $X \times Y$. The projections from $X \times Y$ to its first and second factors are denoted

π_1 and π_2, respectively:



The restrictions of the projections π_1 and π_2 to a subscheme C of $X \times Y$ are denoted by $\pi_1^C := \pi_1|_C : C \to X$ and $\pi_2^C := \pi_2|_C : C \to Y$.

- We will often define schemes using affine models, but the scheme in question should *always* be taken to be the projective closure (or product projective closure) of the affine model. The scheme with an affine model cut out by an ideal I is denoted by $V(I)$.

- If V is a variety, then its arithmetic genus is denoted by $p_a(V)$; its function field and coordinate ring are denoted by $k(V)$ and $\mathcal{O}_V$, respectively. If f is a nonzero function in $k(V)$ and P is a subvariety of V, then we define $\mathrm{ord}_P(f)$ to be the order of vanishing of f along P — so $\mathrm{ord}_P(f) = m$ (resp. $-m$) if f has a zero (resp. pole) of order m at P. The module of differential d-forms on V is denoted by Ω_V^d. We denote the set of K-rational points of V by $V(K)$.

- The coordinate functions on an affine plane model of a curve are denoted u and v. The corresponding coordinate functions on the product $X \times Y$ are denoted u_1 and v_1 (for the X factor) and u_2 and v_2 (for the Y factor): so $\pi_1(u_1, v_1, u_2, v_2) = (u_1, v_1)$ and $\pi_2(u_1, v_1, u_2, v_2) = (u_2, v_2)$.

1.3 Algorithms and pseudocode

In the course of this investigation, we will present a number of algorithms. The algorithms will be defined in a pseudocode similar to the language of the Magma computational algebra system [8], and (hopefully) accessible to the reader familiar with any procedural programming language. Sequences

are enclosed in square brackets; comments begin with the string "//", and continue to the end of the line. We will presume the existence of the following functions:

- Coefficient(F, m): Given a polynomial F and a monomial m, returns the coefficient of m in F.
- Roots(F, k): The roots in the field k of the polynomial F.
- XGCD($F_1, F_2, \ldots$): The extended Euclidean algorithm. Given a list of polynomials $F_1, F_2, \ldots$, returns their greatest common divisor g together with a list of elements $a_1, a_2, \ldots$ such that $g = \sum_i a_i F_i$.
- Curve(F): Given a polynomial $F(u, v)$, returns the plane curve with affine model $F(u, v) = 0$.
- AbsoluteIgusaInvariants(X): Given a genus two curve X, returns a sequence consisting of the absolute Igusa invariants of X, as defined by Mestre [43, page 325].

Chapter 2

Geometric preliminaries

In this chapter, we will survey some of the required background from algebraic geometry. We assume a rough familiarity with the basic geometry of curves. For detailed results, the reader is encouraged to refer to Hartshorne [29, Chapters I, IV], Hindry & Silverman [31, Chapter A] and Milne [45, 46].

Among surfaces, $X \times Y$ is far from general. It is a product of reduced, irreducible, nonsingular projective curves, and so we know that it is a reduced, irreducible, nonsingular, projective surface. The arithmetic genus of $X \times Y$ is given by [29, Exercise I.7.2(e)]:

$$p_a(X \times Y) = (g_X - 1)(g_Y - 1) + 1 = g_X g_Y - (g_X + g_Y).$$

The following proposition is fundamental to the study of curves.

Proposition 2.0.1. *Any morphism of projective curves is either a finite morphism or a constant map.*

Proof. See Hartshorne [29, Proposition II.6.8]. □

A finite morphism of curves is called a *cover*. We associate an integer *degree* to any morphism of curves as follows.

Definition 2.0.2. Let $\psi : C \to X$ be a morphism of curves. If ψ is a finite cover, then we define its degree, denoted $\deg \psi$, to be the degree of the

corresponding inclusion of function fields:

$$\deg \psi := [k(C) : k(X)].$$

Otherwise, ψ is a constant map, and we define $\deg \psi := 0$.

If X is a curve over the finite field k, then for each positive integer r there is the r^{th} *Frobenius* morphism $\mathcal{F}^{(r)} : X \to X$. If k has q elements, and if X has an affine plane model with coordinate functions u and v, then

$$\mathcal{F}^{(r)}(u, v) = (u^{q^r}, v^{q^r}).$$

2.1 Divisors

Definition 2.1.1. Let V be a nonsingular variety. A *prime Weil divisor* on V is a codimension-one subvariety of V. A *Weil divisor* on V is a finite formal sum of prime divisors on V:

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

The *support* of D is the collection of subvarieties P where $n_P \neq 0$. The Weil divisors on V form an abelian group under addition, which we denote $\mathrm{Div}(V)$.

A Weil divisor $\sum_{P \subset V} n_P \cdot P$ on V is K-rational if it is stable under the action of the Galois group of $\overline{K}/K$. Note that this does *not* require each of the subvarieties P to be defined over K.

Definition 2.1.2. Let V be a nonsingular variety. A *Cartier divisor* on V is an equivalence class of sets of pairs $\{(U_i, f_i)\}$, where the U_i are open subsets of V such that $\bigcup_i U_i = V$, and the f_i are functions on the U_i such that f_i/f_j has no poles or zeroes on $U_i \cap U_j$ for all i and j. The sets of pairs $\{(U_i, f_i)\}$ and $\{(U'_j, f'_j)\}$ are equivalent, and thus define the same Cartier divisor, if f_i/f'_j has no poles or zeroes on $U_i \cap U'_j$ for all i and j. The Cartier divisors

on V form an abelian group, under the operation

$$\{(U_i, f_{U_i})\} + \{(U'_j, f_{U'_j})\} := \{(U_i \cap U'_j, f_{U_i} f_{U'_j})\}.$$

Suppose $C = \{U_i, f_i\}$ specifies a Cartier divisor. We construct a Weil divisor D from C as follows: for each subvariety P of V, we let n_P be the order of vanishing of f_i along P for any i such that U_i intersects nontrivially with P, and then set $D = \sum_P n_P P$. It is easily verified that this map from the group of Cartier divisors on V to the group of Weil divisors on V is well-defined. In fact, when V is a nonsingular variety, the map is an isomorphism of groups (see Hartshorne [29, Proposition II.6.11]). We will henceforward identify Weil divisors with their corresponding Cartier divisors, and use the term *divisor* for both.

We say that a divisor $D = \sum_P n_P \cdot P$ is *effective* if $n_P \geq 0$ for all P. Effective divisors may be represented by a subscheme of V, which is generally neither reduced nor irreducible.

Definition 2.1.3. Let $\phi : V' \to V$ be a morphism of nonsingular varieties. We define the *pullback* $\phi^* : \mathrm{Div}(V) \to \mathrm{Div}(V')$ in terms of Cartier divisors, by

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

In terms of Weil divisors, we have

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

where t_Q denotes a local parameter at the subvariety Q of V.

In this investigation, we use divisors on curves and surfaces. Divisors on a curve are formal sums of (closed) points; divisors on a surface are formal sums of curves. In either case, the group of divisors on a variety is free and not finitely generated, and so its group structure carries no information about the intrinsic geometry of the variety. We use *rational equivalence* to cut the divisor group down to size, forming a quotient reflecting the geometric structure of the variety. Rational equivalence for divisors on curves is often

called *linear equivalence*; we will use the more general term.

Definition 2.1.4. Let V be a nonsingular variety. For each nonzero function f in $k(V)$, we define a divisor

$$\mathrm{div}(f) := \sum_{P \subset V} \mathrm{ord}_P(f) P.$$

We say that a divisor is *principal* if it is equal to $\mathrm{div}(f)$ for some f in $k(V)$. We say that divisors are *rationally equivalent* if they differ by a principal divisor. We denote the group of principal divisors on V by $\mathrm{Prin}(V)$. Note that the divisor $\mathrm{div}(f)$ is equal to the Cartier divisor $\{(U_i, f)\}$ for any open covering $\{U_i\}$ of V.

It is easily verified that $\mathrm{Prin}(V)$ is in fact a subgroup of $\mathrm{Div}(V)$. For all nonzero functions f and f' in $k(V)^\times$, we have $\mathrm{div}(f) + \mathrm{div}(f') = \mathrm{div}(ff')$; further, $\mathrm{div}(\alpha) = 0$ for all α in $k^\times$. It follows that rational equivalence is indeed a well-defined equivalence relation on the divisor group.

Definition 2.1.5. Let V be a nonsingular variety. The quotient group

$$\mathrm{Pic}(V) := \mathrm{Div}(V)/\mathrm{Prin}(V)$$

of divisors modulo rational equivalence is called the *Picard group* of V. We denote the image in $\mathrm{Pic}(V)$ of a divisor D on V by $[D]$.

Lemma 2.1.6. *Suppose $\phi : V' \to V$ is a morphism of nonsingular varieties. Then the pullback $\phi^* : \mathrm{Div}(V) \to \mathrm{Div}(V')$ induces a well-defined pullback $\phi^* : \mathrm{Pic}(V) \to \mathrm{Pic}(V')$.*

Proof. It is easily checked that $\phi^*(\mathrm{div}(f)) = \mathrm{div}(f \circ \phi)$ for all functions f in $k(V)^\times$. Thus ϕ^* sends $\mathrm{Prin}(V)$ into $\mathrm{Prin}(V')$; the statement follows. □

The following lemma is known as the see-saw principle; it is particularly useful when dealing with divisor classes on products of curves.

Lemma 2.1.7 (The see-saw principle). *Let X and Y be varieties; for all points x of X, define a morphism $i_x : Y \to X \times Y$ by $i_x(y) = (x, y)$.*

If $[C]$ is a class in $\mathrm{Pic}(X \times Y)$ such that $i_x^*([C]) = 0$ for all points x of X, then $[C] = {\pi_1}^*([C_X])$ for some class $[C_X]$ in $\mathrm{Pic}(X)$. Further, if the restriction of $[C]$ to $X \times y$ is trivial for some point y of Y, then $[C] = 0$.

Proof. See Hindry & Silverman [31, Lemma A.7.2.3] or Milne [45, §5]. □

We now turn our attention to the particular case of divisors on curves. Let X be a nonsingular projective curve.

Definition 2.1.8. The degree map $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ is defined by

$$\deg(\sum_i n_i P_i) := \sum_i n_i.$$

Remark 2.1.9. We warn the reader that there is no analogous degree map for divisors on the surfaces that we are concerned with. In place of the degree map, we will need intersection numbers, which are defined in Chapter 4.

The degree map is a homomorphism; its kernel is the subgroup of divisors on X of degree zero, denoted $\mathrm{Div}^0(X)$. We have a short exact sequence

$$0 \longrightarrow \mathrm{Div}^0(X) \hookrightarrow \mathrm{Div}(X) \xrightarrow{\deg(\cdot)} \mathbb{Z} \longrightarrow 0\ .$$

Since X is complete and nonsingular, all principal divisors have degree zero: $\mathrm{Prin}(X)$ is a subset of $\mathrm{Div}^0(X)$ (see [56, Proposition II.1] or [29, Corollary II.6.10]). It follows that the degree map is well-defined on rational equivalence classes, and induces a homomorphism $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$. The kernel of this homomorphism, which we denote $\mathrm{Pic}^0(X)$, is the subgroup of $\mathrm{Pic}(X)$ generated by $\mathrm{Div}^0(X)$; hence there is a short exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(X) \hookrightarrow \mathrm{Pic}(X) \xrightarrow{\deg(\cdot)} \mathbb{Z} \longrightarrow 0\ .$$

If we assume X has a rational divisor of degree one, say D, then there is a homomorphism $\mathbb{Z} \to \mathrm{Pic}(X)$ defined by $n \mapsto [nD]$. This homomorphism splits the exact sequence, and we see that

$$\mathrm{Pic}(X) \cong \mathbb{Z} \oplus \mathrm{Pic}^0(X).$$

Lemma 2.1.10. *If $\phi : C \to X$ is a morphism of curves, then* $\deg \phi^*(D) = \deg \phi \cdot \deg D$ *for all divisors D on X.*

Proof. See Hartshorne [29, Proposition II.6.9]. □

Lemma 2.1.11. *Let $\phi : V' \to V$ be a morphism of nonsingular varieties. The pullback $\phi^* : \mathrm{Pic}(V) \to \mathrm{Pic}^0(V)$ maps $\mathrm{Pic}^0(V)$ into $\mathrm{Pic}^0(V')$, and so restricts to a well-defined homomorphism*

$$\phi^* : \mathrm{Pic}^0(V) \longrightarrow \mathrm{Pic}^0(V').$$

Proof. Immediate from Lemma 2.1.10. □

Every morphism of curves induces a second homomorphism of divisor groups, in addition to the pullback. This homomorphism is called the *pushforward*, and is defined in a straightforward way; it is essentially the $\mathbb{Z}$-linear extension of the morphism itself.

Definition 2.1.12. Let $\psi : C \to X$ be a morphism of curves. We define the *pushforward* $\psi_* : \mathrm{Div}(C) \to \mathrm{Div}(X)$ as follows: If ψ is a finite cover, then we define

$$\psi_*(\sum_i n_i P_i) := \sum_i n_i \psi(P_i).$$

Otherwise, ψ is a constant map, and we define ψ_* to be zero.

Lemma 2.1.13. *Let $\psi : C \to X$ be a morphism of curves. The pushforward ϕ_* induces a homomorphism on Picard groups*

$$\psi_* : \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}(X),$$

which restricts to a homomorphism

$$\psi_* : \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(X).$$

Proof. Let $N_{k(C)/k(X)}$ denote the norm map from $k(C)$ to $k(X)$. We have $\psi_*(\mathrm{div}(g)) = \mathrm{div}(N_{k(C)/k(X)}(g))$ for all g in $k(C)$; so $\psi_*(\mathrm{Prin}(C)) \subset \mathrm{Prin}(X)$,

and we therefore have a well-defined pushforward on Picard groups. Suppose $D = \sum_P n_P P$ is an element of $\mathrm{Div}^0(C)$: then $\sum_P n_P = 0$. Hence

$$\deg(\psi_*(D)) = \deg(\sum_P n_P \psi(P)) = \sum_P n_P = 0,$$

so $\psi_*(D)$ is in $\mathrm{Div}^0(X)$, and $\psi_*([D])$ is in $\mathrm{Pic}^0(X)$. □

We recall the definition of the canonical class of a variety, following Hindry & Silverman [31, Example A.2.2.3]. Suppose V is a nonsingular d-dimensional variety, and let ω be a differential d-form on V. If U is an affine patch of V , and $u_1, \ldots, u_d$ are algebraically independent functions on U, then there is a function f_U in $k(U)$ such that $\omega = f_U du_1 \wedge \cdots \wedge du_d$. The collection $\{(U, f_U)\}$ over all affine patches U of V specifies a Cartier divisor $\mathrm{div}(\omega)$ on V associated to the differential ω. Every differential d-form ω' on V is equal to $f\omega$ for some function f in $k(V)$, and $\mathrm{div}(\omega') = \mathrm{div}(\omega) + \mathrm{div}(f)$. Therefore, the divisors associated to the differential d-forms on V form a single rational equivalence class, called the *canonical class* on V. We call any divisor in the canonical class a *canonical divisor*; by abuse of notation, we denote any of the canonical divisors on V by K_V.

Lemma 2.1.14. *If K_X is a canonical divisor on a curve X, then the degree of K_X is*

$$\deg K_X = 2g_X - 2.$$

Proof. See Hindry & Silverman [31, Corollary A.4.2.2] or Hartshorne [29, V.1.3.3]. □

Given differential 1-forms on curves X and Y, we may construct a differential 2-form on the product $X \times Y$. It follows that a canonical divisor on $X \times Y$ may be constructed from canonical divisors on X and Y.

Lemma 2.1.15. *If K_X and K_Y are canonical divisors on curves X and Y respectively, then*

$$K_{X\times Y} := {\pi_1}^*(K_X) + {\pi_2}^*(K_Y)$$

is a canonical divisor on $X \times Y$.

Proof. See Hartshorne [29, Ex. II.8.3]. □

2.2 Abelian varieties and Jacobians

A *group variety* is a variety whose points form a group, and where the group operations are morphisms of varieties. An *abelian variety* is a projective group variety. The group structure of an abelian variety is necessarily commutative, so we write the group law additively.

A homomorphism of abelian varieties is a morphism that is also a homomorphism of abelian groups. The image of a homomorphism $A \to B$ is an abelian subvariety of B, and the kernel is a group subscheme of A. In fact, the kernel of a homomorphism of abelian varieties is the extension of a finite group scheme by an abelian subvariety of A, which may be zero (see Milne [45, §8]).

For each point a of an abelian variety A, there is a *translation* morphism $t_a : A \to A$, defined by $t_a(P) = P + a$. Every morphism of abelian varieties is the composition of a homomorphism and a translation (see Milne [45, Corollary 2.2] or Hindry & Silverman [31, Corollary A.7.1.2]).

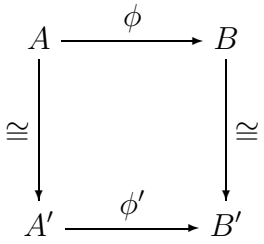
Lemma 2.2.1. *Let A and B be abelian varieties. Then* $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of finite rank:*

$$\mathrm{rk}\ \mathrm{Hom}(A, B) \leq (2 \dim A)(2 \dim B).$$

Proof. See Milne [45, Theorem 12.5]. □

An *isogeny* of abelian varieties is a finite dominant homomorphism of abelian varieties. If there exists an isogeny between abelian varieties A and B, then we say that A and B are *isogenous*. Isogenies $\phi : A \to B$ and $\phi' : A' \to B'$ are *isomorphic* if there are isomorphisms $A \cong A'$ and $B \cong B'$

such that the diagram



commutes. In order for abelian varieties A and B to be isogenous, it is necessary (but not sufficient) that $\dim A = \dim B$. Given an isogeny $\phi : A \to B$, the kernel of ϕ is a finite group subscheme of A, denoted $A[\phi]$, of order $\deg \phi$. By the structure theorem for finitely generated modules over principal ideal domains (see Lang [38, §III.7]), there exists a unique integer r and a unique sequence of integers $n_1, \ldots, n_r$ with $n_{i+1} | n_i$ for $1 \leq i < r$, such that $A[\phi]$ is isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$. If ϕ is separable, then we say that ϕ is an $(n_1, \ldots, n_r)$-*isogeny*.

An *endomorphism* of an abelian variety A is a homomorphism from A to itself. The endomorphisms of A form a $\mathbb{Z}$-algebra, denoted $\mathrm{End}(A)$; we denote $\mathrm{End}(A) \otimes \mathbb{Q}$ by $\mathrm{End}^0(A)$. For every abelian variety A and integer n, we have a multiplication-by-n endomorphism on A, denoted $[n]_A$:

$$[n]_A : P \mapsto P + \cdots + P \quad (n \text{ times}).$$

Thus if A is a nontrivial abelian variety, then there is a subring of $\mathrm{End}(A)$ isomorphic to $\mathbb{Z}$. Multiplication by n is always an isogeny.

We say that an abelian variety is *simple* if it has no proper nonzero abelian subvarieties. Every abelian variety A is isogenous to a product $\prod_i A_i^{r_i}$, with each of the A_i simple (see Lang [37, Corollary of Theorem II.6]). If A is simple, then every nonzero endomorphism is an isogeny.

The $\mathbb{Q}$-algebra $\mathrm{End}^0(A)$ is a finite-dimensional semisimple algebra over $\mathbb{Q}$ (see Milne [45, §12]). If A is simple, then $\mathrm{End}^0(A)$ is a division algebra. If $A = \prod_i A_i^{r_i}$, with each of the A_i simple, then $\mathrm{End}^0(A) = \prod_i \mathrm{End}^0(A_i^{r_i})$, with $\mathrm{End}^0(A_i^{r_i}) = M_{r_i}(\mathrm{End}^0(A_i))$ (see Milne [45, §12]). If there is an injection of a subring R of a real extension of $\mathbb{Q}$ into $\mathrm{End}^0(A)$, then we say that A has

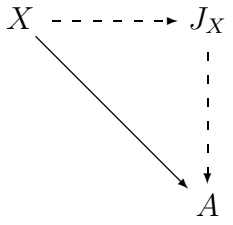
real multiplication (RM) by R. Similarly, if there is an injection of a subring S of a complex extension of $\mathbb{Q}$ into $\mathrm{End}^0(A)$, then we say A has *complex multiplication (CM)* by S.

Let A and B be abelian varieties. For each point a of A, we define a map $i_a : B \to A \times B$ by $i_a(b) = (a, b)$; similarly, for each point b of B we define a map $i_b : A \to A \times B$ by $i_b(a) = (a, b)$. We say that A and B are *dual* to one another if there is a divisor class $\mathcal{P}$ in $\mathrm{Pic}(A \times B)$ (called the *Poincaré class*) such that the maps $A \to \mathrm{Pic}^0(B)$ and $B \to \mathrm{Pic}^0(A)$ defined by $a \mapsto i_a^*(\mathcal{P})$ and $b \mapsto i_b^*(\mathcal{P})$ respectively are both isomorphisms. A dual abelian variety exists for every abelian variety A, and is unique up to isomorphism, together with the Poincaré class $\mathcal{P}$ (see Hindry & Silverman [31, Theorem A.7.3.4]); we denote the dual of A by $\hat{A}$. An ample divisor L on A defines an isogeny $\phi_L : A \to \hat{A}$ into the dual of A, called a *polarisation*. If a polarisation is an isomorphism, then we say that it is a *principal polarisation*, and that A is *principally polarised*.

For every homomorphism $\phi : A \to B$, there is a dual homomorphism $\hat{\phi} : \hat{B} \to \hat{A}$ induced by the pullback of ϕ, as in the following diagram.

$$\begin{array}{ccc} \mathrm{Pic}^0(B) & \xrightarrow{\phi^*} & \mathrm{Pic}^0(A) \\ \cong \uparrow & & \downarrow \cong \\ \hat{B} & \xrightarrow{\hat{\phi}} & \hat{A} \end{array}$$

The *Jacobian* J_X of a curve X is a principally polarised abelian variety, satisfying the following universal property: any map from X into another abelian variety A factors through J_X, as in the diagram below.



The Jacobian of X is unique up to isomorphism: consider the universal

property with J_X in place of A. A curve of genus greater than zero may always be embedded in its own Jacobian (if X is a curve of genus zero, then J_X is trivial by Theorem 2.2.2 below, and so X cannot embed in J_X). For the embedding to be defined over k, it suffices for X to have a k-rational divisor of degree one; suppose that D is such a divisor. There is a canonical embedding $\alpha_D : X \hookrightarrow J_X$, defined by $P \mapsto [P - D]$, which sends D to the zero element of J_X.

Theorem 2.2.2. *Let X be a curve, with $g_X > 0$. Let J_X be the Jacobian of X, and $\alpha : X \hookrightarrow J_X$ an embedding. For each integer $r \geq 0$, let*

$$W_r := \underbrace{\alpha(X) + \cdots + \alpha(X)}_{r \text{ times}} \subset J_X$$

and define $\Theta := W_{(g_X-1)}$. The following properties hold:

1. *Extending α linearly to a map on divisors, we have an isomorphism of groups between $\mathrm{Pic}^0(X)$ and J_X.*
2. *W_r is a subvariety of J_X of dimension $\dim W_r = \min(r, g_X)$.*
3. *$W_{g_X} = J_X$: we say that X generates J_X.*
4. *$\dim J_X = g_X$.*
5. *$\Theta = W_{(g_X-1)}$ is an irreducible ample divisor on J_X.*

Proof. See Hindry & Silverman [31, Theorem A.8.1.1]. □

The divisor Θ on J_X of Theorem 2.2.2 is particularly important; we call it a *theta divisor*. The isomorphism between J_X and $\mathrm{Pic}^0(X)$ provided by Theorem 2.2.2 is particularly useful: in the sequel, we will use $\mathrm{Pic}^0(X)$ and J_X interchangeably. Note that under this isomorphism, the embedding $\alpha_x : X \to J_X$ sends P to $[P - x]$.

Corollary 2.2.3. *Let $\psi : C \to X$ be a morphism of curves. The pullback ψ^* and the pushforward ψ_* induce well-defined homomorphisms of Jacobians*

$$\psi^* : J_X \to J_C \quad \text{and} \quad \psi_* : J_C \to J_X.$$

Proof. Theorem 2.2.2 gives isomorphisms $\mathrm{Pic}^0(X) \cong J_X$ and $\mathrm{Pic}^0(C) \cong J_C$. The statement then follows immediately from Lemmas 2.1.11 and 2.1.13. □

Corollary 2.2.4. *Let X and Y be curves; then $\mathrm{Hom}(J_X, J_Y)$ is a free $\mathbb{Z}$-module of rank at most $4g_Xg_Y$.*

Proof. Statement (4) of Theorem 2.2.2 gives us $\dim J_X = g_X$; the result then follows from Lemma 2.2.1. □

Example 2.2.5. Let X be a curve of genus one. By Theorem 2.2.2, J_X is one-dimensional, so it is a curve. Given a rational point x of X, the embedding $\alpha_x : X \to J_X$ is an isomorphism. Hence J_X is isomorphic to a curve of genus one with a rational point; we call such Jacobians *elliptic curves*.

Theorem 2.2.2 proves our earlier assertion that if X is a curve of genus zero, then J_X is a point. If X is a curve of genus two, then J_X is a surface; thus we call Jacobians of curves of genus two *Jacobian surfaces*.

Suppose Θ is a theta divisor on J_X. One nice property of Θ is that it gives us a principal polarisation $\lambda_\Theta : J_X \to \widehat{J_X}$, defined by $\lambda_\Theta(P) = t_P^*(\Theta) - \Theta$. If we use λ_Θ to identify J_X with $\widehat{J_X}$, let $p_i : J_X \times J_X \to J_X$ be the projection to the i^{th} factor and $\mu : J_X \times J_X \to J_X$ be the addition map, then

$$\mathcal{P} = \mu^*(\Theta) - (p_1^*(\Theta) + p_2^*(\Theta))$$

is a Poincaré divisor on $J_X \times J_X$. If we fix a rational degree-one divisor D on X and let Θ be the theta divisor corresponding to the embedding α_D, then we denote the principal polarisation λ_Θ by λ_X.

Definition 2.2.6. Fix principal polarisations λ_X for J_X and λ_Y for J_Y. For each homomorphism $\phi : J_X \to J_Y$, we set $\phi^\dagger := \lambda_X^{-1} \circ \widehat{\phi} \circ \lambda_Y$:

$$\begin{array}{ccc} \widehat{J_Y} & \xrightarrow{\widehat{\phi}} & \widehat{J_X} \\ {\scriptstyle \lambda_Y}\uparrow & & \downarrow{\scriptstyle \lambda_X^{-1}} \\ J_Y & \xrightarrow{\phi^\dagger} & J_X \end{array}$$

The map $\mathrm{Hom}(J_X, J_Y) \longrightarrow \mathrm{Hom}(J_Y, J_X)$ defined by $\phi \mapsto \phi^\dagger$ is called the *Rosati involution*, and $\phi^\dagger$ is called the *Rosati dual* of ϕ.

If an endomorphism ϕ is defined over k, then so is $\phi^\dagger$. It is clear from the definition that $(\phi^\dagger)^\dagger = \phi$, so the Rosati involution is indeed an involution. It is well-known that the Rosati involution is positive, in the sense of the following lemma.

Lemma 2.2.7. *The map* $\mathrm{End}(J_X)^2 \to \mathbb{Z}$ *defined by* $(\phi, \psi) \mapsto \mathrm{Tr}(\phi \circ \psi^\dagger)$ *is a positive definite bilinear form.*

Proof. See Milne [45, Theorem 17.3] or Lang [37, §V.3]. □

2.3 Hyperelliptic curves and their Jacobians

Definition 2.3.1. We say that a curve X is *hyperelliptic*[1] if $g_X > 0$ and there is a covering $h_X : X \to \mathbb{P}^1$ of degree two. (The map h_X is called a *hyperelliptic cover*.)

Any curve of genus one with a rational point is hyperelliptic. All curves of genus two are hyperelliptic (see Hartshorne [29, Ex. IV.1.7]); for curves of genus greater than two, hyperellipticity is quite special. The geometry of hyperelliptic curves is quite different from that of generic curves.

Suppose X is a hyperelliptic curve. Since the covering $h_X : X \to \mathbb{P}^1$ has degree two, it induces a quadratic extension of function fields $k(X)/k(\mathbb{P}^1)$. If the characteristic of k is not two, we may take an affine plane model for X in the form

$$X : v^2 = f_X(u)$$

where $f_X(u)$ is a squarefree polynomial in $k[u]$. We call f_X the *hyperelliptic polynomial* of X. There is an involution ι_X on X called the *hyperelliptic involution* such that h_X is the quotient by $\langle \iota_X \rangle$. On the affine plane model above, ι_X acts as $(u, v) \mapsto (u, -v)$ and h_X is $(u, v) \mapsto u$. The roots of

[1] The reader should note that some authors reserve the term hyperelliptic for curves of genus strictly greater than one; we will not make this restriction.

f_X are precisely the branch points of h_X; the Riemann–Hurwitz formula (Hartshorne [29, §IV.2], Hindry & Silverman [31, Theorem A.4.2.5]) implies that $\deg f_X = 2g_X + 1$ or $2g_X + 2$ (if the degree of f_X is odd, then there is an additional ramification at infinity.) The hyperelliptic involution ι_X induces an involution of J_X equal to $[-1]_{J_X}$. The following lemma shows that any cover of hyperelliptic curves commuting with the hyperelliptic involutions is essentially induced by a map on the underlying projective lines.

Lemma 2.3.2. *Let X and Y be hyperelliptic curves, and let $\pi : X \to Y$ be a covering such that $\pi \circ \iota_X = \iota_Y \circ \pi$. Then π is a map of the form*

$$\pi : (u, v) \mapsto (P(u), v)$$

for some rational function P.

We will now describe the standard methods for computing explicitly in hyperelliptic Jacobians, following Cantor [9] and Mumford [48]. Suppose X is a hyperelliptic curve of genus g, with an (affine) model

$$v^2 = f_X(u) = u^{2g+1} + c_{2g}u^{2g} + \cdots + c_0,$$

with each c_i in k. Let ∞ denote the point at infinity of this model. A point P in $J_X(k)$ may be represented as a divisor (class)

$$P = \left[\sum_{i=1}^{m} P_i - m \cdot \infty\right] = \left[\sum_{i=1}^{m} (u_i, v_i) - m \cdot \infty\right],$$

for some m points $P_i = (u_i, v_i)$ in $X(\overline{k})$. In fact, this representation is unique if we also require that $m \leq g$ and $\iota_Y(P_i) \neq P_j$ for any $i \neq j$; we call such a representative *reduced*. Note that while P is k-rational, the points P_i in the support of the divisor need not be: the coordinates (u_i, v_i) of P_i may lie in some finite extension K of k. Thus, for computations, we use instead the Mumford representation for divisors [48], identifying P with the ideal class

$$P = [(a(u), v - b(u))],$$

where a and b are polynomials over k such that $a(u) = \prod_i (u - u_i)$ and $v_i = b(u_i)$ (with correct multiplicity) for all i. Note that the polynomial $a(u)$ should be monic. Cantor [9] provides algorithms to implement the group law for points in this representation: addition of points P and Q is an ideal product, followed by application of a reduction algorithm to produce the unique "reduced" ideal class representing $P + Q$.

Algorithm 2.3.3. Computes the reduced representative of a point on the Jacobian J_X of the hyperelliptic curve $X : v^2 = f_X(u)$.

function CantorReduction($(a(u), v - b(u))$)
  while $\deg(a) > g_X$ **do**
    $a := (f_X - b^2)/a$;
    $b := -b \pmod{a}$;
  end while
  $a := a/\text{LeadingCoefficient}(a)$;
  return $(a(u), v - b(u))$;
end function

Algorithm 2.3.4. Computes the reduced representative of the sum of two points on a Jacobian.

function CantorComposition($(a_1(u), v - b_1(u))$, $(a_2(u), v - b_2(u))$)
  $d, c_1, c_2, c_3 := \text{XGCD}(a_1, a_2, b_1 + b_2)$;
    // that is, $d = \gcd(a_1, a_2, b_1 + b_2) = c_1 a_1 + c_2 a_2 + c_3(b_1 + b_2)$
  $a_3 := a_1 a_2 / d^2$;
  $b_3 := (c_1 a_1 b_2 + c_2 a_2 b_1 + c_3 b_1 b_2)/d$;
  return CantorReduction($(a_3(u), v - b_3(u))$);
end function

2.4 Efficient multiplication on Jacobians

In this section, we give a brief description of Gallant–Lambert–Vanstone (GLV) fast scalar multiplication. The key idea is to use integer eigenvalues of non-integer endomorphisms to improve the efficiency of integer multiplication on (subgroups of) Jacobians. We will sketch this technique here; the reader

is encouraged to refer to Gallant, Lambert, and Vanstone [23], Lange [40], and Sica, Ciet, and Quisquater [58] for a thorough treatment of the methods, and to Solinas [59] and Ciet, Lange, Sica, and Quisquater [13] for discussions of related ϕ-adic multiplication techniques.

Suppose that ϕ is an efficiently computable k-rational endomorphism of J_X that does not equal $[m]_{J_X}$ for any integer m. Let χ_ϕ be the minimal polynomial of ϕ; and let d be the degree of χ_ϕ. Suppose G is a cyclic subgroup of $J_X(k)$ of prime order n. The endomorphism ϕ must act as an integer multiplication on G: in fact, ϕ acts as $[c_\phi]_G$ for some root c_ϕ of χ_ϕ modulo n. We may use this fact to speed up the evaluation of integer multiplication endomorphisms on G.

Suppose we wish to evaluate $[m]_{J_X} P$, where P is an element of G and $|m|$ is relatively large. First, we choose integers m_i for $0 \leq i < d$ such that

$$m \equiv m_0 + m_1 c_\phi + m_2 c_\phi^2 + \cdots + m_{d-1} c_\phi^{d-1} \pmod{n};$$

then we evaluate

$$[m]P = [m_0]P + \phi([m_1](P)) + \phi^2([m_2](P)) + \cdots + \phi^{d-1}([m_{d-1}](P)).$$

Sica, Ciet and Quisquater [58] show that

$$\max |m_i| \leq B^{d-1} 2^{d(d-1)/4} n^{1/d},$$

where B is a polynomial expression in the coefficients of χ_ϕ (see [58, Lemma 4, Theorem 5]). Thus multiplication by a large integer on G has been reduced to a sum of multiplications by smaller integers, which may be efficiently co-computed (ie, computed simultaneously) using joint scalar multiplication techniques. Methods for joint scalar multiplication are discussed in [4]. Techniques for finding optimal decompositions of $[m]$ with respect to ϕ are discussed in [23], [33], [49], and [13].

GLV techniques for elliptic curves are described in [23], and [13]. Günter, Lange and Stein [28] describe the use of Frobenius endomorphisms for fast scalar multiplication on Jacobians of genus two Koblitz curves [34]; Lange

[40] gives methods for Koblitz curves of higher genus. Park, Jeong, and Lim [49] have extended GLV techniques to the Jacobians of a class of curves of genus two and three. Recently, Takashima [61] has extended GLV multiplication techniques to a three-parameter family of Jacobian surfaces with real multiplication described by Hashimoto in [30]. In this work, we extend GLV techniques to higher-dimensional Jacobians with real multiplication.

2.5 The Dickson polynomials $D_n(x, a)$

In this section, we quickly survey the properties of the Dickson polynomials (of the first kind). For a full treatment of the theory of Dickson polynomials, the reader should refer to the book of Lidl, Mullen & Turnwald [42].

Definition 2.5.1. The n^{th} *Dickson polynomial* with parameter a in the indeterminate x is defined by

$$D_n(x, a) := \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

for $n > 0$; we define $D_0(x, a) = 2$. Observe that $D_1(x, a) = x$. The polynomial $D_n(x, a)$ is of degree n in x, with coefficients in the ring $\mathbb{Z}[a]$.

The following properties of Dickson polynomials are stated without proof. See Lidl et. al. [42, Chapter 2] for full proofs and derivations.

Lemma 2.5.2. *The polynomials $D_n(x, a)$ have the following properties:*

1. $D_n(u_1 + u_2, u_1 u_2) = u_1^n + u_2^n$;
2. $D_n(u + a/u, a) = u^n + (a/u)^n$;
3. $D_n(x, a) = ((x + \sqrt{x^2 - 4a})/2)^n + ((x - \sqrt{x^2 - 4a})/2)^n$;
4. $D_{n+2}(x, a) = xD_{n+1}(x, a) - aD_n(x, a)$ *for all* $n \geq 0$;
5. $D_{mn}(x, a) = D_m(D_n(x, a), a^n)$; *in particular, if* $a = 0$ *or* $a = 1$, *then* $D_{mn}(x, a) = D_m(D_n(x, a), a) = D_n(D_m(x, a), a)$;

6. $b^n D_n(x,a) = D_n(bx, b^2 a)$;

7. *If* $p := \text{char } k$ *is not zero, then* $D_{np}(x,a) = D_n(x,a)^p$;

8. $D_n(x,0) = x^n$.

Remark 2.5.3. If $T_n(x)$ denotes the n^{th} Tchebyshev polynomial of the first kind (see [52]), then $T_n(x) = D_n(2x,1)/2$ for all n.

The next lemma describes the factorizations of differences of Dickson polynomials in distinct indeterminates. This will be vital in our analysis of correspondences on hyperelliptic curves in Chapters 6 and 7.

Lemma 2.5.4. *Let* $\alpha_i = \zeta_n^i + \zeta_n^{-i}$ *and* $\beta_i = \zeta_n^i - \zeta_n^{-i}$, *where* ζ_n *is a primitive* n^{th} *root of unity over* k. *If* n *is odd, then for all parameters* a *we have*

$$D_n(u_1,a) - D_n(u_2,a) = (u_1 - u_2) \prod_{i=1}^{(n-1)/2} (u_1^2 + u_2^2 - \alpha_i u_1 u_2 + \beta_i^2 a);$$

if n *is even, then for all parameters* a *we have*

$$D_n(u_1,a) - D_n(u_2,a) = (u_1^2 - u_2^2) \prod_{i=1}^{(n-2)/2} (u_1^2 + u_2^2 - \alpha_i u_1 u_2 + \beta_i^2 a).$$

Further, if $a \neq 0$, *then the factors* $(u_1^2 + u_2^2 - \alpha_i u_1 u_2 + \beta_i^2 a)$ *in the above factorizations are all distinct and irreducible.*

Proof. See Lidl et. al. [42, Theorem 3.12]. □

Lemma 2.5.4 immediately implies the following lemma, which describes the factorization of Dickson polynomials.

Lemma 2.5.5. *Let* $\beta_i = \zeta_n^i - \zeta_n^{-i}$, *where* ζ_n *is a primitive* n^{th} *root of unity over* k. *If* n *is odd, then for all parameters* a *we have*

$$D_n(x,a) = x \prod_{i=1}^{(n-1)/2} (x^2 + \beta_i^2 a);$$

if n is even, then for all parameters a we have

$$D_n(x,a) = x^2 \prod_{i=1}^{(n-2)/2} (x^2 + \beta_i^2 a) + D_n(0,a).$$

Remark 2.5.6. The Dickson polynomials $D_n(x,1)$ have a geometric interpretation. Let $\mathbb{G}_m$ denote the multiplicative group over k, considered as a commutative group scheme. Note that $\mathbb{G}_m$ is isomorphic to $\mathbb{A}^1 \setminus \{0\}$, with the group law defined by $(u_1, u_2) \mapsto u_1 u_2$. If u denotes the coordinate on $\mathbb{A}^1$, then the exponentiation map $[n]_{\mathbb{G}_m}$ is realised by $u \mapsto u^n$. The map $q : \mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^1$ defined by $q(u) = u + u^{-1}$ gives a double cover from $\mathbb{G}_m$ to its Kummer variety $\mathbb{G}_m/\langle \pm 1 \rangle$, considered as a subvariety of $\mathbb{A}^1$. The second property in Lemma 2.5.2 shows that $[n]_{\mathbb{G}_m}$ induces the endomorphism $u \mapsto D_n(u,1)$ on $\mathbb{G}_m/\langle \pm 1 \rangle$, making the following diagram commute:

$$\begin{array}{ccc} \mathbb{G}_m & \xrightarrow[u \mapsto u^n]{[n]_{\mathbb{G}_m}} & \mathbb{G}_m \\ {\scriptstyle u \mapsto u + u^{-1}} \downarrow {\scriptstyle q} & & {\scriptstyle q} \downarrow {\scriptstyle u \mapsto u + u^{-1}} \\ \mathbb{G}_m/\langle \pm 1 \rangle & \xrightarrow[u \mapsto D_n(u,1)]{} & \mathbb{G}_m/\langle \pm 1 \rangle. \end{array}$$

Remark 2.5.7. The reader should note that we use the symbol a in this work to denote both the Dickson polynomial parameter and one of the polynomials in the Mumford representation of points on a hyperelliptic Jacobian. While this is a potential source of confusion — especially in Chapters six and seven, where we consider hyperelliptic curves whose hyperelliptic polynomial is a Dickson polynomial — the ambiguity is always resolved by the context.

Chapter 3

Correspondences

Given a pair of curves X and Y, the theory of correspondences relates divisors on the product $X \times Y$ to homomorphisms between the Jacobians J_X and J_Y. The relationship between a correspondence and its associated homomorphism is analogous to that between the graph of a morphism of curves and the morphism itself.

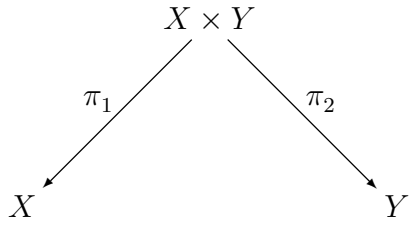
In this chapter, we describe the basic theory of correspondences. In §3.1, we define correspondences as divisors on $X \times Y$, and distinguish fibral and nonfibral correspondences. We then discuss the connection between correspondences and coverings of curves in §3.2, which leads to the definition of the homomorphisms induced by correspondences on divisor groups, Picard groups and Jacobians of curves in §3.3. We show that every homomorphism of Jacobians is induced by some correspondence. After describing the correspondences that induce trivial homomorphisms, we have an isomorphism between a certain quotient of the group of correspondences on $X \times Y$ and the module of homomorphisms from J_X to J_Y. Finally, in §3.4 we describe a composition operation for correspondences, and discuss the resulting ring structure on $\mathrm{Div}(X \times X)$.

The reader is encouraged to refer to Lange & Birkenhake [39, §11.5] and Griffiths & Harris [27, §2.5] for accessible, classical treatments of correspondences over the complex numbers. Fulton [22, Chapter 16] gives a treatment of the geometry of correspondences over an arbitrary field. Lang [37, Ap-

pendix] treats correspondences with a view to applications in the theory of abelian varieties. Deuring [15, 16] expresses the theory of correspondences in terms of extensions of function fields; Kux gives an overview of Deuring's theory in English in his PhD thesis [36].

3.1 Correspondences

Recall that X and Y denote nonsingular, irreducible projective curves; their product is denoted $X \times Y$, and π_i denotes the projection to the i^{th} factor:



Definition 3.1.1. A *correspondence on* $X \times Y$ is a divisor on $X \times Y$.

A correspondence is *prime* if it is a prime divisor: that is, a reduced, irreducible curve on the surface $X \times Y$. A correspondence is *effective* if it is an effective divisor. We may associate each effective correspondence with a subscheme of $X \times Y$, which is generally neither reduced nor irreducible. A correspondence is *principal* if it is the divisor of a function in $k(X \times Y)$.

Our first examples of correspondences are fibres of the projection maps. If P is a point of X and $F = {\pi_1}^{-1}(P)$ is the fibre of π_1 over P, then F is an irreducible, reduced curve, and therefore a prime correspondence. The restricted projection $\pi_2^F : F \to Y$ is an isomorphism, so as a curve, the arithmetic genus of F is g_Y. Similarly, the fibres of π_2 are prime correspondences isomorphic to X, of arithmetic genus g_X.

Definition 3.1.2. Correspondences supported entirely on fibres of the projection maps π_1 and π_2 are called *fibral*. The fibral correspondences form a subgroup of $\mathrm{Div}(X \times Y)$, which we denote $\mathrm{Fib}(X \times Y)$. We say that a correspondence is *nonfibral* if no component of its support is a fibre of one of the projections.

Only the zero correspondence is both fibral and nonfibral. It follows that every correspondence may be written in a unique way as the sum of a fibral correspondence and a nonfibral correspondence. Further, the group $\mathrm{Fib}(X \times Y)$ decomposes naturally into a summand supported on fibres of π_1 and a summand supported on fibres of π_2. There is thus a natural isomorphism

$$\mathrm{Fib}(X \times Y) \cong \mathrm{Div}(X) \times \mathrm{Div}(Y),$$

given by the product of pushforwards $\pi_{1*} \times \pi_{2*}$.

Lemma 3.1.3. *Let C be a correspondence on $X \times Y$. Then there are unique divisors C_X on X and C_Y on Y, and a unique nonfibral correspondence C' on $X \times Y$ such that*

$$C = C' + \pi_1^*(C_X) + \pi_2^*(C_Y).$$

Proof. The set S of reduced, irreducible curves on $X \times Y$ may be naturally partitioned into the set S_1 of fibres of π_1, the set S_2 of fibres of π_2, and the set $S' := S \setminus (S_1 \cup S_2)$ of all the other curves. We take C' to be the part of C with support in S', C_X to be the pushforward under π_1 of the part supported on S_1, and C_Y to be the pushforward under π_2 of the part supported on S_2. □

Lemma 3.1.3 is made effective by the following simple algorithm.

Algorithm 3.1.4. Given a correspondence $C = \sum_i n_i C_i$ on $X \times Y$ with each of the C_i prime, returns a nonfibral correspondence C' on $X \times Y$, together with divisors C_X on X and C_Y on Y such that $C = C' + {\pi_1}^*(C_X) + {\pi_2}^*(C_Y)$ (cf. Lemma 3.1.3.)

function StandardDecomposition($\sum_{i=1}^{r} n_i C_i$)
  $C' := 0_{\mathrm{Div}(X \times Y)}$;
  $C_X := 0_{\mathrm{Div}(X)}$;
  $C_Y := 0_{\mathrm{Div}(Y)}$;
  for i in $[1, \ldots, r]$ **do**
    if $\dim \pi_1(C_i) = 0$ **then**
      $C_X := C_X + n_i \pi_1(C_i)$;

```
        else if dim π₂(C_i) = 0 then
            C_Y := C_Y + n_i π₂(C_i);
        else
            C' := C' + n_i C_i;
        end if;
    end for;
    return C', C_X, C_Y;
end function;
```

There is a natural isomorphism $X \times Y \cong Y \times X$, exchanging the factors of the product. The image of a correspondence C on $X \times Y$ under this isomorphism is called the *transpose* of C, denoted C^t. We say a correspondence C on $X \times X$ is *symmetric* if $C = C^t$. The transpose of a fibral correspondence is fibral, and the transpose of a nonfibral correspondence is nonfibral. The transpose of a principal correspondence is principal, so transposition is well-defined on rational equivalence classes of correspondences.

3.2 Coverings and graphs

If C is a prime correspondence on $X \times Y$, then the projections π_1 and π_2 restrict to morphisms of curves $\pi_1^C : C \to X$ and $\pi_2^C : C \to Y$. Thus correspondences on $X \times Y$ may be viewed as formal sums of curves C with a morphism to *both* X and Y.

Conversely, given a curve $\tilde{C}$ together with morphisms $\phi : \tilde{C} \to X$ and $\phi' : \tilde{C} \to Y$, we may form a correspondence

$$C := (\phi \times \phi')(\tilde{C}) \subset X \times Y.$$

(If both of the morphisms ϕ and ϕ' are constant, then we define C to be the zero correspondence.) If either ϕ or ϕ' is constant, then C is fibral. Otherwise, both morphisms are coverings, and C is nonfibral. The degrees of the restricted projection morphisms are the degrees of the original morphisms: $\deg \pi_1^C = \deg \phi$, and $\deg \pi_2^C = \deg \phi'$. We extend these degrees to general correspondences.

Definition 3.2.1. If C be a prime correspondence on $X \times Y$, then we define

$$d_1(C) := \deg \pi_1^C \quad \text{and} \quad d_2(C) := \deg \pi_2^C,$$

and call $d_1(C)$ and $d_2(C)$ the *degrees* of C. Extending $\mathbb{Z}$-linearly, we obtain homomorphisms $d_1 : \mathrm{Div}(X \times Y) \to \mathbb{Z}$ and $d_2 : \mathrm{Div}(X \times Y) \to \mathbb{Z}$, called the *degree functions* on $X \times Y$. We say C is an (a, b)-*correspondence* if $d_1(C) = a$ and $d_2(C) = b$.

For any correspondence C, transposition exchanges the projection maps π_1^C and π_2^C. Therefore, we have $d_1(C^t) = d_2(C)$ and $d_2(C^t) = d_1(C)$.

Example 3.2.2. For every morphism of curves $f : X \to Y$, we have a prime correspondence

$$\Gamma_f := (\mathrm{Id}_X \times f)(X) \subset X \times Y,$$

called the *graph* of f. The projection $\pi_1^{\Gamma_f}$ is an isomorphism from Γ_f to X, so Γ_f has arithmetic genus $p_a(\Gamma_f) = p_a(X) = g_X$. Further,

$$d_1(\Gamma_f) = 1 \quad \text{and} \quad d_2(\Gamma_f) = \deg f.$$

Definition 3.2.3. We call the graph of the identity morphism $\mathrm{Id}_X : X \to X$ the *diagonal correspondence*, denoted Δ_X:

$$\Delta_X := \Gamma_{\mathrm{Id}_X} = (\mathrm{Id}_X \times \mathrm{Id}_X)(X) \subset X \times X.$$

Clearly $d_1(\Delta_X) = d_2(\Delta_X) = 1$, and ${\Delta_X}^t = \Delta_X$: the diagonal correspondence is therefore our first nontrivial example of a symmetric correspondence. Note that Δ_X has an affine model $V(u_2 - u_1, v_2 - v_1)$.

If k is a finite field, then for each positive integer r we have a Frobenius morphism $\mathcal{F}^{(r)} : X \to X$. The graphs of these morphisms are another source of nontrivial correspondences.

Definition 3.2.4. If k is a finite field and $r > 1$ is an integer, then we define the r^{th} *Frobenius correspondence* on $X \times X$, denoted $\mathfrak{F}_X^r$, to be

$$\mathfrak{F}_X^r := \Gamma_{\mathcal{F}^{(r)}} = (\mathrm{Id}_X \times \mathcal{F}^{(r)})(X).$$

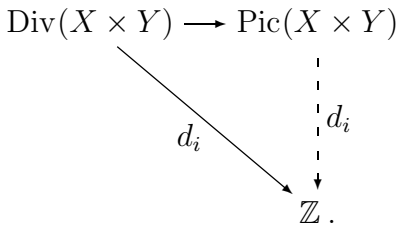
For notational convenience, we define $\mathfrak{F}_X^0 := \Delta_X$.

If $k = \mathbb{F}_q$, then $d_1(\mathfrak{F}_X^r) = 1$ and $d_2(\mathfrak{F}_X^r) = q^r$. In affine coordinates, $\mathfrak{F}_X^r$ has a model $V\left(u_2 - u_1^{q^r}, v_2 - v_1^{q^r}\right)$.

Example 3.2.5. Let F be a fibral correspondence on $X \times Y$. By Lemma 3.1.3, there are divisors F_X on X and F_Y on Y such that $F = {\pi_1}^*(F_X) + {\pi_2}^*(F_Y)$. We have $d_1(F) = \deg F_Y$ and $d_2(F) = \deg F_X$.

Example 3.2.6. Let K_X and K_Y be canonical divisors on X and Y, respectively. The fibral correspondence $K_{X\times Y} = {\pi_1}^*(K_X) + {\pi_2}^*(K_Y)$ is a canonical divisor on $X \times Y$ by Lemma 2.1.15. As in Example 3.2.5, $d_1(K_{X\times Y}) = \deg K_Y$ and $d_2(K_{X\times Y}) = \deg K_X$; it then follows from Lemma 2.1.14 that $d_1(K_{X\times Y}) = 2g_Y - 2$ and $d_2(K_{X\times Y}) = 2g_X - 2$.

Proposition 3.2.7. *The degree functions $d_i : \mathrm{Div}(X \times Y) \to \mathbb{Z}$ are well-defined on rational equivalence classes of correspondences, and hence factor through the Picard group* $\mathrm{Pic}(X \times Y)$*:*



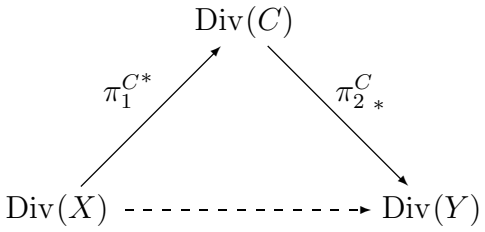
Proof. We will show that if C is a principal correspondence on $X \times Y$, then $d_1(C) = 0$. A similar argument shows that $d_2(C) = 0$, and the claim follows. Suppose $C = \mathrm{div}(f)$ for some f in $k(X \times Y)$. Now, $d_1(C)$ is equal to the degree of the divisor forming each fibre of π_1^C. For each point P of X, the function f restricts to a function f_P on the prime fibral correspondence ${\pi_1}^*(P)$. Thus $\pi_1^{C*}(P)$ is $\mathrm{div}(f_P)$, which has degree zero. □

3.3 Induced homomorphisms

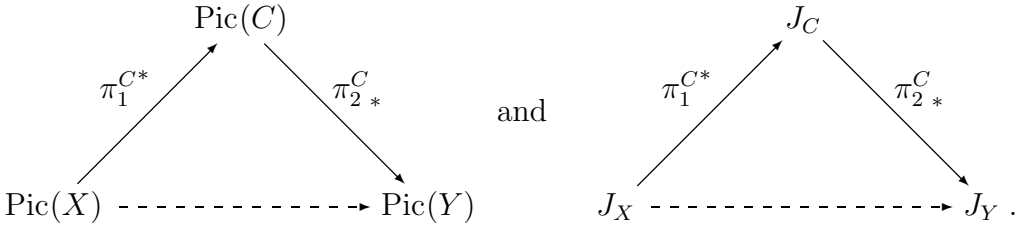
We now come to the central idea of the theory of correspondences: each correspondence on $X \times Y$ induces a homomorphism of the divisor groups of

X and Y. These homomorphisms in turn induce homomorphisms of Picard groups and Jacobians.

Suppose C is a prime correspondence on $X \times Y$. Viewing C as a curve, we have coverings $\pi_1^C : C \to X$ and $\pi_2^C : C \to Y$. We may compose the pullback π_1^{C*} and the pushforward $\pi_{2\,*}^{C}$ to obtain a homomorphism from $\mathrm{Div}(X)$ to $\mathrm{Div}(Y)$:



Lemma 2.1.6, Lemma 2.1.13 and Corollary 2.2.3 give us well-defined pullbacks $\pi_1^{C*} : \mathrm{Pic}(X) \to \mathrm{Pic}(C)$ and $\pi_1^{C*} : J_X \to J_C$, and well-defined pushforwards $\pi_{2\,*}^{C} : \mathrm{Pic}(C) \to \mathrm{Pic}(Y)$ and $\pi_{2\,*}^{C} : J_C \to J_Y$. Therefore, we also have induced homomorphisms



We extend this construction $\mathbb{Z}$-linearly to construct induced homomorphisms for every correspondence on $X \times Y$.

Definition 3.3.1. If $C = \sum_i n_i C_i$ is a correspondence on $X \times Y$, with each of the C_i prime, then we define the *induced homomorphism* of C to be

$$\phi_C := \sum_i n_i (\pi_{2\,*}^{C_i}) \circ (\pi_1^{C_i *}).$$

Unless otherwise noted, we take ϕ_C to indicate the induced homomorphism of Jacobians.

By definition, the map $C \mapsto \phi_C$ is a homomorphism, which we denote

$$\Phi : \mathrm{Div}(X \times Y) \longrightarrow \mathrm{Hom}(J_X, J_Y).$$

In particular, $\phi_0 = 0$.

Example 3.3.2. The diagonal correspondence Δ_X induces the identity endomorphism. By $\mathbb{Z}$-linearity, we have $\phi_{n\Delta_X} = [n]$ for all integers n.

Example 3.3.3. Let $f : X \to Y$ be a morphism, and let Γ_f be its graph. The induced homomorphism of Γ_f is simply the pushforward f_*. Similarly, the transpose ${\Gamma_f}^t$ induces the pullback f^*.

Example 3.3.4. Fibral correspondences induce the zero homomorphism. Let $F = \sum_i F_i$ be a fibral correspondence, with each of the F_i prime. For each fibre F_i, either $(\pi_1^{F_i})^* = 0$ or $(\pi_2^{F_i})_* = 0$; so $\phi_F = \sum_i 0 = 0$.

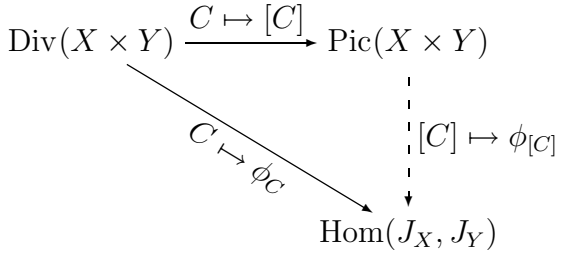
Definition 3.3.5. If correspondences C and D induce the same homomorphisms of Jacobians (that is, $\phi_C = \phi_D$), then we say that C and D are *homomorphically equivalent*, and write $C \approx D$. If $C \approx 0$, then we say C is *homomorphically trivial*.

Example 3.3.4 demonstrates that correspondences differing by a fibral correspondence are homomorphically equivalent. We will now show that rationally equivalent correspondences are homomorphically equivalent. This gives us a well-defined induced homomorphism for each rational equivalence class of correspondences.

Proposition 3.3.6. *If C and D are rationally equivalent correspondences, then C and D are homomorphically equivalent. In particular, if C is principal, then $C \approx 0$.*

Proof. The second statement implies the first. Suppose $C = \mathrm{div}(f)$ for some f in $k(X \times Y)$. For any point P of X, the pullback $\pi_1^{C*}(P) = (\pi_1^C)^{-1}(P)$ may be viewed as the divisor $C_P = \mathrm{div}(f|_{{\pi_1}^{-1}(P)})$, which is a principal divisor on the fibre ${\pi_1}^{-1}(P)$. Since C_P is principal, ${\pi_2^C}_*(C_P)$ is principal; but ${\pi_2^C}_*(C_P) = \phi_C(P)$. It follows that the image of ϕ_C is contained in $\mathrm{Prin}(Y)$, and hence that the induced homomorphisms of Picard groups and Jacobians are trivial. □

Corollary 3.3.7. *The homomorphism* $\Phi : \mathrm{Div}(X \times Y) \to \mathrm{Hom}(J_X, J_Y)$ *factors through* $\mathrm{Pic}(X \times Y)$*:*



That is, there is a well-defined homomorphism $\phi_{[C]}$ *of Jacobians (and Picard groups) for every rational equivalence class of correspondences* $[C]$*.*

The kernel of the homomorphism $\Phi : \mathrm{Div}(X \times Y) \to \mathrm{Hom}(J_X, J_Y)$ is the subgroup of correspondences on $X \times Y$ that are homomorphically equivalent to zero. By Example 3.3.4, the kernel contains $\mathrm{Fib}(X \times Y)$; so by Proposition 3.3.6, it contains the rational equivalence class of every fibral correspondence. The following proposition shows that the kernel is precisely the set of correspondences that are rationally equivalent to a fibral correspondence.

Proposition 3.3.8. *A correspondence is homomorphically trivial if and only if it is rationally equivalent to a fibral correspondence.*

Proof. Suppose C is a correspondence on $X \times Y$, and let x be a point of X. Let $\alpha : X \to J_X$ be the embedding defined by $\alpha(P) = [P - x]$. If $C \approx 0$, then we have $\phi_C(\alpha(P)) = [\phi_C(P) - \phi_C(x)] = 0$ for all P in X. The see-saw principle (Lemma 2.1.7 then implies $[C] = {\pi_1}^*([C_X]) + {\pi_2}^*([\phi_C(x)])$: that is, $[C]$ is a sum of fibral classes. The converse follows from Example 3.3.4 and Proposition 3.3.6. □

The simplest correspondences on $X \times Y$ are those subschemes of $X \times Y$ defined by a single equation. The following useful lemma shows that such correspondences are in fact homomorphically trivial.

Lemma 3.3.9. *Let* H *be an effective correspondence on* $X \times Y$*. If* H *is a hypersurface — that is, if* $H = V(F)$ *for some polynomial* F *in the functions* u_1*,* v_1*,* u_2 *and* v_2 *— then* H *is homomorphically trivial.*

Proof. The statement follows from Proposition 3.3.8. Let a be the total degree of F in u_1 and v_1, and let b the total degree of F in u_2 and v_2. Let $V = aV(u_1) + bV(u_2) = V\big(u_1^a u_2^b\big)$. Observe that V is a fibral correspondence, so $V \approx 0$. Now, $H - V = \operatorname{div}(F/(u_1^a u_2^b))$, which is principal and thus homomorphically trivial, so $H \approx V \approx 0$. □

Lemma 3.3.9 may be viewed in an entirely affine way. Let curves X and Y have the respective affine plane models $X : F_X(u, v) = 0$ and $Y : F_Y(u, v) = 0$. Let S_X and S_Y be the sets of points "at infinity" of X and Y, respectively — that is, the points which are not represented by the affine models. Note that any prime correspondence supported on $S_X \times Y$ or $X \times S_Y$ is fibral, and so homomorphically trivial. Therefore, we may reasonably ignore any such components, and consider only correspondences supported on the affine patch that is the product of the affine models for X and Y; that is, the spectrum of the ring $A_{X\times Y} := k[u_1, v_1, u_2, v_2]/(F_X(u_1, v_1), F_Y(u_2, v_2))$. Lemma 3.3.9 then becomes the following principle:

> Any effective correspondence H on $X \times Y$ with an affine model cut out by a principal ideal is homomorphically trivial.

Example 3.3.10. Let X be the curve defined by $X : v^3 = f_X(u)$ for some polynomial f_X, and consider the correspondence $C = V(u_2 - u_1)$ on $X \times X$. Now C is homomorphically trivial by Lemma 3.3.9, and

$$\begin{aligned} C = V(u_2 - u_1) &= V(u_2 - u_1, v_2^3 - v_1^3) \\ &= V(u_2 - u_1, v_2 - v_1) + V(u_2 - u_1, v_2^2 + v_2 v_1 + v_1^2) \\ &= \Delta_X + V(u_2 - u_1, v_2^2 + v_2 v_1 + v_1^2)\,; \end{aligned}$$

so $V(u_2 - u_1, v_2^2 + v_2 v_1 + v_1^2)$ induces $[-1]_{J_X}$.

Proposition 3.3.8 shows that the kernel of Φ is the group of correspondences that are rationally equivalent to fibral correspondences. The remainder of this section will be devoted to showing that Φ is surjective, and hence that the module $\operatorname{Hom}(J_X, J_Y)$ is isomorphic to the Picard group of $X \times Y$ modulo fibral correspondences. Given a homomorphism of Jacobians, the following lemma constructs a correspondence inducing the homomorphism, generalising the graph correspondences introduced in Example 3.2.2.

Lemma 3.3.11. *Let $\phi : J_X \to J_Y$ be a homomorphism of Jacobians. Then there exists a correspondence Γ_ϕ on $X \times Y$ such that $\phi_{\Gamma_\phi} = \phi$.*

Proof. Suppose that X and Y each have a rational divisor of degree one, and use these divisors to fix embeddings $\alpha_X : X \hookrightarrow J_X$ and $\alpha_Y : Y \hookrightarrow J_Y$. Each point of J_Y is equal to a sum $\sum_i \alpha_Y(y_i)$ for some g_Y points $y_1, \ldots, y_{g_Y}$ of Y. Let $\Theta_Y = \alpha_Y(Y) + \cdots + \alpha_Y(Y)$ be the theta divisor on J_Y determined by α_Y (the sum is taken $g_Y - 1$ times); the points of Θ_Y are precisely those that are equal to the sum $\sum_{i=1}^{g_Y - 1} \alpha_Y(y_i)$ for some $g_Y - 1$ points $y_1, \ldots, y_{g_Y - 1}$ of Y.

Let $\Gamma_\phi := ((\phi \circ \alpha_X) \times \alpha_Y)^* \mu^*(\Theta_Y)$, where $\mu : J_Y \times J_Y \to J_Y$ is the subtraction map, which maps (a, b) to $a - b$. Then

$$\begin{aligned}\Gamma_\phi &= \{(x, y) \in X \times Y : \phi(\alpha_X(x)) - \alpha_Y(y) \in \Theta_Y\} \\ &= \{(x, y_1), \ldots, (x, y_{g_Y}) \in X \times Y : \phi(\alpha_X(x)) = \textstyle\sum_i \alpha_Y(y_i)\}.\end{aligned}$$

The homomorphism of divisors induced by Γ_ϕ maps the prime divisor x on X to a divisor $\sum_{i=1}^{g_Y} y_i$ on Y such that $\phi(\alpha_X(x)) = \sum_{i=1}^{g_Y} \alpha_Y(y_i)$; clearly, then, the induced homomorphism of Jacobians is ϕ, as required. □

Theorem 3.3.12. *There is an isomorphism*

$$\mathrm{Pic}(X \times Y)/\mathrm{Fib}(X \times Y) \xrightarrow{\cong} \mathrm{Hom}(J_X, J_Y).$$

Proof. The homomorphism Φ is surjective by Lemma 3.3.11, and thus induces a surjective homomorphism $\mathrm{Pic}(X \times Y) \to \mathrm{Hom}(J_X, J_Y)$. By Proposition 3.3.8, the kernel of this homomorphism is generated by $\mathrm{Fib}(X \times Y)$; the result follows. □

Theorem 3.3.12 gives us an interesting insight into the structure of the Picard group of $X \times Y$. We may identify the image of $\mathrm{Fib}(X \times Y)$ in $\mathrm{Pic}(X \times Y)$ with $\mathrm{Pic}(X) \times \mathrm{Pic}(Y)$, so as $\mathbb{Z}$-modules

$$\mathrm{Pic}(X \times Y) \cong \mathrm{Pic}(X) \times \mathrm{Pic}(Y) \times \mathrm{Hom}(J_X, J_Y).$$

Thus $\mathrm{Pic}(X \times Y)$ is larger than the product of $\mathrm{Pic}(X)$ and $\mathrm{Pic}(Y)$ precisely when there exists a nontrivial homomorphism between J_X and J_Y.

Example 3.3.13. Let X and Y be curves of genus zero. Both J_X and J_Y are trivial, so $\mathrm{Hom}(J_X, J_Y) = 0$ and $\mathrm{Pic}(X) \cong \mathrm{Pic}(Y) \cong \mathbb{Z}$. By Theorem 3.3.12, then, $\mathrm{Pic}(X \times Y)$ is isomorphic to $\mathbb{Z}^2$. In fact, the isomorphism from $\mathrm{Pic}(X \times Y)$ to $\mathbb{Z}^2$ is the product of the degree functions, $d_1 \times d_2$; so the Picard group of a product of genus zero curves is completely described by the degree functions.

Example 3.3.14. Let X and Y be curves of genus one: J_X and J_Y are elliptic curves. Generically, J_X and J_Y are non-isogenous; so $\mathrm{Hom}(J_X, J_Y) = 0$, and $\mathrm{Pic}(X \times Y)$ is isomorphic to $\mathrm{Pic}(X) \times \mathrm{Pic}(Y)$. On the other hand, if J_X and J_Y are in the same isogeny class, then $\mathrm{Hom}(J_X, J_Y) \neq 0$, and $\mathrm{Pic}(X \times Y)$ strictly contains $\mathrm{Pic}(X) \times \mathrm{Pic}(Y)$.

Example 3.3.15. For any curve X, the group $\mathrm{Pic}(X \times X)$ is isomorphic to $\mathrm{Pic}(X)^2 \times \mathrm{End}(J_X)$. If the genus of X is at least one, then $\mathrm{End}(J_X)$ has a subring isomorphic to $\mathbb{Z}$; thus $\mathrm{Pic}(X \times X)$ has a subgroup isomorphic to $\mathrm{Pic}(X)^2 \times \mathbb{Z}$, where the factor of $\mathbb{Z}$ is generated by Δ_X.

Recall that the transpose of a fibral correspondence is fibral, and that the transpose of a principal correspondence is principal, so the transpose induces an involution $\mathrm{Pic}(X \times Y)/\mathrm{Fib}(X \times Y) \to \mathrm{Pic}(Y \times X)/\mathrm{Fib}(Y \times X)$, and therefore induces an involution $\mathrm{Hom}(J_X, J_Y) \to \mathrm{Hom}(J_Y, J_X)$ by Theorem 3.3.12. The following proposition shows that the induced involution on homomorphisms is in fact the Rosati involution.

Proposition 3.3.16. *The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Div}(X \times Y) & \xrightarrow{\Phi} & \mathrm{Hom}(J_X, J_Y) \\ \Big\downarrow{\scriptstyle (\cdot)^t} & & \Big\downarrow{\scriptstyle (\cdot)^\dagger} \\ \mathrm{Div}(Y \times X) & \xrightarrow{\Phi} & \mathrm{Hom}(J_Y, J_X). \end{array}$$

That is, $\phi_{C^t} = \phi_C^\dagger$ for all correspondences C.

Proof. See [39, Proposition 11.5.3] (the proof is stated for curves X and Y over the complex numbers, but holds without modification for general k). □

Remark 3.3.17. It follows immediately from Proposition 3.3.16 that homomorphisms induced by symmetric correspondences are fixed by the Rosati involution.

3.4 Composition of correspondences

Suppose we have correspondences C_1 on $X \times Y$ and C_2 on $Y \times Z$, with induced homomorphisms $\phi_{C_1} : J_X \to J_Y$ and $\phi_{C_2} : J_Y \to J_Z$ respectively. These homomorphisms may be composed, yielding a homomorphism $\phi : J_X \to J_Z$. A correspondence C inducing the homomorphism ϕ is guaranteed to exist by Lemma 3.3.11. This C is not unique, because any correspondence homomorphically equivalent to C will also induce ϕ. The following algorithm defines a composition operation for correspondences such that the degree functions are multiplicative over the composition.

Algorithm 3.4.1. Given correspondences A on $X \times Y$ and B on $Y \times Z$, returns a correspondence C on $X \times Z$ such that $\phi_C = \phi_B \circ \phi_A$ and $d_i(C) = d_i(A)d_i(B)$ for $i = 1, 2$.

function COMPOSITION(B, A)
  $A', A_X, A_Y :=$ STANDARDDECOMPOSITION(A);
  $B', B_Y, B_Z :=$ STANDARDDECOMPOSITION(B);
  $C' := A' \times_Y B'$;
  $C_X := (d_2(B) + \deg B_Y)A_X + \phi_{A^t}(B_Y)$;
  $C_Z := (d_1(A) + \deg A_Y)B_Z + \phi_B(A_Y)$;
  $C := C' + \pi_1^*(C_X) + \pi_2^*(C_Z)$; // $\pi_1 : X \times Z \to X$ and $\pi_2 : X \times Z \to Z$.
  return C;
end function;

Definition 3.4.2. We call the correspondence produced by Algorithm 3.4.1 with input B and A the *composition* of B with A, denoted $B \circ A$.

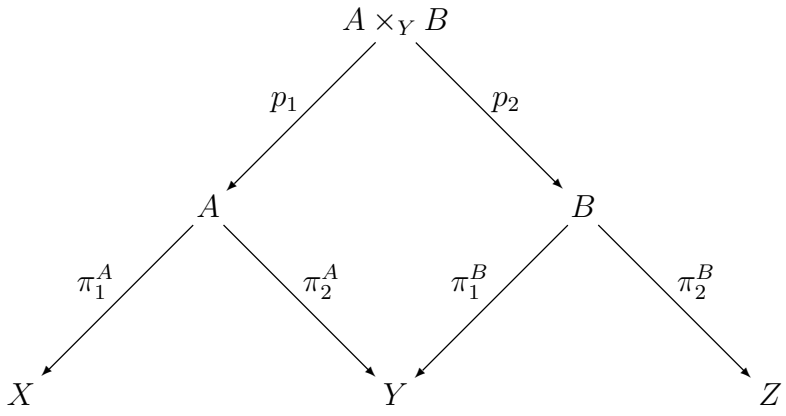
Theorem 3.4.3. *If A and B are correspondences on $X \times Y$ and $Y \times Z$ respectively, then*

$$\phi_{B \circ A} = \phi_B \circ \phi_A.$$

Further, if A' and C are correspondences on $X \times Y$ and $Z \times W$ respectively, and if $f : X \to Y$ and $g : Y \to Z$ are morphisms of curves, then

1. $C \circ (B \circ A) = (C \circ B) \circ A$,
2. $B \circ (A + A') = B \circ A + B \circ A'$,
3. $(B \circ A)^t = A^t \circ B^t$,
4. $B \circ \Gamma_f = (f \times \mathrm{Id}_Z)^*(B)$ *and* $\Gamma_g \circ A = (\mathrm{Id}_X \times g)_*(A)$,
5. $d_1(B \circ A) = d_1(B)d_1(A)$ *and* $d_2(B \circ A) = d_2(B)d_2(A)$.

Proof. Let $B \circ A := C' + \pi_1^*(C_X) + \pi_2^*(C_Z)$ be the composition of A and B, as constructed in Algorithm 3.4.1. Both $\pi_1^*(C_X)$ and $\pi_2^*(C_Z)$ are fibral, and hence are homomorphically trivial. Therefore, it suffices to check that $\phi_{C'} = \phi_B \circ \phi_A$. By definition $C' = A \times_Y B$, and the following diagram commutes:



Now, $\pi_1^{A \times_Y B} = \pi_1^A \circ p_1$ and $\pi_2^{A \times_Y B} = \pi_2^B \circ p_2$; so

$$\begin{aligned} \phi_{A \times_Y B} &= (\pi_2^{A \times_Y B}{}_*) \circ (\pi_1^{A \times_Y B *}) \\ &= \pi_2^B{}_* \circ p_{2*} \circ p_1^* \circ \pi_1^{A*} \\ &= \pi_2^B{}_* \circ \pi_1^{B*} \circ \pi_2^A{}_* \circ \pi_1^{A*} \\ &= \phi_B \circ \phi_A. \end{aligned}$$

For the first five of the algebraic properties, see Fulton [22, Proposition 16.1.1]. For property (6), observe that p_1 lifts π_1^B; therefore $A \times_Y B$ forms

a cover of degree $d_1(B)$ of A, which is in turn a degree-$d_1(A)$ cover of X. Hence $d_1(B \circ A) = d_1(A)d_1(B)$. The proof for d_2 is the same. □

Example 3.4.4. Property (4) of Theorem 3.4.3 implies that when k is a finite field, the r-th Frobenius correspondence $\mathfrak{F}_X^r$ is the r-fold composition of the Frobenius correspondence $\mathfrak{F}_X$ with itself.

Example 3.4.5. Suppose Y is a hyperelliptic curve, ι_Y its hyperelliptic involution, and let C be a correspondence on $X \times Y$. Now, $\phi_C \circ \iota_Y = -\phi_C$, so $C \circ \Gamma_{\iota_Y} \approx -C$. Thus if C is effective, then composition with Γ_{ι_Y} gives us an effective correspondence in the homomorphic equivalence class of $-C$. Property (4) of Theorem 3.4.3 tells us that $(\mathrm{Id}_X \times \iota_Y)_*(C) = C \circ \Gamma_{\iota_Y}$, which is homomorphically equivalent to $-C$. Therefore, we may conclude that any correspondence fixed by the involution $(\mathrm{Id}_X \times \iota_Y)_*$ on $\mathrm{Div}(X \times Y)$ induces the zero homorphism.

If we restrict our attention to correspondences on $X \times X$, Theorem 3.4.3 allows us to view composition of correspondences as a product, giving us a ring structure on $\mathrm{Div}(X \times X)$. This ring is traditionally called the *ring of correspondences on* X.

Corollary 3.4.6. *The group of correspondences* $\mathrm{Div}(X \times X)$*, together with the product*

$$(C, C') \mapsto C \circ C',$$

forms a $\mathbb{Z}$*-algebra with identity element* Δ_X *and involution* $(\cdot)^t$*.*

The composition product is generally not commutative, so in general $\mathrm{Div}(X \times X)$ is not a commutative ring. However, composition of *symmetric* correspondences is commutative by property (3) of Theorem 3.4.3.

Correspondences E on $X \times X$ act on $\mathrm{Div}(X \times Y)$ by $C \mapsto C \circ E$. This action extends $\mathbb{Z}$-linearly, so if we view $\mathrm{Div}(X \times X)$ as a ring then $\mathrm{Div}(X \times Y)$ has a right $\mathrm{Div}(X \times X)$-module structure. Similarly, correspondences E' on $Y \times Y$ act on $\mathrm{Div}(X \times Y)$ by $C \mapsto E' \circ C$, so $\mathrm{Div}(X \times Y)$ also has a left $\mathrm{Div}(Y \times Y)$-module structure.

Theorem 3.4.7. *The homomorphism* $\Phi : \mathrm{Div}(X \times X) \to \mathrm{End}(J_X)$ *of* $\mathbb{Z}$*-modules extends naturally to a homomorphism of* $\mathbb{Z}$*-algebras. In particular, there is an isomorphism of* $\mathbb{Z}$*-algebras*

$$\mathrm{End}(J_X) \cong \mathrm{Pic}(X \times X)/\mathrm{Fib}(X \times X).$$

Proof. Corollary 3.4.6 gives us a $\mathbb{Z}$-algebra structure on $\mathrm{Div}(X \times X)$. Theorem 3.4.3 shows that Φ takes compositions to compositions, and so extends to a $\mathbb{Z}$-algebra homomorphism. To establish the isomorphism, it remains to check that $\mathrm{Fib}(X \times X)$ is a two-sided ideal of $\mathrm{Div}(X \times X)$, since Φ factors through $\mathrm{Pic}(X \times X)$. Indeed, each fibral correspondence is a sum of graphs of constant morphisms, so this follows from properties (2) and (4) of Theorem 3.4.3. □

Remark 3.4.8. For each endomorphism ϕ of J_X, Lemma 3.3.11 constructs a correspondence Γ_ϕ on $X \times X$ inducing ϕ, depending on a choice of embedding of X into J_X. If we fix an embedding of X into J_X, then we may define a distinguished graph Γ_ϕ for each endomorphism ϕ, and composition with Γ_ϕ therefore gives an action of $\mathrm{End}(J_X)$ on $\mathrm{Div}(X \times Y)$: in fact, we have endowed $\mathrm{Div}(X \times Y)$ with the structure of a left $\mathrm{End}(J_X)$-module. In a similar way, we may (simultaneously) view $\mathrm{Div}(X \times Y)$ as a right $\mathrm{End}(J_Y)$-module.

3.5 Differential matrices

Given an arbitrary correspondence, it may not be immediately obvious what the induced homomorphism is. The traditional approach for identifying the induced homomorphism is to examine the action of the correspondence on spaces of differentials.

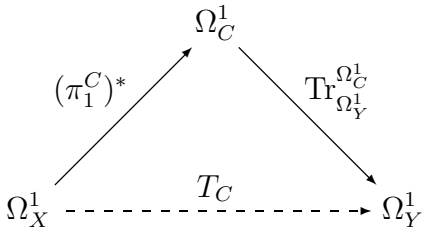
Suppose C is a correspondence on $X \times Y$. We have the natural tangent map $\mathcal{T}_0(\phi_C) : \mathcal{T}_0(J_X) \to \mathcal{T}_0(J_Y)$, which gives us a representation

$$\mathrm{Hom}(J_X, J_Y) \to \mathrm{Hom}(\mathcal{T}_0(J_X), \mathcal{T}_0(J_Y)).$$

The tangent space $\mathcal{T}_0(J_X)$ has a natural isomorphism with the cohomology[1] group $H^0(X, \Omega^1_X)$, which is isomorphic to the g_X-dimensional k-vector space Ω^1_X. Fixing bases for Ω^1_X and Ω^1_Y, we have a representation

$$\mathrm{Hom}(J_X, J_Y) \to \mathrm{Hom}(\Omega^1_X, \Omega^1_Y) \cong \mathrm{Mat}_{g_X \times g_Y}(k).$$

To calculate the image under this representation of a correspondence C on $X \times Y$, we must compute the action of the induced homomorphism of C on the spaces of differentials of X and Y. If C is prime, then we may consider it as a curve; the tangent map induces the homomorphism $T_C : \Omega^1_X \to \Omega^1_Y$ defined by pulling back a differential from Ω^1_X to Ω^1_C, then taking the trace from Ω^1_C to Ω^1_Y, as in the following diagram.



The definition extends $\mathbb{Z}$-linearly to give a homomorphism $T_C : \Omega^1_X \to \Omega^1_Y$ for every correspondence C on $X \times Y$. If we fix bases $\{\omega_1, \ldots, \omega_{g_X}\}$ for Ω^1_X and $\{\omega'_1, \ldots, \omega'_{g_Y}\}$ for Ω^1_Y, then we may write $T_C(\omega_i) = \sum_j m_{ij}\omega'_j$ for some m_ij in k. We define the *differential matrix* of C (with respect to the bases) by

$$M_C := (m_{ij}).$$

We have a diagram

$$\begin{array}{ccccc}
\mathrm{Div}(X \times Y) & \xrightarrow{C \mapsto \phi_C} & \mathrm{Hom}(J_X, J_Y) & \xrightarrow{\phi_C \mapsto \mathcal{T}_0(\phi_C)} & \mathrm{Hom}(\mathcal{T}_0(J_X), \mathcal{T}_0(J_Y)) \\
\Big\downarrow{\scriptstyle C \mapsto M_C} & & & & \Big\downarrow{\scriptstyle \mathcal{T}_0(\phi_C) \mapsto T_C} \\
\mathrm{Mat}_{g_X \times g_Y}(k) & & \xleftarrow{\quad\cong\quad} & & \mathrm{Hom}(\Omega^1_X, \Omega^1_Y)
\end{array}$$

[1]The reader not versed in cohomology theory need not panic; cohomology groups in this document are conveniently camouflaged as more concrete groups.

General functoriality arguments show that the map $C \mapsto M_C$ is in fact a representation. The representation $C \mapsto M_C$ respects composition (again, by functoriality); that is, $M_{C \circ D} = M_D M_C$. If the characteristic of k is zero, then the representation is faithful. On the other hand, if k is a field of positive characteristic p, then the representation cannot be faithful, because $pC \mapsto pM_C = 0$ for all correspondences C on $X \times Y$.

Chapter 4

Intersection theory on $X \times Y$

In this chapter, we give a brief account of intersection theory on the surface $X \times Y$. Intersection numbers provide the most basic tool for analysis of correspondences, much as the degree map is the most basic tool for analysis of plane curves — in fact, the degree of a plane curve is its intersection number with a hyperplane. We will survey the most useful results for intersection theory on general surfaces, specialising to the special case of a product of curves. The reader may refer to Hartshorne [29, §V.1] for an overview of intersection theory on general surfaces; Fulton [22] is the definitive reference.

4.1 Intersection numbers

Correspondences on $X \times Y$ are supported on curves on $X \times Y$. A proper understanding of correspondences therefore requires an understanding of the geometry of curves on $X \times Y$. Curves on a surface with no common component intersect in a finite set of points (with some multiplicities); the cardinality of this intersection gives us information about the relative geometry of the curves. Extending the intersection of curves $\mathbb{Z}$-linearly to intersections of correspondences, we obtain the *intersection number*. Our definition of the intersection number follows that of Hartshorne [29].

Theorem 4.1.1. *There is a unique bilinear, symmetric pairing*

$$\mathrm{Div}(X \times Y)^2 \longrightarrow \mathbb{Z},$$

denoted by $(C, D) \mapsto C.D$*, satisfying the following properties:*

- *if* C *and* D *are nonsingular prime correspondences on* $X \times Y$ *meeting transversally, then* $C.D = \#(C \cap D)$*, the number of points (counting multiplicity) of* $C \cap D$*, and*
- *if* C *is rationally equivalent to* C'*, then* $C.D = C'.D$ *for all correspondences* D*. In particular, this pairing induces a well-defined bilinear symmetric pairing* $\mathrm{Pic}(X \times Y)^2 \longrightarrow \mathbb{Z}$*.*

The integer $C.D$ *is called the* intersection number *of* C *and* D*.*

Proof. The pairing is defined on any nonsingular projective surface. See Hartshorne [29, Theorem V.1.1] for a concise description. □

Definition 4.1.2. If C and C' are correspondences on $X \times Y$ such that $C.D = C'.D$ for all correspondences D on $X \times Y$, then we say C and C' are *numerically equivalent*. The group of correspondences on $X \times Y$ modulo numerical equivalence is called the *Neron–Severi group* of $X \times Y$, denoted $\mathrm{NS}(X \times Y)$.

Since the intersection number is constant on rational equivalence classes, rationally equivalent correspondences are numerically equivalent. However, numerically equivalent correspondences need not be rationally equivalent. If $\mathrm{Pic}^0(X)$ is nontrivial, then we may choose a divisor D on X such that $[D]$ is a nonzero element of $\mathrm{Pic}^0(X)$. The divisor D pulls back to a fibral correspondence $F = \pi_1^*(D)$ on $X \times X$, which is numerically equivalent to zero (because $\deg(D) = 0$) but not rationally equivalent to zero (because $[D] \neq 0$). We will see in the next chapter that the difference between numerical and rational equivalence on $X \times Y$ is completely determined by the groups $\mathrm{Pic}^0(X)$ and $\mathrm{Pic}^0(Y)$.

Given correspondences C and D, Theorem 4.1.1 allows us to choose divisors C' in $[C]$ and D' in $[D]$ with transversally intersecting support; we

may then use $C.D = [C].[D] = C'.D'$ to compute the intersection number of C and D. The following lemma gives a sheaf-theoretic expression for the intersection number.

Lemma 4.1.3. *Let C and D be correspondences on $X \times Y$, with C prime and D effective. If the supports of C and D meet transversally, then*

$$C.D = \deg_C(\mathcal{L}(D) \otimes \mathcal{O}_C).$$

Proof. See Hartshorne [29, Lemma V.1.3] or Fulton [22, Example 2.4.9]. □

Remark 4.1.4. Lemma 4.1.3 may be used to show that if C is a prime correspondence on $X \times Y$ and $\mathcal{N}_{C/X\times Y}$ is the normal sheaf of C in $X \times Y$, then $C.C = \deg_C \mathcal{N}_{C/X\times Y}$ (see Hartshorne [29, Example V.1.4.1]).

We call $C.C$ the *self-intersection number* of C. It is important to note that the self-intersection of a correspondence is in general *not* positive, even if the correspondence is effective (see Example 4.2.8 below). The classical Castelnuovo–Severi inequality gives an effective upper bound for the self-intersection number of a correspondence in terms of its degrees.

Lemma 4.1.5 (Castelnuovo–Severi inequality). *For all correspondences C,*

$$C.C \leq 2d_1(C)d_2(C).$$

Further, $C.C = 2d_1(C)d_2(C)$ if and only if C is numerically equivalent to a fibral correspondence.

Proof. See Hartshorne [29, Theorem V.1.9, Exercise V.1.9] or Fulton [22, Example 16.1.10]. □

The degree functions for correspondences may be expressed as intersection numbers, as shown by the following lemma.

Lemma 4.1.6. *If P and Q are points of X and Y respectively, then $d_1(C) = C.\pi_1^*(P)$ and $d_2(C) = C.\pi_2^*(Q)$ for all correspondences C on $X \times Y$.*

Proof. It is enough to prove the statement in the case where C is prime. The degree $d_1(C)$ is equal to the number of points in the fibre $\pi_1^{C*}(P)$, which is equal to $C.\pi_1^*(P)$; similarly, $d_2(C) = C.\pi_2^*(Q)$. □

In particular, we see that the intersection number of fibres of the same projection is zero, and that the intersection number of fibres of distinct projections is one. Using rational equivalence, we may extend Lemma 4.1.6 to the following useful proposition.

Proposition 4.1.7. *Let C and V be correspondences on $X \times Y$. If V is homomorphically trivial, then*

$$C.V = d_1(C)d_2(V) + d_2(C)d_1(V).$$

Proof. By Proposition 3.3.8, V is rationally equivalent to a fibral correspondence F, and $C.V = C.F$. By Lemma 3.1.3, there are divisors $\sum_i n_i P_i$ on X and $\sum_j m_j Q_j$ on Y such that $F = \pi_1^*(\sum_i n_i P_i) + \pi_2^*(\sum_j m_j Q_j)$. Then

$$\begin{aligned} C.F &= C.\Big(\textstyle\sum_i n_i \pi_1^*(P_i) + \sum_j m_j \pi_2^*(Q_j)\Big) \\ &= (\textstyle\sum_i n_i)(C.\pi_1^*(P_i)) + (\sum_j m_j)(C.\pi_2^*(Q_j)) \end{aligned}$$

Applying Lemma 4.1.6, we have $C.\pi_1^*(P_i) = d_1(C)$ and $C.\pi_2^*(Q_j) = d_2(C)$ for all i and j; Lemma 4.1.6 also gives $d_1(F) = \sum_j m_j$ and $d_2(F) = \sum_i n_i$, so we conclude that $C.V = C.F = d_1(C)d_2(F) + d_2(C)d_1(F)$. □

Example 4.1.8. If V is a homomorphically trivial correspondence on $X \times X$, then Proposition 4.1.7 implies $V.\Delta_X = d_1(V) + d_2(V)$, since $d_1(\Delta) = 1$ and $d_2(\Delta) = 1$.

Proposition 4.1.7 implies that homomorphically trivial correspondences with the same degrees are numerically equivalent; this makes computation of intersection numbers involving homomorphically trivial correspondences particularly easy. Things are not so simple for intersection numbers of homomorphically nontrivial correspondences: homomorphically nontrivial correspondences with the same degrees are generally *not* numerically equivalent. We demonstrate this with an example where two correspondences with the same degrees have different intersection numbers with the diagonal.

Example 4.1.9. Suppose k is a field of characteristic not two or three, and let X be the curve of genus one defined by $X : v^2 = u^3 - u$. The curve X has an automorphism $i : (u, v) \mapsto (-u, \sqrt{-1}v)$ of order four, defined over $k(\sqrt{-1})$. Observe that i^2 is the hyperelliptic involution ι_X of X. Let Γ_i be the graph of i, and Γ_{i^2} the graph of i^2; note that both are $(1,1)$-correspondences. The intersection of the diagonal correspondence Δ_X with the graph of an automorphism counts the number of fixed points of the automorphism. Now, i has two fixed points, namely $(0,0)$ and the point at infinity; so $\Delta_X.\Gamma_i = 2$. On the other hand, i^2 has four fixed points: $(0,0)$, $(1,0)$, $(-1,0)$ and the point at infinity, so $\Delta_X.\Gamma_{i^2} = 4$. Thus Γ_i and Γ_{i^2} are not numerically equivalent, and the intersection number pairing on $X \times X$ is not completely described by the degree functions.

4.2 The adjunction formula

In this section we state the adjunction formula for $X \times Y$, which expresses the arithmetic genus of a prime correspondences in terms of intersection numbers. We may apply this to compute some useful intersection numbers.

Theorem 4.2.1 (Adjunction formula). *If C is a prime correspondence on $X \times Y$, then the arithmetic genus of C is given by*

$$p_a(C) = \frac{1}{2}C.C + (g_X - 1)d_1(C) + (g_Y - 1)d_2(C) + 1.$$

Proof. The classical adjunction formula for curves C on a surface S states

$$2p_a(C) - 2 = C.(C + K_S),$$

where K_S is a canonical divisor on S (see Serre [56, IV.8, Proposition 5] or Hartshorne [29, §V.1.5]). The usual proof is to compute the degree of the canonical sheaf $\mathcal{L}(C + K_{X\times Y}) \otimes \mathcal{O}_C$ on C, which is $2p_a(C) - 2$ by Lemma 2.1.14, and $C.(C + K_{X\times Y})$ by Lemma 4.1.3. Specialising to $S = X \times Y$, we have $C.K_{X\times Y} = (2g_X - 2)d_1(C) + (2g_Y - 2)d_2(C)$ by Lemma 2.1.15 and Proposition 4.1.7; the result follows after some elementary algebra. □

Remark 4.2.2. The arithmetic genus is (by definition) an integer. It therefore follows from Theorem 4.2.1 that the self-intersection of a correspondence is *always* an even integer.

The arithmetic genus is defined only for effective correspondences, but the right-hand-side of the adjunction formula is well-defined for any correspondence. We therefore define the *virtual* arithmetic genus of any correspondence to be this quantity. If a correspondence is effective, then its arithmetic and virtual arithmetic genera coincide.

Definition 4.2.3. Let C be a correspondence on $X \times Y$. We define the *virtual arithmetic genus* of C, denoted $p_a(C)$, to be

$$p_a(C) := \frac{1}{2} C.C + (g_X - 1)d_1(C) + (g_Y - 1)d_2(C) + 1.$$

By definition, every correspondence numerically equivalent to zero has virtual arithmetic genus one. In particular, $p_a(0) = 1$; so the virtual arithmetic genus is *not* additive.

Example 4.2.4. Suppose that F is a homomorphically trivial correspondence on $X \times Y$. By Proposition 4.1.7, $F.F = 2d_1(F)d_2(F)$; substituting into the adjunction formula (Theorem 4.2.1), we have

$$p_a(F) = (d_1(F) - 1)(d_2(F) - 1) + g_X d_1(F) + g_Y d_2(F).$$

In particular, if $H \subset X \times Y$ is a hypersurface — that is, a correspondence defined by a principal ideal — then $H \approx 0$ by Lemma 3.3.9, and thus $p_a(H) = (d_1(H)-1)(d_2(H)-1)+g_X d_1(H)+g_Y d_2(H)$. This is the analogue for $X \times Y$ of the well-known formula for the arithmetic genus of a projective curve: if X is a curve of degree d, then $p_a(X) = (d-1)(d-2)/2$.

Remark 4.2.5. We will see in the next chapter that if we fix integers a and b, then the virtual arithmetic genus of an (a, b)-correspondence is bounded from above. The bound is sharp: in fact, an (a, b)-correspondence has the highest possible virtual genus if and only if it is homomorphically trivial.

Expressing intersection numbers purely in terms of virtual arithmetic genera can be quite useful. If an efficient method is available for computing

arithmetic genera of correspondences, then the following result provides an efficient method for computing intersection numbers[1].

Corollary 4.2.6. *If C and D are correspondences on $X \times Y$, then*

$$C.D = p_a(C + D) - (p_a(C) + p_a(D)) + 1.$$

Proof. Note that $(C + D).(C + D) = C.C + D.D + 2C.D$. We apply Theorem 4.2.1 to express the self-intersections in terms of virtual arithmetic genera and degrees; the formula follows after some elementary algebra. □

Remark 4.2.7. The formula of Corollary 4.2.6 may be written as

$$C.D = \big(p_a(C + D) + p_a(0)\big) - \big(p_a(C) + p_a(D)\big).$$

Hence the intersection number measures the failure of the (virtual) arithmetic genus to be additive on $\mathrm{Div}(X \times Y)$.

Example 4.2.8. Let α be an automorphism of X, and let Γ_α be its graph. The restricted projections $\pi_1^{\Gamma_\alpha}$ and $\pi_2^{\Gamma_\alpha}$ are isomorphisms, so $p_a(\Gamma_\alpha) = g_X$ and $d_1(\Delta_X) = d_2(\Delta_X) = 1$. Applying the adjunction formula (Theorem 4.2.1), we see that $\Gamma_\alpha.\Gamma_\alpha = 2 - 2g_X$. In particular, when $\alpha = \mathrm{Id}_X$, we have

$$\Delta_X.\Delta_X = 2 - 2g_X.$$

We may use this result in combination with Corollary 4.2.6 to see that $p_a(2\Gamma_\alpha) = 1$ — a value completely independent of α (and of X!).

Example 4.2.9. Suppose X is a curve over a finite field k. The intersection number $\mathfrak{F}_X^r.\Delta_X$ counts the fixed points of the r^{th} Frobenius map $\mathcal{F}^{(r)} : X \to X$, which are precisely the k-rational points of X; hence

$$\mathfrak{F}_X^r.\Delta_X = \#X(k).$$

[1]The author has found that in practice, intersection numbers of arbitrary correspondences are often more rapidly computed by computing arithmetic genera via multivariate Hilbert series and applying Corollary 4.2.6 than by using Gröbner basis methods.

Chapter 5

The correspondence pairing

Traditionally, intersection theory is the primary tool in the analysis of divisors on surfaces. When applied to the theory of correspondences, however, the intersection number has a significant shortcoming: it is not well-defined on homomorphic equivalence classes. For example, Proposition 3.3.8 tells us that all fibral correspondences are homomorphically trivial; but it is clear that not all fibral correspondences are numerically equivalent to zero.

In this chapter, we construct a symmetric, bilinear, positive semi-definite pairing on correspondences that is well-defined and positive-definite on homomorphic equivalence classes. The pairing is defined geometrically, in terms of intersection numbers; but since the pairing is well-defined on homomorphic equivalence classes, it also has an interpretation in terms of induced homomorphisms of Jacobians. The main theorem of the chapter shows that the pairing induces a twisted trace form on homomorphisms. This allows us to make precise the relationship between rational, homomorphic, and numerical equivalence on correspondences.

The pairing has appeared in the work of Weil [65]; in [64], Weil proved the positive-definiteness of the pairing on $X \times X$, and used this to give the first complete proof of the Riemann hypothesis for algebraic curves of arbitrary genus. We will extend the pairing to products of possibly distinct curves $X \times Y$, and prove that this more general pairing is positive-definite. Our interest in the pairing is in its application as a computational tool for

identification of correspondences, and detection of $\mathbb{Z}$-linear dependence.

5.1 The pairing

Recall Proposition 4.1.7: if C and F are correspondences on $X \times Y$, and F is homomorphically trivial, then $C.F = d_1(C)d_2(F) + d_2(C)d_1(F)$. This equality does not hold if F is not homomorphically trivial; but it turns out that the difference between $C.F$ and $d_1(C)d_2(F) + d_2(C)d_1(F)$ depends only upon the homomorphic equivalence classes of C and F. This observation forms the basis of our new pairing.

Definition 5.1.1. We define a pairing $\langle \cdot\,, \cdot \rangle : \mathrm{Div}(X \times Y)^2 \to \mathbb{Z}$, called the *correspondence pairing* (or simply *the pairing*), by

$$\langle C, D \rangle \;:=\; (d_1(C)d_2(D) + d_2(C)d_1(D)) - C.D.$$

Theorem 5.1.2. *The pairing of Definition 5.1.1 is symmetric, bilinear, and well-defined on homomorphic equivalence classes. Further, it induces a positive-definite pairing on numerical equivalence classes of correspondences.*

Proof. The pairing inherits symmetry, bilinearity and invariance on rational equivalence classes from the corresponding properties of the intersection number in Theorem 4.1.1. To extend the invariance from rational equivalence classes to homomorphic equivalence classes, we need only that the pairing be trivial on fibral correspondences; this is immediate from Proposition 4.1.7. The positive definiteness on numerical equivalence classes is directly implied by the Castelnuovo–Severi inequality (Lemma 4.1.5). □

Example 5.1.3. In Example 4.2.8, we noted that $\Delta_X.\Delta_X = 2 - 2g_X$; hence

$$\langle \Delta_X, \Delta_X \rangle = 1 \cdot 1 + 1 \cdot 1 - (2 - 2g_X) = 2g_X.$$

We may adapt the adjunction formula (Theorem 4.2.1) to express the self-pairing of a correspondence in terms of its virtual arithmetic genus.

Proposition 5.1.4. *For all correspondences C on $X \times Y$, we have*

$$\langle C, C\rangle = 2\big((d_1(C)-1)(d_2(C)-1) + g_X d_1(C) + g_Y d_2(C) - p_a(C)\big).$$

Proof. We have $C.C = 2p_a(C) - 2 - (2g_X - 2)d_1(C) + (2g_Y - 2)d_2(C)$ by Theorem 4.2.1; the formula follows after some elementary algebra. □

Example 5.1.5. Let X and Y be curves of genus zero, and suppose C is a correspondence on $X \times Y$. The Jacobians J_X and J_Y are both trivial, so $\mathrm{Hom}(J_X, J_Y) = 0$, and thus $C \approx 0$. The self-pairing of C is therefore zero, and so Proposition 5.1.4 implies that

$$p_a(C) = (d_1(C)-1)(d_2(C)-1).$$

5.2 Composition and the pairing

Next, we investigate the behaviour of the pairing with respect to composition of correspondences. We will see that the transpose of a correspondence is its adjoint with respect to the pairing, and thus that the pairing of *any* two correspondences may be expressed as a pairing with a diagonal. This is both a useful calculational device and an essential ingredient in our arithmetic interpretation of the pairing.

Let A be a correspondence on $X \times Y$. We say that a correspondence A^* on $Y \times X$ is an *adjoint*[1] for A if for all curves Z and all correspondences B on $Z \times X$ and C on $Z \times Y$ we have

$$\langle A \circ B, C\rangle = \langle B, A^* \circ C\rangle.$$

It follows from the symmetry of the pairing that A^* is an adjoint for A if and only if A is an adjoint for A^*. Since the pairing is defined in terms of intersection numbers, the adjoint of a correspondence is unique up to numerical equivalence. The following theorem shows that the transpose of a

[1] Our definition of adjoints follows that of Lang [38, Chapter XV] for linear maps of modules with a bilinear symmetric form.

correspondence is its adjoint; thus every correspondence has an adjoint.

Before proving the theorem, we prove a lemma demonstrating a surprising connection between intersection numbers on $X \times Y$, on $X \times X$ and on $Y \times Y$. We will see that every intersection number of correspondences on $X \times Y$ may be transformed to an intersection number on $X \times X$ or $Y \times Y$. This flexibility is inherited by the pairing.

Lemma 5.2.1. *Let C_1 and C_2 be correspondences on $X \times Y$. Then*

$$C_1.C_2 = (C_2{}^t \circ C_1).\Delta_X = (C_1{}^t \circ C_2).\Delta_Y.$$

Proof. See Fulton [22, Example 16.1.3] for a complete proof. Naively, take representatives for C_1 and C_2 intersecting transversally. Then $C_1.C_2$ counts the points (P, Q) on $X \times Y$ that lie on both C_1 and C_2. If (P, Q) appears in the intersection of C_1 and C_2, then the point P on X is mapped to (a divisor containing) Q by ϕ_{C_1}, which is then mapped back to (a divisor containing) P by $\phi_{C_2{}^t}$, and so (P, Q) corresponds to (P, P) on $C_2{}^t \circ C_1$. The point (P, P) clearly lies on Δ_X, and is thus counted by $(C_2{}^t \circ C_1).\Delta_X$. Conversely, if (P, P) lies on $C_2{}^t \circ C_1$, then it is counted by $(C_2{}^t \circ C_1).\Delta_X$. The point P is mapped to some divisor $\sum_i n_i Q_i$ on Y by ϕ_{C_1}. The image of at least one of the Q_i under $\phi_{C_2{}^t}$ must contain P; these pairs (P, Q_i) lie on both C_1 and C_2, and thus are counted by $C_1.C_2$. □

Now we can prove the adjoint theorem, which shows that the transpose of a correspondence is its adjoint. Since every correspondence has a transpose, the theorem implies that every correspodence has an adjoint.

Theorem 5.2.2 (Adjoint theorem). *If A is a correspondence on $Y \times Z$, then A^t is an adjoint for A with respect to the pairing: that is, for all correspondences B on $X \times Y$ and C on $X \times Z$, we have*

$$\langle A \circ B, C \rangle = \langle B, A^t \circ C \rangle.$$

Proof. The pairing is bilinear, and composition is distributive, so we may assume without loss of generality that A, B and C are prime. Further, the

pairing is trivial on fibral correspondences, and transposition and composition both send fibral correspondences to fibral correspondences; so we may assume that A, B and C are nonfibral. By Theorem 3.4.3,

$$\begin{aligned} d_1(A \circ B)d_2(C) &= d_1(A)d_1(B)d_2(C) \\ &= d_1(B)d_2(A^t)d_2(C) \\ &= d_1(B)d_2(A^t \circ C), \end{aligned}$$

and similarly $d_2(A \circ B)d_1(C) = d_2(B)d_1(A^t \circ C)$. It remains to show that $(A \circ B).C = B.(A^t \circ C)$. This is achieved by twice applying Lemma 5.2.1:

$$\begin{aligned} (A \circ B).C &= \Delta_X.(B^t \circ A^t \circ C) \\ &= B.(A^t \circ C), \end{aligned}$$

proving the theorem. □

Example 5.2.3. Let X be a curve over the finite field $\mathbb{F}_q$. We will use the adjoint theorem to compute the pairing on the Frobenius correspondences on $X \times X$. Suppose s and r are positive integers, with $s \geq r$. By Theorem 5.2.2, $\langle \mathfrak{F}_X^s, \mathfrak{F}_X^r \rangle = \left\langle (\mathfrak{F}_X^r)^t \circ \mathfrak{F}_X^s, \Delta_X \right\rangle$; but $(\mathfrak{F}_X^r)^t \circ \mathfrak{F}_X^s = [q^r]_{J_X} \circ \mathfrak{F}_X^{(s-r)}$, so $\langle \mathfrak{F}_X^s, \mathfrak{F}_X^r \rangle = q^r \left\langle \mathfrak{F}_X^{(s-r)}, \Delta_X \right\rangle$. If $s = r$, then $\left\langle \mathfrak{F}_X^{(s-r)}, \Delta_X \right\rangle = \langle \Delta_X, \Delta_X \rangle$, and from Example 5.1.3, $\langle \Delta_X, \Delta_X \rangle = 2g_X$; hence

$$\langle \mathfrak{F}_X^r, \mathfrak{F}_X^r \rangle = 2g_X q^r.$$

If $s > r$, then $\left\langle \mathfrak{F}_X^{(s-r)}, \Delta_X \right\rangle = 1 + q^{(s-r)} - \mathfrak{F}_X^{(s-r)}.\Delta_X$, and from Example 4.2.9 we have $\mathfrak{F}_X^{(s-r)}.\Delta_X = \#X(\mathbb{F}_{q^{(s-r)}})$, so

$$\langle \mathfrak{F}_X^s, \mathfrak{F}_X^r \rangle = q^r + q^s - q^r \#X(\mathbb{F}_{q^{(s-r)}}),$$

and in particular

$$\langle \mathfrak{F}_X^r, \Delta_X \rangle = 1 + q^r - \#X(\mathbb{F}_{q^r}).$$

5.3 Trace formulae

The reader with some knowledge of curves over finite fields may have observed that the value computed for $\langle \mathfrak{F}_X^r, \Delta_X \rangle$ in Example 5.2.3 coincides with the trace of the r^{th} Frobenius endomorphism $\mathcal{F}^{(r)}$ on J_X. The following lemma shows that this is no coincidence: the pairing of any correspondence with a diagonal correspondence is the trace of its induced endomorphism.

Lemma 5.3.1. *Let C be a correspondence on $X \times X$. The pairing of C with the diagonal Δ_X is equal to the trace of (the rational representation[2] of) the induced endomorphism ϕ_C of J_X:*

$$\langle C, \Delta_X \rangle = \mathrm{Tr}(\phi_C).$$

Proof. The statement follows immediately from a classical formula, which states $\mathrm{Tr}(\phi_C) = d_1(C) + d_2(C) - C.\Delta_X$: see Lange & Birkenhake [39, Proposition 11.5.2]. □

Example 5.3.2. The trace formula gives an alternative method of calculating pairings. For example, Δ_X induces the identity $[1]_{J_X}$, so by Lemma 5.3.1

$$\langle \Delta_X, \Delta_X \rangle = \mathrm{Tr}([1]_{J_X}) = 2g_X;$$

this agrees the value for $\langle \Delta_X, \Delta_X \rangle$ that we derived in Example 5.1.3.

The adjoint theorem (Theorem 5.2.2) extends the trace formula (Lemma 5.3.1) to express the pairing of any two correspondences as a *twisted trace*. This gives us a purely arithmetic interpretation of the pairing on the induced homomorphisms.

Theorem 5.3.3. *Let C and D be correspondences on $X \times Y$. Then*

$$\langle C, D \rangle = \mathrm{Tr}_{\mathrm{End}(J_X)/\mathbb{Z}}(\phi_D^\dagger \circ \phi_C) = \mathrm{Tr}_{\mathrm{End}(J_Y)/\mathbb{Z}}(\phi_D \circ \phi_C^\dagger).$$

Proof. Theorem 5.2.2 gives $\langle C, D \rangle = \langle D^t \circ C, \Delta_X \rangle$, which equals $\mathrm{Tr}(\phi_{D^t \circ C})$

[2] we will simply use the word "trace" in the sequel.

by Lemma 5.3.1; but $\phi_{D^t \circ C} = \phi_D^\dagger \circ \phi_C$, so $\langle C, D\rangle = \mathrm{Tr}(\phi_D^\dagger \circ \phi_C)$. Clearly $\langle C, D\rangle = \langle C^t, D^t\rangle$, and so $\langle C, D\rangle = \langle C^t, D^t\rangle = \mathrm{Tr}(\phi_D \circ \phi_C^\dagger)$. □

Example 5.3.4. We may simplify Example 5.2.3 using Theorem 5.3.3: if X is a curve over $\mathbb{F}_q$ then $\langle \mathfrak{F}_X^s, \mathfrak{F}_X^r\rangle = q^{\min(r,s)} \cdot \mathrm{Tr}(\mathcal{F}^{(|s-r|)})$ for all positive integers r and s.

Corollary 5.3.5. *A correspondence C on $X \times Y$ is homomorphically trivial if and only if $\langle C, D\rangle = 0$ for all correspondences D on $X \times Y$.*

Proof. Let C_r denote the r-fold composition of $C \circ C^t$ with itself. Note that $\langle C, C \circ C_r\rangle = \mathrm{Tr}((\phi_C \circ \phi_C^\dagger)^r)$ by Theorem 5.3.3. If $\langle C, D\rangle = 0$ for all D, then for all $r \geq 0$ we have $\langle C, C \circ C_r\rangle = 0$ and thus $\mathrm{Tr}((\phi_C \circ \phi_C^\dagger)^r) = 0$. Therefore, the characteristic polynomial of $\phi_C \circ \phi_C^\dagger$ is zero, which implies $\phi_C \circ \phi_C^\dagger = 0$; but this is only possible if $\phi_C = 0$. The converse follows from Theorem 5.1.2. □

Corollary 5.3.6. *A correspondence is homomorphically trivial if and only if it is numerically equivalent to a fibral correspondence.*

Proof. Let C be a correspondence on $X \times Y$. If F_X is a fibre of π_1, and F_Y a fibre of π_2, then $\langle C, D\rangle = (d_1(C)F_Y + d_2(C)F_X - C).D$ by Lemma 4.1.6. We have $C \approx 0$ if and only if $(d_1(C)F_Y + d_2(C)F_X - C).D = 0$ for all correspondences D on $X \times Y$, if and only if $(d_1(C)F_Y + d_2(C)F_X - C)$ is numerically equivalent to 0, if and only if C is numerically equivalent to $(d_1(C)F_Y + d_2(C)F_X)$, which is fibral. □

Corollary 5.3.7. *The pairing is positive definite on homomorphic equivalence classes.*

Proof. Follows immediately from Theorem 5.1.2 and Corollary 5.3.5. □

Remark 5.3.8. Note that in the case $Y = X$, Corollary 5.3.7 immediately implies Lemma 2.2.7.

Corollary 5.3.9. $\mathrm{Hom}(J_X, J_Y) \cong \mathrm{NS}(X \times Y)/(\mathbb{Z}^2)$.

Proof. By Corollary 5.3.6, a correspondence is homomorphically trivial if and only if it is numerically equivalent to a fibral correspondence; therefore, $\mathrm{Hom}(J_X, J_Y)$ is isomorphic to the quotient of $\mathrm{NS}(X \times Y)$ by the submodule of $\mathrm{NS}(X \times Y)$ generated by the fibral correspondences. All fibres of π_1 are numerically equivalent, as are all fibres of π_2; thus the submodule of $\mathrm{NS}(X \times Y)$ generated by the fibral correspondences is isomorphic to $\mathbb{Z}^2$. □

Corollary 5.3.10. *If X and Y are curves of genus one, then $\langle C, C\rangle = 2\deg(\phi_C)$ for all correspondences C on $X \times Y$.*

Proof. By Theorem 5.3.3, we have $\langle C, C\rangle = \mathrm{Tr}(\phi_C \circ \phi_C^\dagger)$; but it is well-known that if J_X and J_Y are elliptic curves, then $\phi_C \circ \phi_C^\dagger = [\deg \phi_C]$. Thus $\langle C, C\rangle = \mathrm{Tr}([\deg \phi_C]) = 2\deg \phi_C$. □

5.4 Linear algebra

The pairing is positive-definite on homomorphic equivalence classes, and it is a straightforward exercise to show that it is a quadratic form on $\mathrm{Div}(X \times Y)$. Therefore, we may derive an analogue of the Cauchy–Schwartz inequality for correspondences. In the context of vector spaces, equality is attained in the Cauchy–Schwartz inequality precisely when the vectors involved are linearly dependent. The analogous inequality for correspondences provides a useful criterion for $\mathbb{Z}$-linear dependence of induced homomorphisms.

Proposition 5.4.1 (Cauchy–Schwartz inequality for the pairing). *Let C and D be correspondences on $X \times Y$. Then*

$$\langle C, D\rangle^2 \leq \langle C, C\rangle\langle D, D\rangle.$$

Further, equality is attained if and only if the induced homomorphisms ϕ_C and ϕ_D are $\mathbb{Z}$-linearly dependent in $\mathrm{Hom}(J_X, J_Y)$.

Proof. First, we prove the inequality. Since the pairing is positive semi-definite on correspondences,

$$\langle \langle D, D\rangle C - \langle C, D\rangle D, \langle D, D\rangle C - \langle C, D\rangle D\rangle \geq 0;$$

expanding, we have $\langle D,D\rangle^2\langle C,C\rangle - 2\langle C,D\rangle^2\langle D,D\rangle + \langle C,D\rangle^2\langle D,D\rangle \geq 0$, which reduces to $\langle D,D\rangle(\langle C,C\rangle\langle D,D\rangle - \langle C,D\rangle^2) \geq 0$. The factor of $\langle D,D\rangle$ is non-negative, so $\langle C,C\rangle\langle D,D\rangle \geq \langle C,D\rangle^2$, as required. For the second assertion, note that

$$\langle C,C\rangle\langle D,D\rangle - \langle C,D\rangle^2 = \det\begin{pmatrix} \langle C,C\rangle & \langle C,D\rangle \\ \langle D,C\rangle & \langle D,D\rangle \end{pmatrix},$$

which is zero if and only if $(\langle C,C\rangle, \langle C,D\rangle)$ and $(\langle D,C\rangle, \langle D,D\rangle)$ are $\mathbb{Z}$-linearly dependent: that is, when there exist nonzero integers m and n such that $(m\langle C,C\rangle, m\langle C,D\rangle) - (n\langle D,C\rangle, n\langle D,D\rangle) = (0,0)$. This holds precisely when $(\langle mC-nD, C\rangle, \langle mC-nD, D\rangle) = (0,0)$, using the bilinearity of the pairing. Now $\langle mC-nD, mC-nD\rangle = m\langle mC-nD, C\rangle - n\langle mC-nD, D\rangle$, which is $m0 - n0 = 0$ by the above; but $\langle mC-nD, mC-nD\rangle = 0$ precisely when $mC - nD \approx 0$, by Corollary 5.3.7. Therefore $m\phi_C = n\phi_D$. □

Suppose that we have a set of correspondences $\{E_i\}_i$ on $X \times Y$ such that $\{\phi_{E_i}\}_i$ is a $\mathbb{Q}$-basis for $\mathrm{Hom}(J_X, J_Y)$. We may use the pairing to compute a representative for any correspondence C on $X \times Y$ as a linear combination of the E_i. The method is as follows: first, we form the *transfer matrix* $M := (\langle E_i, E_j\rangle)_{(i,j)}$. Note that M is an invertible matrix, because the $e_i = \phi_{E_i}$ are linearly independent by assumption. Next, we set $\underline{s}_C := (\langle C, E_1\rangle, \langle C, E_2\rangle, \ldots, \langle C, E_n\rangle)$. Finally, let $(a_1, \ldots, a_n) := \underline{s}_C M^{-1}$; we have $C \approx \sum_i a_i E_i$.

The transfer matrix may be precomputed and stored for re-use, since it depends only upon the choice of basis. Once the transfer matrix is determined, the induced homomorphism of any correspondence C on $X \times Y$ may be identified with a linear combination of the $\mathbb{Q}$-basis by computing the pairing of C with each of the basis elements. We have derived the following simple algorithm.

Algorithm 5.4.2. Given a correspondence C on $X \times Y$ and a sequence $[E_i : 1 \leq i \leq b]$ of correspondences on $X \times Y$ such that $[\phi_{E_i} : 1 \leq i \leq b]$ is a $\mathbb{Q}$-basis of $\mathrm{Hom}(J_X, J_Y)$, returns a sequence of coefficients $[c_i \in \mathbb{Q} : 1 \leq i \leq b]$ such that $\sum_i c_i E_i$ is homomorphically equivalent to C.

procedure PairingIdentification(C, $[E_i : 1 \leq i \leq b]$)
  for $1 \leq i, j \leq b$ **do**
    $m_{i,j} := \langle E_i, E_j \rangle$;
  end for
  $M := (m_{i,j})$; // Store M for re-use.
  for $0 \leq i \leq b$ **do**
    $s_i := \langle C, E_i \rangle$;
  end for
  $(c_1, \ldots, c_b) := (s_1, \ldots, s_b)M^{-1}$;
  return $[c_1, \ldots, c_b]$;
end procedure

Algorithm 5.4.2 (PairingIdentification) is straight-forward in theory, but presents some computational challenges in practice. Suppose $Y = X$, so $\mathrm{Hom}(J_X, J_Y) = \mathrm{End}(J_X)$. In order to apply Algorithm 5.4.2 we require not only a known $\mathbb{Q}$-basis for $\mathrm{End}(J_X)$, but also a set of representative correspondences for the basis. In many common situations, this is not an obstacle: for example, it may be known that $\mathrm{End}(J_X) \cong \mathbb{Z}$, in which case the diagonal suffices for a $\mathbb{Q}$-basis of $\mathrm{End}(J_X)$. Indeed, this is the case for a generic curve X when the ground field has characteristic zero. In this situation, Algorithm 5.4.2 reduces to

$$\phi_C = [\frac{1}{2g_X}\langle C, \Delta_X \rangle].$$

It may be known that the endomorphism ring $\mathrm{End}(J_X)$ is generated by some automorphisms of X. Computation of the transfer matrix is equivalent to counting fixed points of automorphisms. For example, consider the well-worn example of an elliptic curve with multiplication by $\sqrt{-1}$: take $X : v^2 = u^3 + u$, say. Let α be the automorphism inducing the endomorphism $[\sqrt{-1}]$; then $\mathrm{End}(J_X)$ has a $\mathbb{Q}$-basis $(1, \alpha)$, and we may take $E_1 = \Delta_X$ and $E_2 = \Gamma_\alpha$.

If X is a hyperelliptic curve over a finite field, and if J_X is of ordinary type, then the Frobenius powers $\{\mathcal{F}^{(r)} : 0 \leq r \leq 2g_X - 1\}$ form a $\mathbb{Q}$-basis of $\mathrm{End}^0(J_X)$. In this case, Example 5.3.4 reduces the computation of the transfer matrix M to the computation of traces of Frobenius powers. The traces of the powers of the Frobenius endomorphism of J_X may be derived

from the zeta function of X; efficient algorithms for computing zeta functions are available when the characteristic of k is small (see [32], [24], and [53]). In such cases, we may assume that the transfer matrix can be calculated efficiently with respect to a Frobenius-power basis.

Example 5.4.3. Let $k = \mathbb{F}_5$, and let X be the curve of genus one defined by the Weierstrass equation $X : v^2 = u^3 + u$. We fix a $\mathbb{Q}$-basis $(1, \mathcal{F}^{(1)})$ for $\mathrm{End}(J_X)$; the associated sequence of correspondences is $(\Delta_X, \mathfrak{F}_X)$. The trace of the Frobenius map $\mathcal{F}^{(1)}$ is 2, so the transfer matrix is

$$M = \begin{pmatrix} 2g_X & \mathrm{Tr}(\mathcal{F}^{(1)}) \\ \mathrm{Tr}(\mathcal{F}^{(1)}) & 2g_X \cdot 5 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 10 \end{pmatrix}.$$

Let C be the $(1,1)$-correspondence on $X \times X$ defined by

$$C = V(u_2 + u_1, v_2 - 3v_1)\,.$$

To identify ϕ_C, we must compute $\underline{s}_C$, for which we require the pairings $\langle C, \Delta_X \rangle$ and $\langle C, \mathfrak{F}_X \rangle$. Now, $\langle C, \Delta_X \rangle = 2 - C.\Delta_X$, and direct calculation shows that $C.\Delta_X = 2$; so $\langle C, \Delta_X \rangle = 0$. The intersection number $C.\mathfrak{F}_X$ may also be computed by direct calculation: it is the number of solutions to the system of equations

$$\begin{aligned} u_2 &= -u_1, & v_2 &= -2v_1, \\ u_2 &= u_1^5, & v_2 &= v_1^5, \\ v_1^2 &= u_1^3 + u_1, & v_2^2 &= u_2^3 + u_2, \end{aligned}$$

plus one (to account for the point at infinity). Thus $C.\mathfrak{F}_X = 10$, and $\langle C, \mathfrak{F}_X \rangle = 1 + 5 - 10 = -4$. Thus $\underline{s}_C = (0, -4)$, and $\underline{s}_C M^{-1} = (1/2, -1/2)$. We may conclude that $2C \approx 1 - \mathfrak{F}_X$, and hence that $\phi = \frac{1}{2}(1 - \mathcal{F}^{(1)})$. In particular, the subring $\mathbb{Z}[\phi]$ of $\mathrm{End}(J_X)$ strictly contains $\mathbb{Z}[\mathfrak{F}]$.

Remark 5.4.4. Generally, the Frobenius correspondences are *not* a good choice of basis for the application of this technique. Even if the zeta function of X is known (so the transfer matrix for a Frobenius correspondence basis may be easily computed), computing the pairings for the vector $\underline{s}_C$ can

be prohibitively difficult. If we compute the intersection numbers by direct calculation, the degree of the equations to be solved grows with the $2g_X{}^{\text{th}}$ power of the size of the field. This is impractical when k is a small field, and infeasible when k is only moderate in size.

Chapter 6

Correspondences on hyperelliptic curves

For the remainder of this document, we will turn our attention to correspondences on products of hyperelliptic curves. There are several motivations for studying these correspondences in greater detail. First, the theory of explicit and efficient computation with hyperelliptic Jacobians is very well-developed, in contrast to the theory for general Jacobians. We can use these computational methods to construct efficient and explicit induced homomorphisms of Jacobians for some correspondences, in the form of maps on Mumford ideal class representatives. Second, many examples of hyperelliptic Jacobians known to have nontrivial real and complex multiplication exist in the literature. Finally, in recent times hyperelliptic Jacobians over finite fields have become the subject of great interest in cryptographical research; thus explicit methods for homomorphisms of hyperelliptic Jacobians have potential applications to cryptological problems.

In this chapter, we assume that k is a field of characteristic not two. Recall from Section 2.3 that a curve X of genus at least one is called hyperelliptic if there exists a covering $h_X : X \to \mathbb{P}^1$ of degree two; h_X is called the hyperelliptic cover. Every hyperelliptic curve X over k has an affine plane model of the form

$$X : v^2 = f_X(u),$$

where f_X is a squarefree polynomial of degree $2g_X + 1$ or $2g_X + 2$. We call f_X the hyperelliptic polynomial of X.

Throughout this chapter, let $X : v^2 = f_X(u)$ and $Y : v^2 = f_Y(u)$ be a pair of hyperelliptic curves, with hyperelliptic involutions ι_X and ι_Y and hyperelliptic covers h_X and h_Y, respectively. Our aim in this chapter is to completely describe the correspondences on $X \times Y$ that arise from factors of $f_X(u_1) - f_Y(u_2)$.

6.1 Correspondences on the underlying lines

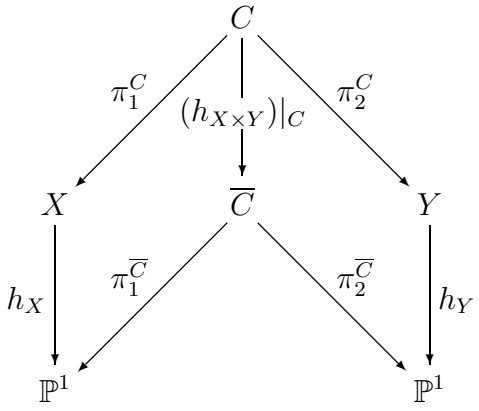
The product $X \times Y$ of hyperelliptic curves X and Y inherits the hyperelliptic involutions of the curves, in the form of the involutions $\mathrm{Id}_X \times \iota_Y$ and $\iota_X \times \mathrm{Id}_Y$. These involutions have the obvious action on correspondences: if C is a correspondence on $X \times Y$, then by Theorem 3.4.3 $(\mathrm{Id}_X \times \iota_Y)_*(C) = \Gamma_{\iota_Y} \circ C$, which is homomorphically equivalent to $-C$. Similarly, $(\iota_X \times \mathrm{Id}_Y)^*(C) \approx -C$.

Definition 6.1.1. If X and Y are hyperelliptic curves, then we define a map $h_{X\times Y}$ by

$$h_{X\times Y} := (h_X \times h_Y) : X \times Y \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1.$$

Note that $h_{X\times Y}$ is the quotient of $X \times Y$ by $\langle (\mathrm{Id}_X \times \iota_Y), (\iota_X \times \mathrm{Id}_Y) \rangle$. If C is a correspondence on $X \times Y$, then we denote the correspondence $(h_{X\times Y})_*(C)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ by $\overline{C}$.

If C is a prime correspondence on $X \times Y$, then $\overline{C}$ is a prime correspondence on $\mathbb{P}^1 \times \mathbb{P}^1$. We have the following diagram of covers of curves:



Observe that $d_1(\overline{C}) = d_1(C)$ and $d_2(\overline{C}) = d_2(C)$; so by the argument of Example 5.1.5 we have $p_a(\overline{C}) = (d_1(C) - 1)(d_2(C) - 1)$. Therefore, we may restate the adjunction formula (Proposition 5.1.4) for hyperelliptic curves as

$$\langle C, C\rangle = 2\big(g_X d_1(C) + g_Y d_2(C) - (p_a(C) - p_a(\overline{C}))\big).$$

Suppose C and D are correspondences on $X \times Y$. Both $\overline{C}$ and $\overline{D}$ are homomorphically trivial, because $\mathrm{Hom}(J_{\mathbb{P}^1}, J_{\mathbb{P}^1}) = 0$. By Proposition 4.1.7, $\overline{C}.\overline{D} = d_1(\overline{C})d_2(\overline{D}) + d_2(\overline{C})d_1(\overline{D}) = d_1(C)d_2(D) + d_2(C)d_1(D)$; so

$$\langle C, D\rangle = \overline{C}.\overline{D} - C.D,$$

where the first intersection number is on $\mathbb{P}^1 \times \mathbb{P}^1$ and the second is on $X \times Y$.

Conversely, we may take a prime correspondence $\overline{C}$ on $\mathbb{P}^1 \times \mathbb{P}^1$ and attempt to lift it to an interesting correspondence C on $X \times Y$. The most obvious correspondence on $X \times Y$ above $\overline{C}$ is the pullback $L = (h_{X\times Y})^*(\overline{C})$. Now L is (by definition) fixed by the involution $\iota_X \times \mathrm{Id}_Y$, so $L = L \circ \Gamma_{\iota_X} \approx -L$; but $\mathrm{Hom}(J_X, J_Y)$ is a torsion-free $\mathbb{Z}$-module, so $L \approx 0$. However, if L is reducible, then it may have components that are not homomorphically trivial.

Example 6.1.2. Let X be a hyperelliptic curve, with an affine plane model $X : v^2 = f_X(u)$. We have

$$\begin{aligned}(h_X \times h_X)^*(\Delta_{\mathbb{P}^1}) &= V(u_2 - u_1)\\ &= V(u_2 - u_1, v_2^2 - v_1^2)\\ &= V(u_2 - u_1, v_2 - v_1) + V(u_2 - u_1, v_2 + v_1)\\ &= \Delta_X + V(u_2 - u_1, v_2 + v_1)\,.\end{aligned}$$

Observe that $V(u_2 - u_1, v_2 + v_1) = (\Gamma_{\iota_Y} \circ \Delta_X) \approx -\Delta_X$.

Of course, not all prime correspondences on $\mathbb{P}^1 \times \mathbb{P}^1$ pull back to reducible correspondences on $X \times Y$.

Example 6.1.3. Let X be the hyperelliptic curve defined by $X : v^2 = u^3+u+1$. The correspondence $\overline{C} = V(u_1 + u_2)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ pulls back via $h_{X\times X}$ to a correspondence $C = V(u_1 + u_2)$ on $X \times X$. Explicit computation shows that C is prime; further, $C \approx 0$ by Lemma 3.3.9.

6.2 Correspondences from $f_X(u_1) - f_Y(u_2)$

Consider the correspondence $\overline{C}$ on $\mathbb{P}^1 \times \mathbb{P}^1$ defined by

$$\overline{C} = V(f_X(u_1) - f_Y(u_2))\,.$$

We have

$$\begin{aligned} h^*_{X\times Y}(\overline{C}) &= V(v_2^2 - v_1^2) \\ &= V(v_2 - v_1) + V(v_2 + v_1)\,. \end{aligned}$$

Both $V(v_2 - v_1)$ and $V(v_2 + v_1)$ are hypersurfaces, and thus homomorphically trivial by Lemma 3.3.9. However, if $f_X(u_1) - f_Y(u_2)$ is a reducible polynomial, then $V(v_2 - v_1)$ and $V(v_2 + v_1)$ are not prime correspondences, and may have components that are not homomorphically trivial. For example, if $F(u_1, u_2)$ is a factor of $f_X(u_1) - f_Y(u_2)$, then

$$C = V(v_2 - v_1, F(u_1, u_2))$$

is a component of $V(v_2 - v_1)$.

In the remainder of this chapter, we will investigate correspondences in the form $V(v_2 - v_1, F(u_1, u_2))$, where F is a factor of $f_X(u_1) - f_Y(u_2)$. We begin by recalling some elementary facts concerning the factors of $f_X(u_1) - f_Y(u_2)$ (cf. Cassou–Noguès & Couveignes [12, §1]), describing the correspondences on $X \times Y$ that arise in each case.

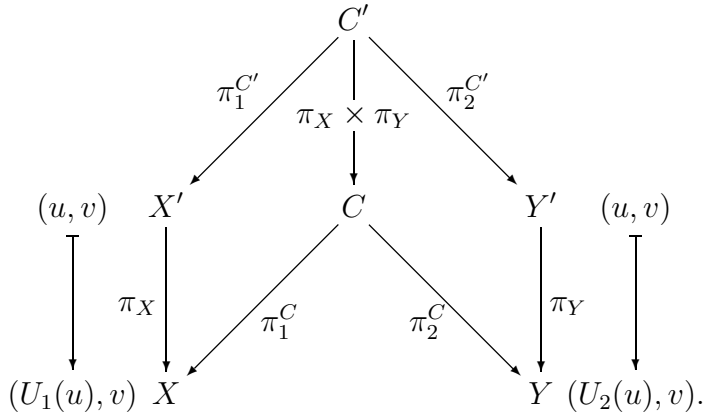
First, suppose $Y = X$. The polynomial $f_X(u_1) - f_X(u_2)$ is always divisible by $u_1 - u_2$. In terms of correspondences on $X \times X$, we have

$$\begin{aligned} & V(v_2 - v_1) \\ = \;& V(v_2 - v_1, u_2 - u_1) + V(v_2 - v_1, (f_X(u_2) - f_X(u_1))/(u_2 - u_1)) \\ = \;& \Delta_X + V(v_2 - v_1, (f_X(u_2) - f_X(u_1))/(u_2 - u_1))\,; \end{aligned}$$

but $V(v_2 - v_1) \approx 0$, so $V(v_2 - v_1, (f_X(u_1) - f_X(u_2))/(u_2 - u_1)) \approx -\Delta_X$.

Next, suppose U_1 and U_2 are polynomials over k of degree at least two. Let X' be the curve defined by $X' : v^2 = f_{X'}(u) = f_X(U_1(u))$, and Y' the curve defined by $Y' : v^2 = f_{Y'}(u) = f_Y(U_2(u))$. As in Lemma 2.3.2, there

are coverings $\pi_X : X' \to X$ and $\pi_Y : Y' \to Y$ defined by $(u, v) \mapsto (U_1(u), v)$ and $(u, v) \mapsto (U_2(u), v)$, respectively. Now, if a polynomial $F(u_1, u_2)$ divides $f_X(u_1) - f_Y(u_2)$, then $F(U_1(u), U_2(u))$ divides $f_{X'}(u_1) - f_{Y'}(u_2)$. Therefore, the correspondence $C = V(v_2 - v_1, F(u_1, u_2))$ on $X \times Y$ automatically lifts to a correspondence $C' = V(v_2 - v_1, F(U_1(u), U_2(u)))$ on $X' \times Y'$. We have the following diagram:



The induced homomorphism $\phi_{C'}$ is the lift of the homomorphism ϕ_C to the isogeny factors of $J_{X'}$ and $J_{Y'}$ associated to J_X and J_Y, respectively.

Finally, let $k(t)$ be a rational function field over k, and suppose that X_t and Y_t are the curves over $k(t)$ defined by $X_t : v^2 = f_{X_t}(u) := f_X(u) + t$ and $Y_t : v^2 = f_{Y_t}(u) := f_Y(u) + t$, respectively. We may regard X_t and Y_t as families of curves over k with parameter t, with $X_0 = X$ and $Y_0 = Y$. Observe that $f_{X_t}(u_1) - f_{Y_t}(u_2) = f_X(u_1) - f_Y(u_2)$; so a polynomial $F(u_1, u_2)$ divides $f_X(u_1) - f_Y(u_2)$ if and only if it divides $f_{X_t}(u_1) - f_{Y_t}(u_2)$. Hence the correspondence $V(v_2 - v_1, F(u_1, u_2))$ on $X \times Y$ lifts automatically to the constant family of correspondences $V(v_2 - v_1, F(u_1, u_2))$ on $X_t \times Y_t$.

Definition 6.2.1. We say that a polynomial f is *decomposable* if there exist polynomials g and h of degree greater than one such that $f = g \circ h$. Otherwise, we say f is *indecomposable*.

By Lemma 2.3.2, if the hyperelliptic polynomial f_X of a hyperelliptic curve X is decomposable, then X covers a hyperelliptic curve of lower genus. In this case, J_X is certainly not simple, because it has factor isogenous to

the Jacobian of the covered curve.

Example 6.2.2. The curve $X : v^2 = u^6 + u^2 - 1$ has a decomposable hyperelliptic polynomial: $f_X = (u^3 + u - 1) \circ u^2$. Hence there is a cover $\pi : X \to E$ defined by $(u, v) \mapsto (u^2, v)$, where E is the curve of genus one defined by $E : v^2 = u^3 + u - 1$. The pullback π^* induces an isogeny from the elliptic curve J_E to a one-dimensional factor of J_X; so J_X is not simple.

The problem of determining when $f_X(u_1) - f_Y(u_2)$ is reducible is completely resolved in the case where both f_X and f_Y are indecomposable. If f_X or f_Y is decomposable, then the problem is unresolved. The following example shows that we cannot simply reduce to the indecomposable case: there may be factors of $f_1(g_1(u_1)) - f_2(g_2(u_2))$ that do not arise from factors of $f_1(u_1) - f_2(u_2)$ (or from factors of $g_1(u_1) - g_2(u_2)$).

Example 6.2.3. Let $F_1 = f_1 \circ g_1$ and $F_2 = f_2 \circ g_2$, where

$$\begin{aligned} f_1 &= u^2 + u + 1, \quad f_2 = u^2 + 3u + 3, \\ g_1 &= u^2 - u + 2, \quad g_2 = u^2 - u + 1. \end{aligned}$$

Observe that $F_1 = F_2$, so $u_1 - u_2$ divides $F_1(u_1) - F_2(u_2)$; but $u_1 - u_2$ divides neither $f_1(u_1) - f_2(u_2)$ nor $g_1(u_1) - g_2(u_2)$.

Definition 6.2.4. We say that polynomials f and g over k are *linearly related* if $f(u) = g(au + b)$ for some a and b in k. We say f and g are *weakly linearly related* if $f(u) = cg(au + b) + d$ for some a, b, c and d in k.

If f_X and f_Y are linearly related, then X and Y are isomorphic: if $f_X(u) = f_Y(au + b)$, then the isomorphism from Y to X is given by $(u, v) \mapsto (au + b)$. If f_X and f_Y are weakly linearly related, then they are not necessarily isomorphic.

Example 6.2.5. Consider the curves of genus one defined by $X : v^2 = u^3+u+1$ and $Y v^2 = u^3+u+2$. We have $f_Y = f_X+1$, so f_X and f_Y are weakly linearly related; but the curves X and Y have different j-invariants, so they cannot be isomorphic.

In fact, if X and Y are hyperelliptic curves such that their hyperelliptic polynomials f_X and f_Y are weakly linearly related, then X and Y are each

isomorphic over a quadratic extension of k to elements of the same rationally parametrised family of curves.

Example 6.2.6. Suppose $X : v^2 = f_X(u)$ and $Y : v^2 = f_X(u)$ are hyperelliptic curves, with $f_X(u) = cf_Y(au + b) + d$. Let X_t be the curve over $k(t)$ defined by $X_t : v^2 = f_X(u) + t$, considered as a family of curves over k, rationally parametrised by t. Clearly $X = X_0$; further, there is an isomorphism $i : Y \to X_{d/c}$, defined over $k(\sqrt{c})$ by $i(u, v) = (au + b, (1/\sqrt{c})v)$.

If X and Y are not isomorphic, then the work of Cassou–Noguès and Couveignes [12] shows that the pairs of indecomposable polynomials f_X and f_Y such that $f_X(u_1) - f_Y(u_2)$ is reducible form a finite set (up to weak linear relation). We will investigate the correspondences arising from factors of these polynomials below. First, in order to identify the homomorphisms induced by these correspondences, we will derive an algorithm for computing their differential matrices.

Suppose that we are given a correspondence $C = V(v_2 - v_1, F(u_1, u_2))$ on $X \times Y$; without loss of generality, we may assume C is prime. For each $1 \leq i \leq g_X$, let t_i be the image of u_1^i under the trace map from $\mathcal{O}_C$ to $\mathcal{O}_Y$. Note that if $e_1, \ldots, e_{d_2(C)}$ are the solutions to the equation $F(x, u) = 0$ in x, then $t_n = \sum_j e_j^n$, the n^{th} power-sum symmetric polynomial in the e_i. If s_m denotes the m^{th} elementary symmetric polynomial in the e_i (which, up to sign, is the coefficient of u_1^m in F), then we may invert the standard recurrence

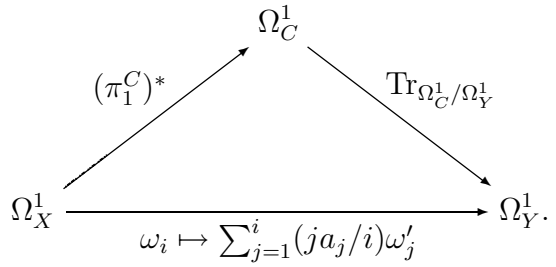
$$ns_n = \sum_{i=1}^{n} (-1)^{i+1} s_{n-i} t_i$$

to compute each of the required traces t_i.

Fix bases $\{\omega_i : 1 \leq i \leq g_X\}$ for Ω^1_X and $\{\omega'_j : 1 \leq i \leq g_Y\}$ for Ω^1_Y, with $\omega_i = (u^{i-1}/v)du$ on X and $\omega'_j = (u^{j-1}/v)du$ on Y. To determine M_C with respect to these bases, we must express $\mathrm{Tr}_{\Omega^1_C/\Omega^1_Y}((\pi_1^C)^*(\omega_i))$ in terms of the ω'_j for each of the ω_i. Now, $(\pi_1^C)^*(\omega_i) = (u_1^{i-1}/v_1)du_1$, which is equal to $1/(iv_2)d(u_1^i)$; the trace of this differential to Ω^1_Y is $1/(iv')dt_i$.

Now, if $t_i = \sum_{j=0}^{i} a_j u'^j$ then $dt_i = \sum_{j=1}^{i} j a_j \omega'_j$, and the homomorphism

on differentials induced by C is



Hence the (i,j)-th entry of M_C is $(j/i)a_j$. We have thus derived the following algorithm for computing the differential matrix of C.

Algorithm 6.2.7. Computes the differential matrix M_C of a prime correspondence $C = V(v_2 - v_1, F(u_1, u_2))$ on $X \times Y$.

function DIFFERENTIALMATRIX(C)
  $d := \deg F$;
  $l :=$ COEFFICIENT(F, u_1^d); // l is the leading coefficient.
  $s_0 := 1$;
  for i in $[1, \ldots, g_X]$ **do**
    if $i \leq d$ **then**
      $s_i := (-1)^i$COEFFICIENT$(F, u_1^{d-i})/l$;
    else
      $s_i := 0$;
    end if
    $t_i := (-1)^{i+1}(is_i + \sum_{k=1}^{i-1}(-1)^k s_{i-k}t_k)$;
    for j in $[1, \ldots, g_Y]$ **do**
      $m_{i,j} := (j/i)$COEFFICIENT(t_i, u_2^j);
    end for
  end for
  $M_C := (m_{i,j})$;
  return M_C;
end function

6.3 Endomorphisms from $f_X(u_1) - f_X(u_2)$

Suppose $X : v^2 = f_X(u)$ is a hyperelliptic curve. In the previous section, we saw that the correspondence $V(v_2 - v_1)$ on $X \times X$ is reducible:

$$V(v_2 - v_1) = \Delta_X + V(v_2 - v_1, (f_X(u_1) - f_X(u_2))/(u_1 - u_2)).$$

The correspondence $V(v_2 - v_1, (f_X(u_1) - f_X(u_2))/(u_1 - u_2))$ is reducible if $(f_X(u_1) - f_X(u_2))/(u_1 - u_2)$ is reducible. The conditions required of f_X for this to happen are well-known (see Fried [21] and in Lidl et. al. [42, §6.4]); we will interpret these results in terms of correspondences.

Definition 6.3.1. We say a nonconstant polynomial f over k is *tame* if the ramification of the covering $\mathbb{P}^1 \to \mathbb{P}^1$ defined by $u \mapsto f(u)$ is tame.

A polynomial f is tame if the characteristic of k divides neither the degree of f nor the multiplicity of any zero of $f(x) - c$ in $\overline{k}$ for all c in $\overline{k}$. If the characteristic of k is zero, then every polynomial over k is tame. If k is a field of positive characteristic p, then we may be sure that a polynomial is tame if its degree is less than p.

The following lemma completely describes the indecomposable tame polynomials f such that $f(u_1) - f(u_2)$ has nontrivial factors other than $u_1 - u_2$ and $(f(u_1) - f(u_2))/(u_1 - u_2)$. It turns out that every such polynomial is weakly linearly related to a Dickson polynomial (see Definition 2.5.1).

Lemma 6.3.2. *Let f be a tame, indecomposable polynomial over k of degree $n > 1$, such that $(f(u_1) - f(u_2))/(u_1 - u_2)$ is not absolutely irreducible. Then n is an odd prime, and f is weakly linearly related to the Dickson polynomial $D_n(u, a)$ for some a in k. Further, if $n = 3$, then $a = 0$.*

Proof. See Lidl et. al. [42, Corollary 6.18]. □

Theorem 6.3.3. *Let X be a hyperelliptic curve over k such that f_X is indecomposable and tame. If $V(v_2 - v_1) - \Delta_X$ is not a prime correspondence, then* $\deg f_X$ *is prime, and X has a model*

$$X : v^2 = cD_n(u + b, a) + d,$$

for some a, b, c and d in k, with c and d not zero. Further, if $g_X = 1$, then $n = 3$ and $a = 0$.

Proof. The assertions follow directly from Lemma 6.3.2. □

Example 6.3.4. Suppose X is a curve of genus one such that the correspondence $V(v_2 - v_1) - \Delta_X$ on $X \times X$ is not prime. By Theorem 6.3.3, f_X is weakly linearly related to $D_3(u, 0)$; but $D_3(u, 0) = u^3$ by Lemma 2.5.2, so X has a model

$$X : v^2 = f_X(u) = c(u + b)^3 + d.$$

If ζ_3 is a cube root of unity over k, then $V(v_2 - v_1) = C_0 + C_1 + C_2$, where

$$C_i = V\big(v_2 - v_1, u_2 + b - \zeta_3^i(u_1 + b)\big)$$

(note that $C_0 = \Delta_X$). Observe that while C_1 and C_2 are defined only over $k(\zeta_3)$, the correspondence $C_1 + C_2$ is k-rational. It is easily verified that $C_1 \circ C_1 = C_2$ and $C_1 \circ C_1 \circ C_1 = C_0 = \Delta_X$; therefore $\mathrm{End}(J_X)$ has a subring $\mathbb{Z}[\phi_{C_1}]$ isomorphic to $\mathbb{Z}[\omega]$, where ω is a primitive cube root of unity over $\mathbb{Q}$.

We will completely describe the endomorphism rings of the Jacobians of the curves $v^2 = cD_n(u + b, a) + d$ of Theorem 6.3.3. For each curve, we construct correspondences inducing generators of the endomorphism rings, and give explicit realisations of the induced endomorphisms in terms of maps on Mumford ideal class representatives. We will treat the case $a = 0$ in the following section; we will return to the case $a \neq 0$ in the next chapter.

6.4 Cyclotomic CM: the curve $v^2 = u^p + 1$

Let us consider the curves arising in Theorem 6.3.3 where the parameter of the Dickson polynomial is zero: that is, the curves defined by models

$$v^2 = cD_p(au + b, 0) + d$$

where p is a prime and a, b, c and d are elements of k (if the characteristic of k is not zero, then we assume that $p >$ char k). We will see that every

such curve has complex multiplication by the ring of integers of a cyclotomic field; further, we will give an explicit construction of correspondences whose induced homomorphisms are generators for the endomorphism ring.

Suppose X is a hyperelliptic curve with a model

$$X : v^2 = f_X(u) = cD_p(au + b, 0) + d.$$

Property (8) of Lemma 2.5.2 tells us that $D_p(x, 0) = x^p$, so in fact $f_X(u) = c(au + b)^p + d$, and the map $(u, v) \mapsto ((d/c)^{1/p}(au + b), d^{-1/2}v)$ therefore defines an isomorphism from X to the curve

$$Y_p : v^2 = f_{Y_p}(u) = u^p + 1.$$

For simplicity, we restrict our investigation to Y_p; the isomorphism above renders the application of our results to X an exercise in elementary algebra. The issue of point counting on the curves Y_p is addressed by Buhler and Koblitz in [7].

Let ζ_p be a p^{th} root of unity over k. The curve Y_p has an automorphism ζ of order p, defined over $k(\zeta_p)$ by

$$\zeta(u, v) := (\zeta_p u, v).$$

The minimal polynomial of ζ is the p^{th} cyclotomic polynomial, $\Phi_p(x) = (x^p-1)/(x-1)$, so the subring $\mathbb{Z}[\zeta]$ of $\text{End}(J_{Y_p})$ is isomorphic to $\mathbb{Z}[x]/(\Phi_p(x))$. However, $\mathbb{Z}[x]/(\Phi_p(x))$ is the ring of integers of the p^{th} cyclotomic field, so $\mathbb{Z}[\zeta]$ is a maximal subring of $\text{End}(J_{Y_p})$ — that is, $\text{End}(J_{Y_p}) \cong \mathbb{Z}[\zeta]$.

Over $k(\zeta_p)$, the polynomial $f_{Y_p}(u_1) - f_{Y_p}(u_2)$ splits completely:

$$\begin{aligned} f_{Y_p}(u_1) - f_{Y_p}(u_2) &= u_1^p - u_2^p \\ &= \textstyle\prod_{i=0}^{p-1}(u_2 - \zeta_p^i u_1). \end{aligned}$$

Therefore, the correspondence $V(v_2 - v_1)$ on $Y_p \times Y_p$ decomposes into a sum

$V(v_2 - v_1) = \sum_{i=0}^{p-1} C_{p,i}$, where

$$C_{p,i} = V\big(v_2 - v_1, u_2 - \zeta_p^i u_1\big)\,.$$

It is easy to see that $C_{p,i} = \Gamma_{\zeta^i}$; hence $C_{p,0} = \Delta_{Y_p}$, and $C_{p,i}$ is the i-fold composition of $C_{p,1} = \Gamma_\zeta$ with itself. The correspondences $C_{p,i}$ therefore induce a $\mathbb{Z}$-basis $\{\zeta^i : 0 \le i < p\}$ of $\mathrm{End}(J_X)$, and so every endomorphism of J_{Y_p} is induced by a $\mathbb{Z}$-linear combination of the $C_{p,i}$.

It is straightforward to give an effective realisation of the endomorphism $\phi_{C_{p,i}}$ as a map on Mumford ideal class representatives: we have

$$\phi_{C_{p,i}}([(a(u), v - b(u))]) = \big[(\zeta^{i \deg a} a(\zeta^{-i}u), v - b(\zeta^{-i}u))\big].$$

Evaluation of this map on ideals is highly efficient — after all, it is nothing more than a direct linear substitution in $k[u]$. These effective endomorphisms $\phi_{C_{p,i}}$ may not appear very interesting at first; however, they do have a useful application when k is a finite field.

Suppose k is a finite field, and that the group structure of $J_{Y_p}(k)$ is cyclic of prime order n. The endomorphism $\phi_{C_{p,1}}$ must act as multiplication by some integer c on $J_{Y_p}(k)$; the integer c will be a p^{th} root of unity modulo n. Further, the endomorphism $\phi_{C_{p,i}}$ acts as $[c^i \pmod n]$ on $J_{Y_p}(k)$ for each $1 \le i \le p$. Therefore our effective endomorphisms actually give highly efficient means of evaluating the integer multiplications $[c^i \pmod n]$ on $J_{Y_p}(k)$, which may be used to greatly speed up arithmetic on the group of rational points of J_{Y_p}. The genus of Y_p is $(p-1)/2$, so each point P of J_{Y_p} has a reduced representative

$$P = \left[\left(u^d + \sum_{j=0}^{d-1} a_j u^j, v - \sum_{j=0}^{d-1} b_j u^j\right)\right],$$

with $0 \le d \le (p-1)/2$. The image of P under ϕ_{C_i} is

$$\phi_{C_i}(P) = \left[\left(u^d + \sum_{j=0}^{d-1} \zeta_p^{i(d-j)} a_j u^j, v - \sum_{j=0}^{d-1} \zeta_p^{i(d-j)} b_j u^j\right)\right];$$

note that this representative is already reduced, so no further reduction is

required. Thus if we precompute the values ζ_p^{ij} for $0 \leq j < (p-1)/2$, then we may evaluate $\phi_{C_i}(P)$ at a cost of at most $2(((p-1)/2)-1) = p-3$ field multiplications in k. This makes ϕ_{C_i} particularly suited for use in GLV techniques (see §2.4).

Example 6.4.1. Suppose k is a finite field of characteristic 29, and let t be a free parameter. Let X_t be the hyperelliptic curve of genus three over $k(t)$ defined by the affine plane model

$$X_t : v^2 = u^7 + t.$$

Observe that 20 is a seventh root of unity in k, and that the inverse of 20 is 16. As in the above discussion, the correspondence $V(v_2 - v_1)$ decomposes over $k(t)$ into a sum $V(v_2 - v_1) = \sum_{i=0}^{6} C_i$, where

$$C_i = V\big(v_2 - v_1, u_2 - 20^i u_1\big)\,.$$

We may identify the endomorphism ϕ_{C_i} with multiplication-by-ζ_7^i, where ζ_7 is a seventh root of unity over $\mathbb{Q}$. In particular, the correspondence

$$C_1 = V(v_2 - v_1, u_2 - 20u_1)$$

induces multiplication-by-ζ_7 on J_Y; the map

$$[(a(u), v - b(u))] \longmapsto \big[\big(20^{\deg a} a(16u), v - b(16u)\big)\big]$$

gives an explicit realisation of ϕ_{C_1} on Mumford ideal class representatives.

Example 6.4.2. We may use the explicit map on Mumford ideal class representatives of Example 6.4.1 to give an example of an efficient integer multiplication. Let $k = \mathbb{F}_{29^{11}}$, and consider the curve

$$X_{10} : v^2 = u^7 + 10$$

over k. As in Example 6.4.1, for each $0 \leq i \leq 6$ we have a correspondence

$$C_i = V\big(v_2 - v_1, u_2 - 16^i u_1\big)$$

on $X_{10} \times X_{10}$, inducing an explicit endomorphism

$$\phi_{C_i} : [(a(u), v - b(u))] \longmapsto \big[\big(20^{i \deg a} a(16^i u), v - b(16^i u)\big)\big].$$

Each endomorphism ϕ_{C_i} acts as multiplication-by-ζ_7^i on $J_{X_{10}}$, where ζ_7 is a seventh root of unity over $\mathbb{Q}$. Now, $\#J(k) = 25243 \cdot N$, where

$$N = 71943732797984772333979215054479116158556553$$

is prime. Let $G = [25243]_{J_{X_{10}}} J_{X_{10}}$; then G is a cyclic subgroup of $J_{X_{10}}$ of prime order N. The roots of $u^7 - 1$ in $\mathbb{Z}/N\mathbb{Z}$ are

$$\begin{aligned}
&1,\\
&23519305668795492023698995177489738656048400,\\
&26168451107185642403155464096384433792544313,\\
&31794316175824031036315847293785691884863803,\\
&67085897870801989693884158740970392233786916,\\
&67957780198888565596300220736534264730743643, \text{ and}\\
&71249180170443368582562174172751943336239136.
\end{aligned}$$

Each ϕ_{C_i} must act as multiplication by one of these roots on G. Explicit calculation shows that

$$\begin{aligned}
\phi_{C_0}|_G &= [1]_G,\\
\phi_{C_1}|_G &= [71249180170443368582562174172751943336239136]_G,\\
\phi_{C_2}|_G &= [67957780198888565596300220736534264730743643]_G,\\
\phi_{C_3}|_G &= [26168451107185642403155464096384433792544313]_G,\\
\phi_{C_4}|_G &= [23519305668795492023698995177489738656048400]_G,\\
\phi_{C_5}|_G &= [67085897870801989693884158740970392233786916]_G, \text{ and}\\
\phi_{C_6}|_G &= [31794316175824031036315847293785691884863803]_G.
\end{aligned}$$

Each endomorphism ϕ_{C_i} may be evaluated at any point of $J_{X_{10}}$ at a cost of at most five multiplications in k. This is essentially negligible, and is clearly much faster than the many point doublings required in the equivalent traditional integer multiplication.

6.5 Isogenies from $f_X(u_1) - f_Y(u_2)$

In [12], Cassou–Noguès and Couveignes describe the pairs of polynomials f_X and f_Y that are not linearly related, such that $f_X(u_1) - f_Y(u_2)$ has a nontrivial factor (if f_X and f_Y are linearly related, then we may transform to the case $f_X = f_Y$ and apply the results of the previous section). Their work completes that of Cassels [10], who showed that the problem is essentially determined by the monodromy group of the surface defined by the equations $z = f_X(x)$, $z = f_Y(y)$. Using the classification of finite simple groups[1], Cassou–Noguès and Couveignes prove the following theorem.

Theorem 6.5.1 (Cassou–Noguès & Couveignes). *Let f_X and f_Y be a pair of non-constant, indecomposable polynomials over $\mathbb{C}$ that are not linearly related, such that $f_X(u_1) - f_Y(u_2)$ is reducible. Then $\deg f_X = \deg f_Y$, and $\deg f_X$ is 7, 11, 13, 15, 21, or 31. Further, f_X is weakly linearly related to a polynomial g defined over a quadratic imaginary extension K of a real number field k', and f_Y is weakly linearly related to the Galois conjugate of g over K_0. If $\deg f_X$ is 11, 21 or 31, then g is unique; if $\deg f_X$ is 7, 13 or 15, then g is an element of a one-dimensional family of polynomials.*

Proof. See [12, Théorème 1]. □

Theorem 6.5.1 holds over the field of complex numbers, and thus for polynomials over any number field k, although we must then allow the coefficients in the weak linear relations to be taken from a finite extension of k. The polynomials for degrees seven and eleven were originally discovered by Birch (see [10]); Kux [36, §4.1] interprets these polynomials in terms of

[1] Sometimes called the "enormous theorem", the classification of finite simple groups is well beyond the scope of this discussion. See [25, 26, 60] for an introduction to the theory.

correspondences of curves over $\mathbb{C}$. We will describe each of the polynomials listed in [12, §5], retaining as much generality as possible with respect to the ground field k. In each case, we give an interpretation of the results in terms of correspondences, and describe the induced homomorphisms. We may completely describe all correspondences arising from factors of $f_X(u_1) - f_Y(u_2)$, where X is not isomorphic to Y, when k embeds in the complex field (in particular, when k is a number field). The resulting curves also reduce to interesting correspondences over the finite fields where f_X and f_Y have good reduction.

Genus three

Suppose X and Y are curves of genus three, with $\deg f_X = \deg f_Y = 7$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $K = k(a)$, where a is a root of the polynomial $u^2 + u + 2$ over k; let σ be the nontrivial element of the Galois group of K/k, and let $\bar{a} = a^\sigma$. Let t be a free parameter. According to [12, §5.1], f_X is weakly linearly related to a polynomial in the rationally parametrised family

$$\begin{aligned} g = \frac{1}{7}u^7 + (1+a)tu^5 + (1+a)tu^4 - (3-2a)t^2u^3 \\ -2(1-2a)t^2u^2 - \frac{1}{28}(5+3a)(28t-2-11a)t^2u - (1+a)t^3 \end{aligned}$$

defined over $K(t)$, and f_Y is weakly linearly related to the Galois conjugate g^σ.

Suppose $f_X = g$ and $f_Y = g^\sigma$. The polynomial $f_X(u_1) - f_Y(u_2)$ has an absolutely irreducible factor

$$F_3 = u_1^3 - u_2^3 - \bar{a}u_1^2u_2 + au_1u_2^2 + (5+3a)tu_1 - (5+3\bar{a})tu_2 + (a-\bar{a})t;$$

the cofactor of F_3 is also absolutely irreducible. We therefore have a $(3,3)$-correspondence $C_3 = V(v_2 - v_1, F_3)$ on $X \times Y$. Computing differential ma-

trices with Algorithm 6.2.7 (DifferentialMatrix), we see that

$$M_{C_3} = \begin{pmatrix} \bar{a} & 0 & 0 \\ 0 & \bar{a} & 0 \\ (1+2a)t & 0 & a \end{pmatrix}$$

and $M_{C_3{}^t} = M_{C_3}^{\sigma}$; hence $M_{C_3} M_{C_3{}^t} = 2I_3$. Thus $\mathcal{T}_0(\phi_{C_3}^{\dagger} \circ \phi_{C_3}) = 2$, and we may conclude that $\phi_{C_3}^{\dagger} \circ \phi_{C_3} = [2]_{J_X}$ — that is, ϕ_{C_3} splits multiplication by two on J_X.

Genus five

Suppose X and Y are curves of genus five, with $\deg f_X = \deg f_Y = 11$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $K = k(a)$, where a is a root of the polynomial $u^2 + u + 3$ over k; let σ be the nontrivial element of the Galois group of K/k, and let $\bar{a} = a^{\sigma}$. According to [12, §5.2], f_X is weakly linearly related to the polynomial

$$\begin{aligned} g_5 = \frac{1}{11}u^{11} + \bar{a}u^9 + 2u^8 + 3(a-3)u^7 + 16\bar{a}u^6 + 3(7a+12)u^5 \\ + 30(a-3)u^4 - 63au^3 + 20(5a+6)u^2 + 3(8a-39)u + 18\bar{a} \end{aligned}$$

over K, and f_Y is weakly linearly related to the Galois conjugate g_5^{σ} of g_5. We find that the irreducible polynomial

$$\begin{aligned} F_5 = {} & u_1^5 - u_2^5 - \bar{a}u_1^4u_2 + au_1u_2^4 \\ & - u_1^3u_2^2 + u_1^2u_2^3 - 2(2a+1)u_1^3 + 2(2\bar{a}+1)u_2^3 \\ & - (a-5)u_1^2u_2 + (\bar{a}-5)u_1u_2^2 + 2(a+6)u_1^2 - 2(\bar{a}+6)u_2^2 \\ & + 6(2a+1)u_1u_2 - (8a+15)u_1 + (8\bar{a}+15)u_2 - 6(2a+1) \end{aligned}$$

divides $g_5(u_1) - g_5^{\sigma}(u_2)$. If we suppose $f_X = g_5$ and $f_Y = g_5^{\sigma}$, then we have a nontrivial $(5,5)$-correspondence $C_5 = V(v_2 - v_1, F_5)$ on $X \times Y$. Computing differential matrices using Algorithm 6.2.7 (DifferentialMatrix), we see

that

$$M_{C_5} = \begin{pmatrix} \bar{a} & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 \\ \bar{a}+6 & 0 & \bar{a} & 0 & 0 \\ 0 & 0 & 0 & \bar{a} & 0 \\ 15a+24 & 8\bar{a}+4 & 3\bar{a}+18 & 0 & \bar{a} \end{pmatrix}$$

and $M_{C_5{}^t} = M_{C_5}^{\sigma}$, so $M_{C_5{}^t} M_{C_5} = 3I_5$. We conclude that $\phi_{C_5}^{\dagger} \circ \phi_{C_5} = [3]_{J_X}$ — that is, that ϕ_{C_5} splits $[3]_{J_X}$.

Remark 6.5.2. In the remaining examples, we will not give all the entries of the differential matrices. The reader may readily recompute the matrices if required, using Algorithm 6.2.7.

Genus six

Suppose X and Y are curves of genus six, with $\deg f_X = \deg f_Y = 13$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $k' = k(b)$, where b is a root of the polynomial $u^2 - 5u + 3$ over k, and let $K = k'(a)$, where a is a root of the polynomial $u^2 + (b-2)u + b$ over k'. Let σ be the nontrivial element of the Galois group of K/k', and let $\bar{a} = a^{\sigma}$. Let t be a free parameter. By [12, §5.3], f_X is weakly linearly related to a polynomial in the rationally parametrised family g_6 over $K(t)$, described by Table 6.1 below, and f_Y is weakly linearly related to the Galois conjugate g_6^{σ}.

Suppose $f_X = g_6$ and $f_Y = g_6^{\sigma}$. The polynomial $f_X(u_1) - f_Y(u_2)$ has an absolutely irreducible factor

$$\begin{aligned} F_6 = {} & u_1^4 + u_2^4 \\ & - ((b-4)a + 2)u_1^3 u_2 - ((b-4)\bar{a} + 2)u_1 u_2^3 \\ & + (b-3)u_1^2 u_2^2 \\ & + 3((17b-73)a - 2(6b-25))tu_1^2 + 3((17b-73)\bar{a} - 2(6b-25))tu_2^2 \\ & - 9(3b-14)tu_1 u_2 \\ & + 3((5b-22)a - 9b + 38)tu_1 + 3((5b-22)\bar{a} - 9b + 38)tu_2 \\ & + 12(47b-202)t^2; \end{aligned}$$

the cofactor of F_6 is also absolutely irreducible. Hence we have a nontrivial

Table 6.1: The polynomial g_6 for genus six

d	Coefficient of u^d in $g_6(u)$
13	1
12	0
11	$39((3b-13)a-2b+8))t$
10	$39((3b-13)a-4b+17)t$
9	$39((-58b+251)a+173b-739)t^2$
8	$234((90b-387)a-2b+9)t^2$
7	$117\left(\begin{array}{l}((-3309b+14235)a+1332b-5739)t\\ +((182b-783)a-145b+624)\end{array}\right)t^2$
6	$351((-5479b+23574)a+5037b-21674)t^3$
5	$351\left(\begin{array}{l}((18653b-80257)a-21681b+93294)t\\ +((-668b+2874)a+4442b-19113)\end{array}\right)t^3$
4	$351\left(\begin{array}{l}((-41886b+180228)a-61944b+266532)t\\ +((2652b-11411)a-1397b+6011)\end{array}\right)t^3$
3	$1053\left(\begin{array}{l}((22561b-97076)a+32325b-139089)t\\ +((-98835b+425265)a+42632b-183436)\end{array}\right)t^4$
2	$1053\left(\begin{array}{l}((619226b-2664391)a-390378b+1679709)t\\ +((-41278b+177610)a+46232b-198926)\end{array}\right)t^4$
1	$351\left(\begin{array}{l}((-1006352b+4330108)a+412548b-1775100)t^2\\ +((2726523b-11731617)a-3587121b+15434577)t\\ +((28536b-122784)a-11256b+48432)\end{array}\right)t^4$
0	$4212\left(\begin{array}{l}((-149259b+642228)a-149259b)t\\ +((-40928b+176104)a-40928b)\end{array}\right)t^5$

$(4,4)$-correspondence $C_6 = V(v_2 - v_1, F_6)$ on $X \times Y$. Computing differential matrices using Algorithm 6.2.7 (DifferentialMatrix), we see that M_{C_6} is a lower-triangular matrix, with diagonal entries

$$(b-4)a+2,\ a+1,\ (b-4)a+2,\ (-b+4)a+b-3,\ a+1,\ a+1.$$

The differential matrix of the transpose is $M_{C_6{}^t} = M_{C_6}^{\sigma}$, and we find that $M_{C_6{}^t} M_{C_6} = 3I_6$. We conclude that $\phi_{C_6}^{\dagger} \circ \phi_{C_6} = [3]_{J_X}$ — that is, that ϕ_{C_6} splits $[3]_{J_X}$.

Genus seven

Suppose X and Y are curves of genus seven, with $\deg f_X = \deg f_Y = 15$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $K = k(a)$, where a is a root of the polynomial $u^2 - u + 4$; let σ be the nontrivial element of the Galois group of K/k, and let $\bar{a} = a^{\sigma}$. According to [12, §5.4], f_X is weakly linearly related to a polynomial in the rationally parametrised family g_7 over K (with parameter t) described in Table 6.2 below, and f_Y is weakly linearly related to the Galois conjugate g^{σ} of g_7.

Suppose $f_X = g_7$ and $f_Y = g_7^{\sigma}$. The polynomial $f_X(u_1) - f_Y(u_2)$ has an absolutely irreducible factor

$$\begin{aligned}
F_7 = {} & u_1^7 + u_2^7 + \bar{a}u_1^6u_2 + au_1u_2^6 - 2u_1^5u_2^2 - 2u_1^2u_2^5 \\
& + (a+1)u_1^4u_2^3 + (\bar{a}+1)u_1^3u_2^4 + (7a-3)tu_1^5 + (7\bar{a}-3)tu_2^5 \\
& + 22t(u_1^4u_2 + u_1u_2^4) - (10a+2)tu_1^3u_2^2 - (10\bar{a}+2)tu_1^2u_2^3 \\
& + 5((a+13)tu_1^4 + (\bar{a}+13)tu_2^4) \\
& + 10((5\bar{a}+2)tu_1^3u_2 + (5a+2)tu_1u_2^3) - 90tu_1^2u_2^2 \\
& + 3((3a-23)t^2u_1^3 + (3\bar{a}-23)t^2u_2^3) \\
& + 3((13a+11)t^2u_1^2u_2 + (13\bar{a}+11)t^2u_1u_2^2) \\
& + 30((7a-5)t^2u_1^2 + (7\bar{a}-5)t^2u_2^2) + 450t^2u_1u_2 \\
& - 9(((7a+5)t^3 - 25(a+4)t^2)u_1 + ((7\bar{a}+5)t^3 - 25(\bar{a}+4)t^2)u_2) \\
& - 375t^3;
\end{aligned}$$

the cofactor of F_7 is also absolutely irreducible. Hence, there is a nontrivial

Table 6.2: The polynomial g_7 for genus seven

d	Coefficient of u^d in $g_7(u)$
15	1
14	0
13	$15\bar{a}t$
12	$15(a+7)t$
11	$-15(5a+21)t^2$
10	$30(37a-71)t^2$
9	$-5(261a-349)\left(t+\frac{45(3135a-2428)}{151598}\right)t^2$
8	$-(649a+703)t^3$
7	$45(46a+239)\left(t+\frac{20(9913a-23128)}{76579}\right)t^3$
6	$-60(548a-1939)\left(t+\frac{5(21273a-5284)}{259891}\right)t^3$
5	$9(1945a-1581)\left(t+\frac{25(587433a-4548020)}{7278308}\right)t^4$
4	$45(3233a+2051)\left(t+\frac{25(53589a-86500)}{877444}\right)t^4$
3	$405(9a-133)\left(t^2-\frac{5(4051a+31524)}{6306}t-\frac{125(2563a-188)}{50448}\right)t^4$
2	$270(403a-1559)\left(t+\frac{(9165a-39620)}{5108}\right)t^5$
1	$-2025(7a+5)\left(t+\frac{25}{4}(a+4\bar{a})\right)\left(t-\frac{1}{4}(a-4\bar{a})\right)t^5$
0	$10125(a-8)(t-16)t^6$

$(7,7)$-correspondence $C_7 = V(v_2 - v_1, F_7)$ on $X \times Y$. Computing differential matrices with Algorithm 6.2.7 (DifferentialMatrix), we see that M_{C_7} is a lower-triangular matrix, with diagonal entries

$$-\frac{4}{a},\ \frac{4}{a},\ -2,\ \frac{4}{a},\ 2,\ 2,\ -a.$$

The differential matrix of the transpose is $M_{C_7{}^t} = M_{C_7}^{\sigma}$, and we find that $M_{C_7{}^t} M_{C_7} = 4I_7$. We conclude that $\phi_{C_7}^{\dagger} \circ \phi_{C_7} = [4]_{J_X}$ — that is, that ϕ_{C_7} splits $[4]_{J_X}$.

Genus ten

Suppose X and Y are curves of genus ten, with $\deg f_X = \deg f_Y = 21$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $K = k(a)$, where a is a root of the polynomial $u^2 - u + 2$. Let σ be the nontrivial element of the Galois group of K/k, and let $\bar{a} = a^{\sigma}$. According to [12, §5.5], f_X is weakly linearly related to the polynomial g_{10} over K described by Table 6.3 below, and f_Y is weakly linearly related to the Galois conjugate g_{10}^{σ} of g_{10}.

Suppose $f_X = g_{10}$ and $f_Y = g_{10}^{\sigma}$. The polynomial $f_X(u_1) - f_X(u_2)$ is divisible by the absolutely irreducible polynomial

$$\begin{aligned} F_{10} = {} & (u_1^5 - u_2^5) + (a+1)u_1^4 u_2 - (\bar{a}+1)u_1 u_2^4 + 2a u_1^3 u_2^2 - 2\bar{a} u_1^2 u_2^3 \\ & + (7a + 9/2\bar{a})u_1^3 - (9/2a + 7\bar{a})u_2^3 + (6a - 2\bar{a})u_1^2 u_2 + (2a - 6\bar{a})u_1 u_2^2 \\ & + (3a + 1/2\bar{a})u_1^2 - (1/2a + 3\bar{a})u_2^2 + (2a - 2\bar{a})u_1 u_2 \\ & + (81/8a + 55/16\bar{a})u_1 - (55/16a + 81/8\bar{a})u_2 \\ & + 17/8(a - \bar{a}); \end{aligned}$$

the cofactor of F_{10} is also absolutely irreducible. Hence, there is a nontrivial $(5,5)$-correspondence $C_{10} = V(v_2 - v_1, F_{10})$ on $X \times Y$. Computing differential matrices using Algorithm 6.2.7, we see that $M_{C_{10}}$ is a lower-triangular matrix, with diagonal entries

$$-a-1,\ -(a+1),\ a+1,\ -(a+1),\ a-2,\ a+1,\ 2,\ -(a+1),\ -(a-2),\ a-2.$$

The differential matrix of the transpose is $M_{C_{10}{}^t} = M_{C_{10}}^{\sigma}$, and we find that

Table 6.3: The polynomial g_{10} for genus ten

d	Coefficient of u^d in $g_{10}(u)$
21	1
20	0
19	$21/2(2a+\bar{a})$
18	$21/2(2a+\bar{a})$
17	$21/2^4(70a-41\bar{a})$
16	$21/2^3(74a-31\bar{a})$
15	$-7/2^3(317a+1153\bar{a})$
14	$-7/2^3(707a+2735\bar{a})$
13	$-105/2^7(4921a+6907\bar{a})$
12	$-273/2^5(1267a+1553\bar{a})$
11	$-7/2^8(714488a+655555\bar{a})$
10	$-231/2^8(43352a+29639\bar{a})$
9	$-7/2^{11}(14566036a+7465459\bar{a})$
8	$-7/2^{10}(7968980a+572663\bar{a})$
7	$-27/2^{11}(3818747a-1232159\bar{a})$
6	$-7/2^{11}(2437813a-17913025\bar{a})$
5	$7/2^{16}(197210623a+8174109 15\bar{a})$
4	$21/2^{13}(19063495a+31958147\bar{a})$
3	$7/2^{17}(1127341210a+1303007163\bar{a})$
2	$7/2^{17}(651148938a+590134531\bar{a})$
1	$21/2^{20}(849646746a+438356795\bar{a})$
0	$1174191921/2^{19}a$

$M_{C_{10}{}^t} M_{C_{10}} = 4I_{10}$. We conclude that $\phi^{\dagger}_{C_{10}} \circ \phi_{C_{10}} = [4]_{J_X}$ — that is, $\phi_{C_{10}}$ splits $[4]_{J_X}$.

Genus fifteen

Suppose X and Y are curves of genus fifteen, with $\deg f_X = \deg f_Y = 31$, such that the correspondence $V(v_2 - v_1)$ on $X \times Y$ is reducible. Let $k' = k(b)$, where b is a root of the polynomial $u^2 - 13u^2 + 46u - 32$ over k, and let $K = k'(a)$, where a is a root of the polynomial $u^2 - 1/2(b^2 - 7b + 4)u + b$ over k. Let σ be the nontrivial element of the Galois group of K/k'. According to [12, §5.6], f_X is weakly linearly related to the polynomial g over K described by Tables 6.4, 6.5 and 6.4 below, and f_Y is weakly linearly related to the Galois conjugate g_{15}^{σ} of g_{15} over k'.

Suppose $f_X = g_{15}$ and $f_Y = g_{15}^{\sigma}$. The polynomial $f_X(u_1) - f_Y(u_2)$ has an absolutely irreducible factor F_{15} of degree 15; the cofactor of F_{15} is also absolutely irreducible. Hence there is a nontrivial $(15, 15)$-correspondence $C_{15} = V(v_2 - v_1, F_{15})$ on $X \times Y$. Computing differential matrices using Algorithm 6.2.7, we see that $M_{C_{15}}$ is a lower-triangular matrix, with diagonal entries

$$-(a+1),\ -(a+1),\ a+1,\ -(a+1),\ a-2,\ a+1,\ 2,\ -(a+1),$$
$$-(a-2)\ a-2,\ -(a+1),\ a+1,\ a-2,\ 2,\ -(a-2).$$

The differential matrix of the transpose is $M_{C_{15}{}^t} = M_{C_{15}}^{\sigma}$, and we find that $M_{C_{15}{}^t} M_{C_{15}} = 8I_{15}$. We conclude that $\phi^{\dagger}_{C_{15}} \circ \phi_{C_{15}} = [8]_{J_X}$ — that is, $\phi_{C_{15}}$ splits $[8]_{J_X}$.

Table 6.4: The polynomial g_{15} for genus fifteen

d	Coefficient of u^d in $g_{15}(u)$
31	1
30	0
29	$\frac{31}{2^4}\left((-b^2+5b+10)a + 2^2(b^2-7b+12)\right)$
28	$\frac{31}{2^4}\left((-b^2+5b+10)a + 2^2(b^2-7b+12)\right)$
27	$\frac{31}{2^6}\left((43b^2-1011b+2854)a + 2(453b^2-3055b+3248)\right)$
26	$\frac{31}{2^5}\left((41b^2-977b+2802)a + 2(443b^2-2993b+3248)\right)$
25	$\frac{31}{2^8}\left((-17521b^2+74509b+60450)a + 2^4(3523b^2-19318b+17095)\right)$
24	$\frac{31}{2^8}\left((-48519b^2+204491b+184718)a + 2^4\cdot 13(771b^2-4256b+3877)\right)$
23	$\frac{31}{2^{10}}\left((-1776161b^2+9373621b-3292454)a + 2(2041603b^2-11554557b+8612300)\right)$
22	$\frac{31}{2^{10}}\left((-1471159b^2+7727523b-2737610)a + 2^3(1759337b^2-10050935b+7513220)\right)$
21	$\frac{31}{2^{12}}\left((-109481293b^2+596329857b-368885054)a + 2^2\cdot 11(4234205b^2-24114867b+17025124)\right)$
20	$\frac{31}{2^{12}}\left((-384855193b^2+2112196605b-1408837958)a + 2^2\cdot 77(1995919b^2-11313121b+7849292)\right)$

Table 6.5: The polynomial g_{15} for genus fifteen (continued)

d	Coefficient of u^d in $g_{15}(u)$
19	$\frac{31}{2^{14}}\left(\begin{array}{l}(-52901848 05b^2+29820077413b-21851209042)a\\ +2\cdot 7(360226879b^2-1996954813b+1324931952)\end{array}\right)$
18	$\frac{31}{2^{13}}\left(\begin{array}{l}(-8697236749b^2+497637386 85b-38332116082)a\\ +2(2955570637b^2-16017539527b+10063185520)\end{array}\right)$
17	$\frac{31}{2^{16}}\left(\begin{array}{l}(-186111470445b^2+1067698578649b-833400031142)a\\ +2^3(47423906 75b^2-23773118387b+8368459966)\end{array}\right)$
16	$\frac{31}{2^{16}}\left(\begin{array}{l}(-494148938071b^2+2839948380571b-2256232777618)a\\ +2^3(-152886725 15b^2+92070460731b-91551968486)\end{array}\right)$
15	$\frac{31}{2^{17}}\left(\begin{array}{l}(-22140316356 15b^2+12716268790027b\\ -10156041792602)a+2(-960101407852b^2\\ +5535136704359b-4581193619353)\end{array}\right)$
14	$\frac{31}{2^{14}}\left(\begin{array}{l}(-560557994899b^2+3218369818879b\\ -2580185154146)a+2(-526496086692b^2\\ +3014302384861b-2383956611299)\end{array}\right)$
13	$\frac{31}{2^{20}}\left(\begin{array}{l}(-63813876335979b^2+367007052549207b\\ -296370094708306)a+2^2(-52401417590341b^2\\ +299616088960507b-233801230247956)\end{array}\right)$
12	$\frac{31}{2^{20}}\left(\begin{array}{l}(-845950678375 87b^2+488413358269471b\\ -399412816680130)a+2^2\cdot 13(-111503606490 73b^2\\ +63701009207311b-49349331671940)\end{array}\right)$
11	$\frac{31}{2^{22}}\left(\begin{array}{l}(-2769781233663 39b^2+1621224937178539b\\ -1399602523915382)a+2\cdot 13(-212034170543241b^2\\ +1210431089174019b-934256824364744)\end{array}\right)$
10	$\frac{31}{2^{21}}\left(\begin{array}{l}(164996225556971b^2-911562557305603b\\ +591654846604694)a+2\cdot 11(-2625201273221 01b^2\\ +14978038249706 31b-1154022167812424)\end{array}\right)$

Table 6.6: The polynomial g_{15} for genus fifteen (continued)

d	Coefficient of u^d in $g_{15}(u)$
9	$\frac{31}{2^{24}}\left(\begin{array}{l}(8153525016709589b^2 - 46226784686942241b \\ + 3446566113637359 0)a + 2^4(-5441429387111027b^2 \\ + 31035465825224200b - 23885784348462829)\end{array}\right)$
8	$\frac{31}{2^{24}}\left(\begin{array}{l}(21507787300535771b^2 - 122360462847124879b \\ + 92829028744745354)a + 2^4(-8984909831498167b^2 \\ + 51240081924362918b - 39413833154124867)\end{array}\right)$
7	$\frac{31}{2^{26}}\left(\begin{array}{l}(172549107727779319b^2 - 982848727924637571b \\ + 750639722104375338)a + 2(-4187685913103592 09b^2 \\ + 23881745617576566 43b - 1836495177429186664)\end{array}\right)$
6	$\frac{31}{2^{24}}\left(\begin{array}{l}(69182745118413131b^2 - 394265847737496263b \\ + 302027911629477314)a + 2 \cdot 3(-442263465716758 83b^2 \\ + 252216588414697081b - 193920457022904536)\end{array}\right)$
5	$\frac{31}{2^{28}}\left(\begin{array}{l}(14614941938055670 97b^2 - 83309392171884117 41b \\ + 639134618659306919 0)a + 2^2(-11326915405652144 43b^2 \\ + 64595187688623575 33b - 4965998974814592772)\end{array}\right)$
4	$\frac{31}{2^{28}}\left(\begin{array}{l}(15904704113723853 57b^2 - 90677054138259344 65b \\ + 696280801683722118 2)a + 2^2(-99941505081106445 5b^2 \\ + 56993541345040088 65b - 4381372565564213972)\end{array}\right)$
3	$\frac{31}{2^{30}}\left(\begin{array}{l}(54586547359926463 73b^2 - 31124897594589327589b \\ + 239123146324228816 18)a + 2(-55127010815078440 17b^2 \\ + 31436273506520022779b - 24164866978481400776)\end{array}\right)$
2	$\frac{31}{2^{29}}\left(\begin{array}{l}(17568721578970420 25b^2 - 10018233805014343961b \\ + 769896473917971738 6)a + 2(-13157507302059684 33b^2 \\ + 75028305025072951 95b - 5766576375747149288)\end{array}\right)$
1	$\frac{31}{2^{32}}\left(\begin{array}{l}(60990478806873593 69b^2 - 347800552762916659 89b \\ + 267340498191134930 38)a + 2^3(-74485258373686673 9b^2 \\ + 42472681086294607 83b - 3263765943271992018)\end{array}\right)$
0	$\frac{31}{2^{32}}\left(\begin{array}{l}(12903436308847515 23b^2 - 73584263081115356 07b \\ + 56570921186740734 02)a + 2^2(-10636665924628070 25b \\ + 836989554040862527)\end{array}\right)$

Chapter 7

Explicit real multiplication

In this chapter, we describe several families of hyperelliptic curves whose Jacobians have real multiplication. For each family, we give a correspondence inducing a nontrivial real multiplication, and derive an explicit, efficiently computable form for the induced endomorphism. Some of the families have been described by Mestre [44], Hashimoto [30], and by Tautz, Top and Verberkmoes [62]. Takashima [61] provides explicit formulae for the induced endomorphism of Mestre's curve in the genus two case. To our knowledge, the explicit forms for the induced endomorphisms of every other family are new in this work.

All of the families share the following construction. We find a curve $\tilde{C}$, with automorphisms α and σ such that $\langle\sigma\rangle$ is not stabilised under conjugation by α. We then define X to be the quotient of $\tilde{C}$ by $\langle\sigma\rangle$. Since conjugation by α does not stabilise $\langle\sigma\rangle$, the automorphism α does not induce an automorphism of X. However, we will see below that the endomorphism α_* of $J_{\tilde{C}}$ *does* induce an endomorphism of J_X.

For each of these families, we will give a correspondence inducing a nontrivial real multiplication and an explicit form for the induced endomorphism. The explicit endomorphisms may be used to extend GLV efficient multiplication techniques (see §2.4) to these families of hyperelliptic curves.

Throughout this chapter, k denotes a field of characteristic not two, and ζ_n denotes a primitive n^{th} root of unity over $\mathbb{Q}$.

7.1 Deriving RM from coverings

Let $\tilde{C}$ be a curve, and S a subgroup of $\mathrm{Aut}(\tilde{C})$. Let X be the quotient of $\tilde{C}$ by S, with $\pi : \tilde{C} \to X$ the quotient map; observe that π is a covering of degree $\#S$. Recall from §3.2 that for every cover $\pi' : \tilde{C} \to X$, there is a correspondence $(\pi \times \pi')(\tilde{C})$ on $X \times X$; therefore, for each automorphism α of $\tilde{C}$, we set

$$C_\alpha := (\pi \times (\pi \circ \alpha))(\tilde{C}).$$

The endomorphism of J_X induced by C_α is $\phi_{C_\alpha} = \pi_* \alpha_* \pi^*$.

Now, if P is a prime divisor on X, then $\pi^*(P)$ is the sum of an S-orbit on $\tilde{C}$ — that is, $\pi^*(P) = \sum_{\sigma \in S} \sigma(Q)$ for some prime divisor Q on $\tilde{C}$. Hence

$$\phi_{C_\alpha}(P) = \pi_*(\sum_{\sigma \in S} \alpha\sigma(Q)).$$

If α is an element of S, then $\sum_{\sigma \in S} \alpha\sigma = \sum_{\sigma \in S} \sigma$, so $\phi_C = \pi_* \pi^* = [\#S]_{J_X}$. In fact, if α is an element of S, then $C_\alpha = \#S\Delta_X$.

Following the work of Mestre [44], Brumer, and Tautz, Top and Verberkmoes [62], Ellenberg [19] describes the derivation of Jacobians with real multiplication from curves with a dihedral automorphism (sub-)group. This is the special case of the situation above where S is generated by an involution σ, and α is an element of $\mathrm{Aut}(\tilde{C}) \setminus S$ such that $\sigma\alpha\sigma = \alpha^{-1}$.

Proposition 7.1.1. *Suppose $\tilde{C}$ is a curve such that $\mathrm{Aut}(\tilde{C})$ contains a dihedral group $\langle \sigma, \alpha \mid \sigma^2 = 1, \alpha^n = 1, \alpha\sigma = \sigma\alpha^{-1} \rangle$ for some odd prime n. Let X be the quotient of $\tilde{C}$ by $\langle \sigma \rangle$, and let $\pi : \tilde{C} \to X$ be the quotient projection. Then the subring $\mathbb{Z}[\pi_* \alpha_* \pi^*]$ of $\mathrm{End}(J_X)$ is isomorphic to the subring $\mathbb{Z}[\alpha_* + \alpha_*^{-1}]$ of $\mathrm{End}(J_{\tilde{C}})$. In particular, there is a subring*

$$\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subset \mathrm{End}(J_X)$$

— that is, J_X has real multiplication by $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Proof. See Ellenberg [19, §3]. □

Corollary 7.1.2. *If $\tilde{C}$, X, π, and α are as in Proposition 7.1.1, then*

$$C_\alpha = (\pi \times \pi \circ \alpha)(\tilde{C})$$

is a $(2,2)$-correspondence on $X \times X$, and the subring $\mathbb{Z}[\phi_{C_\alpha}]$ of $\mathrm{End}(J_X)$ is isomorphic to $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Proof. We know $d_1(C_\alpha) = \deg \pi$ and $d_2(C_\alpha) = \deg(\pi \circ \alpha)$ – but both π and $\pi \circ \alpha$ are coverings of degree two, so C_α is a $(2,2)$-correspondence. The endomorphism of J_X induced by C_α is $\pi_* \circ (\pi \circ \alpha)^* = \pi_* \circ \alpha_* \circ \pi^*$, so the second assertion follows from Proposition 7.1.1. □

In the next section, we derive an algorithm for computing explicit forms for the endomorphisms induced by some $(2,2)$-correspondences, allowing us to make some of the real multiplications described by Proposition 7.1.1 completely effective. Our explicit endomorphisms will be in the form of maps of Mumford ideal class representatives. We have seen a particularly simple example of this kind of construction, for the $(1,1)$-correspondences $C_{p,i}$ on the curves $Y_p : v^2 = u^p + 1$ constructed in §6.4.

7.2 Explicit induced homomorphisms

Suppose $C = V(v_1 - v_2, E(u_1, u_2))$ is a $(2,2)$-correspondence on $X \times Y$, where $E(u_1, u_2)$ is a factor of $f_X(u_1) - f_Y(u_2)$. Note that $E(u_1, u_2)$ must be a polynomial of degree two in both u_1 and u_2. Consider E to be a polynomial in u_2 over $k[u_1]$, and suppose that e_1 and e_2 are its roots in $\overline{k(C)}$. The image of the generic point (u, v) of X under the homomorphism ϕ_C is

$$\phi_C((u,v)) = (e_1, v) + (e_2, v).$$

Hence, given an ideal class representative $[(a(u), v - b(u))]$ we have

$$\begin{aligned}\phi_C([(a(u), v - b(u))]) &= [(a(e_1), v - b(e_1))] + [(a(e_2), v - b(e_2))] \\ &= [(a(e_1), v - b(e_1))(a(e_2), v - b(e_2))].\end{aligned}$$

The image is an ideal of $\mathcal{O}_C$, and may be expressed in terms of symmetric polynomials in the e_i and the coefficients of the polynomials $a(u)$ and $b(u)$. The following proposition makes this precise.

Proposition 7.2.1. *If $C = V(v_2 - v_1, E(u_1, u_2))$ is a $(2,2)$-correspondence on $X \times Y$, then there exist maps $T_C : k[u] \to k(u)$ and $N_C : k[u] \to k(u)$, depending only upon C, such that for any point $[(a(u), v - b(u))]$ of J_X,*

$$\phi_C([(a(u), v - b(u))]) = \left[\left(\frac{N_C(a)}{g}, v - \left(\frac{(f_Y + N_C(b))/g}{T_C(b)/g} \bmod \frac{N_C(a)}{g}\right)\right)\right]$$

where $g = \gcd(N_C(a), T_C(b))$, scaled if necessary so that g and $N_C(a)$ have the same leading coefficient.

Proof. Suppose that α and $\overline{\alpha}$ are the solutions to the quadratic equation $E(u,x) = E_2(u)x^2 + E_1(u)x + E_0(u) = 0$ over $k(u)$. Note that $\alpha + \overline{\alpha} = -E_1/E_2$ and $\alpha\overline{\alpha} = E_0/E_2$; both are rational functions of u. For $i \geq 0$, we define

$$t_i := \alpha^i + \overline{\alpha}^i, \quad n_i := (\alpha\overline{\alpha})^i, \quad \text{and} \quad n_{i,j} := \alpha^i\overline{\alpha}^j + \alpha^j\overline{\alpha}^i.$$

The elements t_i, n_i and $n_{i,j}$ satisfy the following recurrences:

1. $n_{i+1} = (\alpha\overline{\alpha})n_i$ for $i \geq 0$, with $n_0 := 1$;
2. $t_{i+1} = (\alpha + \overline{\alpha})t_i - (\alpha\overline{\alpha})t_{i-1}$ for $i \geq 1$, with $t_0 = 2$ and $t_1 = (\alpha + \overline{\alpha})$;
3. $n_{i,i} = n_i$ and $n_{i,j} = n_i t_{j-i}$ for $i \geq 0$ and $j > i$.

Each of the t_i, n_i and $n_{i,j}$ may thus be written as a polynomial expression in $\alpha + \overline{\alpha} = -E_1/E_2$ and $\alpha\overline{\alpha} = E_0/E_2$; so the t_i, n_i and $n_{i,j}$ are rational functions of u. Now, define $N_C : k[u] \longrightarrow k(u)$ by

$$N_C(\sum_i a_i u^i) := \sum_{i,j} a_i a_j n_{i,j}$$

and $T_C : k[u] \longrightarrow k(u)$ by

$$T_C(\sum_i a_i u^i) := \sum_i a_i t_i.$$

Observe that $N_C(a) = a(\alpha)a(\overline{\alpha})$ and $T_C(a) = a(\alpha) + a(\overline{\alpha})$ for all polynomials a over k. Therefore, if a point P of J_X represented by the ideal class $[(a(u), v - b(u))]$, then

$$\begin{aligned}\phi_C([(a, v-b)]) &= [(a(\alpha), v - b(\alpha))] + [(a(\overline{\alpha}), v - b(\overline{\alpha}))] \\ &= [(a(\alpha), v - b(\alpha)) \cdot (a(\overline{\alpha}), v - b(\overline{\alpha}))] \\ &= [(a(\alpha)a(\overline{\alpha}), v^2 - (b(\alpha) + b(\overline{\alpha}))v + b(\alpha)b(\overline{\alpha}))] \\ &= [(N_C(a), T_C(b)v - (v^2 + N_C(b)))].\end{aligned}$$

Let $g = \gcd(N_C(a), T_C(b))$, scaling g if necessary so that g and $N_C(a)$ have the same leading coefficients. We have

$$T_C(b) = b(e_1) + b(e_2) \equiv 0 \pmod{g},$$

so $b(e_1) \equiv -b(e_2) \pmod{g}$; thus

$$b(e_1)^2 \equiv b(e_2)^2 \equiv -N_C(b) \pmod{g}.$$

Now, $b(e_1)^2 \equiv v^2 \pmod{a(e_1)}$ and $b(e_2)^2 \equiv v^2 \pmod{a(e_2)}$, so

$$\begin{aligned}(v^2 - b(e_1)^2)(v^2 - b(e_2)^2) &\equiv 0 \pmod{N_C(a)} \\ &\equiv 0 \pmod{g},\end{aligned}$$

and so $(v^2 + N_C(b))^2 \equiv 0 \pmod{g}$. Hence g divides $v^2 + N_C(b)$, which is equal to $f_Y(u) + N_C(b)$, and

$$\begin{aligned}\phi_C([(a, v-b)]) &= [(N_C(a), T_C(b)v - (f_Y + N_C(b)))] \\ &= [(g)\left((T_C(b)/g)v - (f_Y + N_C(b))/g\right)] \\ &= [(N_C(a)/g, (T_C(b)/g)v - (f_Y + N_C(b))/g)] \\ &= \left[\left(\frac{N_C(a)}{g}, v - \left(\frac{(f_Y + N_C(b))/g}{T_C(b)/g} \bmod \frac{N_C(a)}{g}\right)\right)\right],\end{aligned}$$

proving the claim. □

The recurrences in the proof of Proposition 7.2.1 show that the functions t_i, n_i and $n_{i,j}$ are dependent *only* upon t_1 and n_1, which may be read off from

the coefficients of $E(u_1, u_2)$ when considered as a polynomial in u_2. Thus, given $t_1 = -E_1/E_2$ and $n_1 = n_{1,1} = E_0/E_2$, the recurrences give us a simple and efficient algorithm for computing all of the functions t_i and $n_{i,j}$, and thus for computing the maps T_C and N_C. We need only ever evaluate our explicit map for ϕ_C on *reduced* Mumford ideal class representatives — that is, classes $[(a, v - b)]$ where $\deg(a) \leq g_X$ and $\deg b < \deg a$ — so we need only compute the t_i and $n_{i,j}$ for $0 \leq i \leq g_X$. The t_i and $n_{i,j}$ may of course be precomputed, reducing the maps T_C and N_C to functions of the coefficients of their arguments. The following algorithm makes Proposition 7.2.1 effective.

Algorithm 7.2.2. Given a $(2, 2)$-correspondence $C = V(v_2 - v_1, E(u_1, u_2))$ on $X \times Y$, computes the polynomial maps T_C and N_C of Proposition 7.2.1.

function ExplicitMappings(C)
  // Consider $E(u_1, u_2)$ to be a polynomial in u_2.
  $t_0 := 2$;
  $n_0 := 1$;
  $n_{0,0} := n_0$;
  $t_1 := -\text{Coefficient}(E, u_2)/\text{Coefficient}(E, u_2^2)$;
  $n_1 := \text{Coefficient}(E, u_2^0)/\text{Coefficient}(E, u_2^2)$;
  for i in $[2, \ldots, g_X]$ **do**
    $n_i := n_1 n_{i-1}$;
    $t_i := t_1 t_{i-1} - n_1 t_{i-2}$; // Store for re-use.
    $n_{i,i} := n_i$; // Store for re-use.
    for $i < j \leq g_X$ **do**
      $n_{i,j} := n_i t_{j-i}$; // Store for re-use.
    end for
  end for
  $T_C := \left(\sum_{i=0}^{g_X} a_i u^i \longmapsto \sum_{i=0}^{g} a_i t_i\right)$;
  $N_C := \left(\sum_{i=0}^{g_X} a_i u^i \longmapsto \sum_{0 \leq i \leq j \leq g} a_i a_j n_{i,j}\right)$;
  return T_C, N_C;
end function

In the next chapter, we will apply this method to a number of families of correspondences of hyperelliptic curves, in each case constructing explicit

representations for the homomorphisms induced by the correspondences.

7.3 RM from cyclotomic coverings

We now return to the curves $X_n : v^2 = D_n(u, a) + t$ over $k(t)$ of Theorem 6.3.3 where a is not zero. Theorem 6.3.3 implies that the correspondence $V(v_2 - v_1)$ on $X_n \times X_n$ is reducible. We will show that X_n has a covering such that J_X has real multiplication as in Proposition 7.1.1, and that this real multiplication is induced by the components of $V(v_2 - v_1)$ other than the diagonal.

Let $n > 2$ be an integer not divisible by the characteristic of k, and set $m = \lfloor (n+1)/2 \rfloor$. Let X_n be the curve over $k(t)$ defined by

$$X_n : v^2 = f_{X_n}(u) = D_n(u, a) + t,$$

where a is a nonzero element of k and $D_n(u, a)$ is the n^{th} Dickson polynomial with parameter a. Let $\tilde{C}_n$ be the curve defined by

$$\tilde{C}_n : v^2 = f_{\tilde{C}_n}(u) = u^{2m} f_{X_n}(u + a/u).$$

Recall that $D_n(u + a/u, a) = u^n + (a/u)^n$ by Lemma 2.5.2, so $f_{\tilde{C}_n}$ is in fact a polynomial in u. If n is even, then $f_{\tilde{C}_n}(u) = u^{2n} + tu^n + a^n$; if n is odd, then $f_{\tilde{C}_n}(u) = u(u^{2n} + tu^n + a^n)$.

In addition to its hyperelliptic involution, the curve $\tilde{C}_n$ has an involution σ defined by

$$\sigma : (u, v) \mapsto (a/u, v(a/u)^m).$$

It is easy to see that X_n is the quotient of $\tilde{C}_n$ by $\langle \sigma \rangle$; the quotient map $\pi : \tilde{C}_n \to X_n$ is defined by $\pi(u, v) = (u + a/u, vu^{-m})$.

The families $\tilde{C}_n$ and X_n coincide with curves described by Tautz et. al. in [62] when $a = 1$. When n is odd, our curves are the families $\mathcal{D}_n$ and $\mathcal{C}_n$ of [62]; when n is even, $\tilde{C}_n$ and X_n are not the curves $\mathcal{D}_n$ and $\mathcal{C}_n$, but rather the curves mentioned in a remark of [62, page 1058].

Suppose λ_{2n} is a primitive $2n^{\text{th}}$ root of unity over k; let $\lambda_n = \lambda_{2n}^2$ and

$\eta_n = \lambda_n + \lambda_n^{-1}$. The curve $\tilde{C}_n$ has an automorphism ζ defined by

$$\zeta : (u, v) \longmapsto (\lambda_n u, \lambda_{2n} v).$$

The order of ζ is clearly $2n$; further, $\zeta^n = \iota_{\tilde{C}_n}$.

Observe that $\zeta\sigma = \sigma\zeta^{-1}$, so $\langle \sigma, \zeta \rangle$ is a dihedral subgroup of $\mathrm{Aut}(\tilde{C}_n)$, and $\pi \circ \zeta \neq \pi$. We have a correspondence $C_n := C_\zeta = (\pi \times (\pi \circ \zeta))(\tilde{C}_n)$ on $X_n \times X_n$, with a model

$$C_n = V\left(v_2 - v_1, u_1^2 - \eta_n u_1 u_2 + u_2^2 + (\eta_n^2 - 4)a\right).$$

Note that while the automorphism ζ is defined over $k(\lambda_{2n})$, the correspondence C_n is defined over the subfield $k(\lambda_n)$. Applying Proposition 7.1.1, we see that J_{X_n} has real multiplication by $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Further, C_n satisfies the hypotheses of Proposition 7.2.1, so we may compute an explicit form for its induced endomorphism. Applying Algorithm 7.2.2 (ExplicitMappings) with $t_1 = \eta_n u$ and $n_1 = u^2 + (\eta_n^2 - 4)a$, we compute maps T_{C_n} and N_{C_n} such that ϕ_{C_n} is realised by

$$[(a(u), v - b(u))] \longmapsto \left[\left(\frac{N_{C_n}(a)}{g}, v - \left(\frac{(f_{X_n} + N_{C_n}(b))/g}{T_{C_n}(b)/g} \bmod \frac{N_{C_n}(a)}{g}\right)\right)\right],$$

where g is the greatest common divisor of $N_{C_n}(a)$ and $T_{C_n}(b)$, scaled to have the same leading coefficient as $N_{C_n}(a)$.

Example 7.3.1 *(Real Multiplication by* $(-1+\sqrt{5})/2$*).* Consider the genus two curve X_5, where $a = 1$:

$$X_5 : v^2 = f_{X_5} = u^5 - 5u^3 + 5u + t.$$

The curve X_5 is covered by the curve $\tilde{C}_5$ of genus five defined by

$$\tilde{C}_5 : y^2 = x(x^{10} + tx^5 + 1);$$

the covering map $\pi : \tilde{C}_5 \to X_5$ maps (x, y) to $(u, v) = (x + x^{-1}, yx^{-3})$.

Let $\eta_5 = \lambda_5 + \lambda_5^{-1}$, where λ is a fifth root of unity over k. By Proposition

7.1.1, the correspondence $C_5 := (\pi \times \pi \circ \zeta)(\tilde{C}_5)$ induces an endomorphism of J_{X_n}, defined over $k(\eta_5)$, with minimal polynomial that of ζ_5 over $\mathbb{Q}$. Note that one embedding of $\mathbb{Q}(\zeta_5)$ into $\mathbb{C}$ sends $\zeta_5 + \zeta_5^{-1}$ to $(-1+\sqrt{5})/2$.

A generic point on J_{X_5} has a reduced representative $[(a(u), v - b(u))]$, with $\deg a = 2$ and $\deg b = 1$. Therefore, write $a(u) = u^2 + a_1 u + a_0$ and $b(u) = b_1 u + b_0$. By Proposition 7.2.1, there are polynomial maps N_{C_5} and T_{C_5} such that ϕ_{C_5} is realised by

$$[(a(u), v - b(u))] \longmapsto \left[\left(\frac{N_{C_5}(a)}{g}, v - \left(\frac{(f_{X_5} - N_{C_5}(b))/g}{T_{C_5}(b)/g} \bmod \frac{N_{C_5}(a)}{g}\right)\right)\right],$$

where $g = \gcd(N_{C_5}(a), T_{C_5}(b))$, scaled so that g and $N_{C_5}(a)$ have the same leading coefficient. To compute N_{C_5} and T_{C_5}, we apply Algorithm 7.2.2 (ExplicitMappings) to C_5. We derive

$$\begin{aligned} N_{C_5}(a) &= n_{2,2} + a_1 n_{1,2} + a_1^2 n_{1,1} + a_0 n_{0,2} + a_1 a_0 n_{0,1} + a_0^2 n_{0,0}, \\ N_{C_5}(b) &= b_1^2 n_{1,1} + b_1 b_0 n_{0,1} + b_0^2 n_{0,0}, \\ T_{C_5}(b) &= \eta_5 u b_1 + 2 b_0, \end{aligned}$$

with the polynomials $n_{i,j}$ given in the table below:

$n_{0,0}$	1	$n_{1,1}$	$u^2 - \eta_5^2 - 4$
$n_{0,1}$	$\eta_5 u$	$n_{1,2}$	$\eta_5 u^3 - \eta_5^3 u - 4\eta_5 u$
$n_{0,2}$	$(\eta_5^2 - 2)u^2 - 2\eta_5^2 + 8$	$n_{2,2}$	$u^4 - 2(\eta_5^2 - 4)u^2 + 8(\eta_5^2 + 2)$

One iteration of Algorithm 2.3.3 (CantorReduction) will produce a reduced representative for the image.

Example 7.3.2. Let $k = \mathbb{F}_p$ where $p = 100019$, and let X be the curve X_5 with $a = 1$ and $t = 38$:

$$X : v^2 = u^5 - 5u^3 + 5u + 38.$$

By construction, J_X has an efficiently computable endomorphism $[\eta_5] = \phi_{C_5}$, where $[\eta_5]^2 + [\eta_5] - [1]_{J_X} = 0$. In fact, we may take a 10^{th} root of unity λ_{10} over k such that $\lambda_{10} + \lambda_{10}^{-1} = 96937$ in k, so the endomorphism $[\eta_5]$ is defined over k. We have $\#J_X = 19 \cdot N$, where $N = 524594129$. The polynomial

$u^2 + u - 1$ has roots 56956504 and 467637324 modulo N. We find that $[\eta_5] \equiv [56956504]$ on $19J_X$.

7.4 RM from Artin–Schreier coverings

Our next families of Jacobians with real multiplication are derived from coverings by Artin–Schreier curves. For each odd prime characteristic p, we define a one-parameter rational family of hyperelliptic curves of genus $(p-1)/2$, together with a correspondence inducing a real multiplication on the Jacobian of any curve in the family. The family and the correspondence are defined over $\mathbb{F}_p$ (and hence over every field of characteristic p).

Suppose k is a field of characteristic p, where p is odd. Let

$$S_p := \{\ n^2 \bmod p\ : 1 \leq n \leq p-1\}$$

be the set of (nonzero) quadratic residues modulo p; set $m := \#S = (p-1)/2$. Let t be a free parameter, and $\tilde{A}_p$ the Artin–Schreier curve over $k(t)$ defined by

$$\tilde{A}_p : y^p - y = x - \frac{t}{x}.$$

(We may consider $\tilde{A}_p$ to be a rational family of Artin–Schreier curves over k, parametrised by t). The curve $\tilde{A}_p$ has an involution σ, defined by

$$\sigma : (x, y) \longmapsto (t/x, -y),$$

and an automorphism ζ of order p, defined by

$$\zeta : (x, y) \longmapsto (x, y + 1).$$

It is easily verified that $\zeta\sigma = \sigma\zeta^{-1}$; thus $\langle \sigma, \zeta \rangle$ is a dihedral subgroup of $\mathrm{Aut}(\tilde{A}_p)$, and we may apply Proposition 7.1.1 to construct a Jacobian with multiplication by $\zeta_p + \zeta_p^{-1}$.

Let $X_p := \tilde{A}_p/\langle\sigma\rangle$ be the quotient of $\tilde{A}_p$ by the action of σ. We have an

affine plane model

$$X_p : v^2 = f_{X_p}(u) = u(u^m - 1)^2 - 4t;$$

it is clear from this model that X_p is hyperelliptic. The hyperelliptic polynomial f_{X_p} has degree $2m + 1 = p$, so X_p is a curve of genus m. Note that f_{X_p} is *not* tame, since char $k = \deg f_{X_p}$, so Theorem 6.3.3 does not apply here. The covering map $\pi : \tilde{A}_p \to X_p$ is of degree two, and is defined by

$$\pi : (x, y) \mapsto (u, v) = (y^2, x + t/x).$$

Since $\langle\sigma\rangle$ is not stable under conjugation by ζ, the covers $\pi \circ \zeta$ and π are distinct: in fact, $(\pi \circ \zeta)$ maps (x, y) to $(u, v) = ((y + 1)^2, x + t/x)$.

The polynomial $f_{X_p}(u_1) - f_{X_p}(u_2)$ factors into a product of $m + 1$ irreducible polynomials

$$f_{X_p}(u_1) - f_{X_p}(u_2) = (u_1 - u_2) \prod_{\tau \in S_p} \left((u_1 - u_2)^2 - 2\tau(u_1 + u_2) + \tau^2\right)$$

over k; in terms of correspondences on $X_p \times X_p$, we have

$$V(v_2 - v_1) = \Delta_X + \sum_{\tau \in S_p} A_{p,\tau},$$

where each correspondence $A_{p,\tau}$ is defined by

$$A_{p,\tau} = V\left(v_2 - v_1, (u_1 - u_2)^2 - 2\tau(u_1 + u_2) + \tau^2\right).$$

Observe that $A_{p,\tau} = (\pi \times (\pi \circ \zeta^{\sqrt{\tau}}))(\tilde{A}_p)$ for each quadratic residue τ in S_p, where $\sqrt{\tau}$ is any integer whose square has residue τ modulo p. The correspondence $A_{p,\tau}$ induces the endomorphism $\phi_{A_{p,\tau}} = \pi_* \circ (\zeta^\tau)_* \circ \pi^*$ on J_{X_p}, which we may identify with $\zeta_p^\tau + \zeta_p^{-\tau}$ by Proposition 7.1.1.

The correspondence $A_{p,\tau}$ satisfies the hypotheses of Proposition 7.2.1, so we may apply Algorithm 7.2.2 ExplicitMappings with $t_1 := 2(u + \tau)$ and $n_1 := (u - \tau)^2$ to construct maps $T_{A_{p,\tau}}$ and $N_{A_{p,\tau}}$ such that the image of

$[(a(u), v - b(u))]$ under $\phi_{A_{p,\tau}}$ is given by

$$\left[\left(\frac{N_{A_{p,\tau}}(a)}{g}, v - \left(\frac{(f_{X_p} + N_{A_{p,\tau}}(b))/g}{T_{A_{p,\tau}}(b)/g} \bmod \frac{N_{A_{p,\tau}}(a)}{g}\right)\right)\right],$$

where $g = \gcd(N_{A_{p,\tau}}(a), T_{A_{p,\tau}}(b))$ (scaled appropriately). A reduced representative for this image is produced after one iteration of Algorithm 2.3.3 (CantorReduction).

Example 7.4.1. Consider $p = 3$. There is only one quadratic residue modulo 3 — namely, 1 — so $S_3 = \{1\}$. The curve X_3 is of genus one, so J_{X_3} is an elliptic curve, and the real multiplication $\phi_{A_{3,1}}$ is therefore multiplication by some integer. By Proposition 7.1.1, there is an isomorphism $\mathbb{Z}[\phi_{A_{3,1}}] \cong \mathbb{Z}[\zeta_3 + \zeta_3^{-1}]$ sending $\phi_{A_{3,1}}$ to $\zeta_3 + \zeta_3^{-1}$; but $\zeta_3 + \zeta_3^{-1} = -1$, so $\phi_{A_{3,1}} = [-1]_{J_{X_3}}$. Alternatively, note that $A_{3,1} = V(v_2 - v_1) - \Delta_{X_3} \approx -\Delta_{X_3}$, so $\phi_{A_{3,1}} = -\phi_{\Delta_{X_3}} = [-1]_{J_{X_3}}$.

Example 7.4.2. For $p = 5$, we have two quadratic residues: $S_5 = \{1, -1\}$. We derive the one-parameter family of genus two hyperelliptic curves defined over $\mathbb{F}_5$ by

$$X_5 : v^2 = f_{X_5}(u) = u(u^2 - 1)^2 + t.$$

By Proposition 7.1.1, we may explicitly construct a subring of $\mathrm{End}(J_{X_5})$ isomorphic to $\mathbb{Z}[\zeta_5 + \zeta_5^{-1}]$. We have $V(v_2 - v_1) = \Delta_{X_5} + A_{5,-1} + A_{5,1}$, where

$$A_{5,1} = V\big(v_2 - v_1, (u_1 - u_2)^2 - 2(u_1 + u_2) + 1\big)$$

and

$$A_{5,-1} = V\big(v_2 - v_1, (u_1 - u_2)^2 + 2(u_1 + u_2) + 1\big)$$

We (arbitrarily) identify $\phi_{A_{5,1}}$ with $\zeta_5 + \zeta_5^{-1} = \frac{1}{2}(-1 + \sqrt{5})$, using Proposition 7.1.1; we must then identify $\phi_{A_{5,-1}}$ with $-1 - \eta_5 = \frac{1}{2}(-1 - \sqrt{5})$. A generic point of J_{X_5} may be represented by a reduced Mumford ideal $[(a(u), v - b(u))]$, where a is a monic polynomial of degree two, and b is linear. Suppose $a(u) = u^2 + a_1 u + a_0$ and $b(u) = b_1 u + b_0$. Applying Algorithm 7.2.2 (ExplicitMappings), we find that the image of $[(a(u), v - b(u))]$ un-

der the endomorphism $\phi_{A_{5,\tau}}$ is given explicitly by

$$\left[\left(\frac{N_{A_{5,\tau}}(a)}{g}, v - \left(\frac{(f_{X_5} + N_{A_{5,\tau}}(b))/g}{T_{A_{5,\tau}}(b)/g} \bmod \frac{N_{A_{5,\tau}}(a)}{g}\right)\right)\right],$$

where $g = \gcd(N_{A_{5,\tau}}(a), T_{A_{5,\tau}}(b))$ (scaled appropriately), and

$$\begin{aligned} T_{A_{5,\tau}}(b) &= 2(u+\tau)b_1 + 2b_0, \\ N_{A_{5,\tau}}(a) &= n_{2,2} + a_1 n_{1,2} + a_1^2 n_{1,1} + a_0 n_{0,2} + a_1 a_0 n_{0,1} + a_0^2 n_{0,0}, \\ N_{A_{5,\tau}}(b) &= b_1^2 n_{1,1} + b_1 b_0 n_{0,1} + b_0^2 n_{0,0}, \end{aligned}$$

with the $n_{i,j}$ precomputed in the table below.

$n_{0,0}$	1	$n_{0,2}$	$2(u^2+6\tau u+1)$	$n_{1,2}$	$2(u^2-1)(u-\tau)$
$n_{0,1}$	$2(u+\tau)$	$n_{1,1}$	$(u-\tau)^2$	$n_{2,2}$	$(u-\tau)^4$

Note that $\phi_{A_{5,1}} - \phi_{A_{5,-1}}$ is identified with $\frac{1}{2}(-1+\sqrt{5}) - \frac{1}{2}(-1-\sqrt{5}) = \sqrt{5}$, so we may use our explicit endomorphisms to further construct an explicit square root of $[5]$ in $\mathrm{End}(J_X)$.

Example 7.4.3. For $p = 7$, we derive a family of hyperelliptic curves of genus three defined by

$$X_7 : v^2 = u(u^3-1)^2 + 3t$$

over any field of characteristic 7. There is an explicitly constructible subring $\mathrm{End}(J_{X_7})$ isomorphic to the totally real ring $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}] \cong \mathbb{Z}[x]/(x^3 + x^2 - 2x - 1)$.

Example 7.4.4. Let us consider an example of fast scalar multiplication derived from the Artin–Schreier family for $p = 5$. Let $k = \mathbb{F}_5[\xi]$, where $\xi^{37} + 4\xi^2 + 3\xi + 3 = 0$, and let $t = 3\xi^5 + \xi^4 + 3\xi^3 + \xi^2 + 2\xi + 3$. The element t is a square in k; let y be a square root of t. Now, let X be the curve defined by

$$X : v^2 = u(u^2-1)^2 + t,$$

By construction, there is an explicit real multiplication η_5 in $\mathrm{End}(J_X)$, which satisfies $\eta_5^2 + \eta_5 - [1] \equiv [0]$. We have $\#J_X(k) = 5n$, where

$$n = 10587911840677016896746370253405315654560117903413 11.$$

If P is the image in $J_X(k)$ of the point $(0, y)$ in $X(k)$, then $[5]P$ generates a cyclic subgroup of J_X of order n; η acts as a solution to $\eta_5^2 + \eta_5 - 1 \equiv 0 \pmod{n}$ on this subgroup. We find that $\eta_5(5P) = [m](5P)$, where

$$m = 336894053941004885519266617028956898972619907667301.$$

7.5 RM from elliptic isogeny kernels

Finally, we consider families of hyperelliptic Jacobians with explicit real multiplications introduced by Mestre in [44]. These families form subfamilies of the families described by Brumer in the unpublished work [6] and reconstructed by Hashimoto in [30].

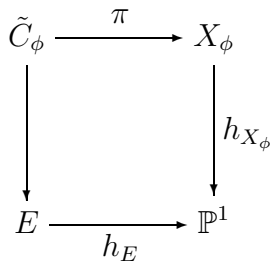
Suppose E and E' are curves of genus one, each with a rational point, such that there exists an isogeny $\phi : J_E \to J_{E'}$ with cyclic kernel of order $n > 2$. The injections $\alpha_E : E \to J_E$ and $\alpha_{E'} : E' \to J_{E'}$ are isomorphisms, so ϕ induces a covering $\alpha_{E'}^{-1} \circ \phi \circ \alpha_E : E \to E'$. Let f_ϕ be the rational function over k such that the induced morphism $f_\phi : \mathbb{P}^1 \to \mathbb{P}^1$ makes the diagram

$$\begin{array}{ccccccc} E & \xrightarrow{\alpha_E} & J_E & \xrightarrow{\phi} & J_{E'} & \xrightarrow{\alpha_{E'}^{-1}} & E' \\ \downarrow{\scriptstyle h_E} & & & & & & \downarrow{\scriptstyle h_{E'}} \\ \mathbb{P}^1 & & & \xrightarrow{f_\phi} & & & \mathbb{P}^1 \end{array}$$

commute. The degree of f_ϕ is n.

Now, let t be a free parameter, and let X_ϕ be the hyperelliptic curve over $k(t)$ defined by the affine plane model $X_\phi : v^2 = f_\phi(u) + t$ (we may regard X_ϕ as a family of curves over k, parametrised by t). Let the curve $\tilde{C}_\phi$ be the

product of X_ϕ and E over $\mathbb{P}^1$, as in the diagram below.



The hyperelliptic involution ι_E of E lifts to an involution σ of $\tilde{C}_\phi$. Since h_E is the quotient by $\langle \iota_E \rangle$, the projection $\pi : \tilde{C}_\phi \to X_\phi$ in the diagram above is the quotient by $\langle \sigma \rangle$.

Let R be an element of $\ker \phi$. It is easily verified that the translation map

$$t_R : P \mapsto \alpha_E^{-1}(\alpha_E(P) + R)$$

is an automorphism of E of order n with inverse t_{-R}, and that $t_R \circ \iota_E = \iota_E \circ t_{-R}$. We have $f_\phi(h_E(t_R(P))) = f_\phi(h_E(P))$ for all points P of E. The automorphism t_R of E lifts to an automorphism α_R of $\tilde{C}_\phi$. In fact, the automorphisms α_R and σ anticommute: $\alpha_R \sigma = \sigma \alpha_R^{-1}$. Therefore, $\mathrm{Aut}(\tilde{C}_\phi)$ contains a dihedral subgroup $\langle \sigma, \alpha_R \rangle$. By Proposition 7.1.1, the endomorphism ring $\mathrm{End}(J_X)$ contains a subring isomorphic to $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

It remains to construct a suitable n-isogeny ϕ; but these are parametrised by the modular curves $X_0(n)$. In particular, if $X_0(n)$ is a curve of genus zero, then it is rationally parametrised — by a free parameter s, say — and so we have a rationally parametrised family of isogenies $\phi_s : J_{E_s} \to J_{E'_s}$. Using ϕ_s in the above construction, we obtain a family of coverings $\pi : \tilde{C}_n \to X_n$ over k parametrised by s and t. The Jacobian J_{X_n} has real multiplication by $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, where the correspondence $C_n := (\pi \times (\pi \circ \zeta))(\tilde{C}_n)$ induces $[\zeta_n + \zeta_n^{-1}]_{J_{X_n}}$.

Example 7.5.1. Let s and t be free parameters, and $k(s,t)/k$ a rational function field. Let X_5 be the curve of genus two over $k(s,t)$ defined by

$$X_5 : v^2 = f_{X_5}(u) = u^4(u-s) - s(u+1)(u-s)^3 + s^3u^3 - tu^2(u-s)^2,$$

and let C_5 be the correspondence on $X_5 \times X_5$ defined by

$$C_5 = V\big(v_2 - v_1, u_1^2 u_2^2 + s(s-1)u_1 u_2 - s^2(u_1 - u_2) + s^3\big).$$

The subring $\mathbb{Z}[\phi_{C_5}]$ of $\mathrm{End}(J_{X_5})$ is isomorphic to $\mathbb{Z}[\zeta_5 + \zeta_5^{-1}] = \mathbb{Z}[(-1+\sqrt{5})/2]$, and the isomorphism sends ϕ_{C_5} to $\zeta_5 + \zeta_5^{-1}$.

Generically, points on J_{X_5} may be represented by Mumford ideal class representatives $[(a(u), v - b(u))]$ with $a = u^2 + a_1 u + a_0$ and $b = b_1 u + b_0$, since X_5 is a curve of genus two. By Proposition 7.2.1, the image of $[(a(u), v - b(u))]$ ϕ_{C_5} is given by

$$\left[\left(\frac{N_{C_5}(a)}{g}, v - \left(\frac{(f_{X_5} + N_{C_5}(b))/g}{T_{C_5}(b)/g} \bmod \frac{N_{C_5}(a)}{g}\right)\right)\right],$$

where $g = \gcd(N_{C_5}(a), T_{C_5}(b))$ (scaled appropriately), and where the maps T_{C_5} and N_{C_5} are computed using Algorithm 7.2.2 (ExplicitMappings). We derive

$$\begin{aligned} T_{C_5}(b) &= -s((s-1)u - s)b_1/u^2 + 2b_0, \\ N_{C_5}(a) &= n_{2,2} + a_1 n_{1,2} + a_1^2 n_{1,1} + a_0 a_2 n_{0,2} + a_1 a_0 n_{0,1} + a_0^2 n_{0,0}, \\ N_{C_5}(b) &= b_1^2 n_{1,1} + b_1 b_0 n_{0,1} + b_0^2 n_{0,0}, \end{aligned}$$

where the $n_{i,j}$ are listed in the table below:

$n_{0,0}$	1
$n_{0,1}$	$-s((s-1)u - s)/u^2$
$n_{0,2}$	$s^2(((s-1)u - s)^2 - 2u^2(u+s))/u^4$
$n_{1,1}$	$s^2(u+s)/u^2$
$n_{1,2}$	$-s^3(u+s)((s-1)u - s)/u^4$
$n_{2,2}$	$s^4(u+s)^2/u^4$

Note that the denominators in this representative should be cleared before applying Algorithm 2.3.3 (CantorReduction) to obtain the reduced representative of $\phi_{C_5}([(a, v-b)])$.

Remark 7.5.2. Takashima [61] provides an alternative construction of the explicit real multiplication in Example 7.5.1, based on Hashimoto's recon-

struction of this family of curves [30].

Example 7.5.3. Let s and t be free parameters, and X_7 the hyperelliptic curve of genus three over $k(s,t)$ defined by

$$X_7 : v^2 = f_7(u) = \phi_7(u) - t\,\psi_7(u)^2,$$

where $\psi_7(u) := u(u - s^3 + s^2)(u - s^2 + s)$ and

$$\begin{aligned}\phi_7(u) := u\psi_7(u)^2 &+ s(s-1)(s^2-s+1)(s^3+2s^2-5s+1)u^5\\ &- s^3(s-1)^2(6s^4-11s^3+12s^2-11s-1)u^4\\ &+ s^4(s-1)^3(s^2-s-1)(s^3+2s^2+6s+1)u^3\\ &- s^6(s-1)^4(s+1)(3s^2-5s-3)u^2\\ &+ s^8(s-1)^5(s^2-3s-3)u + s^{10}(s-1)^6.\end{aligned}$$

We may regard X_7 as a family of curves over k parametrised by s and t. Let C_7 be the correspondence on $X_7 \times X_7$ defined by

$$C_7 = V\left(v_2 - v_1, u_1^2u_2^2 - w(s^2-s-1)u_1u_2 - w^2(u_1+u_2) + w^3\right).$$

We have an explicitly constructible subring $\mathbb{Z}[\phi_{C_7}]$ of $\mathrm{End}(J_{X_7})$, isomorphic to $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$; the isomorphism sends ϕ_{C_7} to $\zeta_7 + \zeta_7^{-1}$. Let $w = s^2(s-1)$. Applying Algorithm 7.2.2 (ExplicitMappings) to C_7, we obtain maps N_{C_7} and T_{C_7} such that ϕ_{C_7} is realised by

$$[(a, v-b)] \mapsto \left[\left(\frac{N_{C_7}(a)}{g}, v - \left(\frac{(f_{X_7} + N_{C_7}(b))/g}{T_{C_7}(b)/g} \bmod \frac{N_{C_7}(a)}{g}\right)\right)\right],$$

where $g = \gcd(N_{C_7}(a), T_{C_7}(b))$ (scaled appropriately).

The constructions for Mestre's curves are considerably more complicated than those for the cyclotomic and Artin–Schreier families, because the function f_ϕ is not a polynomial. However, Mestre's curves are the most general of the families. The cyclotomic families result when the curve E in Mestre's construction degenerates to a singular cubic: that is, when the elliptic curve J_E is replaced by the multiplicative group $\mathbb{G}_n$. Indeed, in this situation f_ϕ may be taken to be $D_n(u,1)$ (see Remark 2.5.6), yielding our families

of cyclotomic coverings. The Artin–Schreier families extend the cyclotomic families to the case where the characteristic of k is equal to n. Here, the hyperelliptic polynomial of X_n is not tame, and Theorem 6.3.3 does not apply. Similarly, the CM-curves of §6.4 complete the cyclotomic families where the Dickson parameter a is zero. In particular, the the endomorphism rings of the CM-curve family Jacobians have real multiplication by $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Chapter 8

Richelot correspondences

Throughout this chapter, X denotes a hyperelliptic curve of genus two, over a field k of characteristic not two. Let X have an affine plane model

$$X : v^2 = f_X(u) = \Pi_{i=1}^{6}(u - \alpha_i),$$

where the elements α_i may lie in some extension of k. The hyperelliptic cover $h_X : X \to \mathbb{P}^1$ ramifies at six points $\omega_i := (\alpha_i, 0)$ of $X(\overline{k})$; these ramification points are *Weierstrass* points of the curve X.

In this chapter we will describe the theory of Richelot isogenies, which split multiplication by two on Jacobians of genus two curves. A beautiful exposition of the classical theory over the real numbers may be found in Bost & Mestre [5]. See Cassels & Flynn [11, Chapter 9] for a treatment over an arbitrary base field. For our treatment, we introduce *quadratic splittings*, a data structure relating Richelot isogenies to factorizations of hyperelliptic polynomials. Quadratic splittings allow us to work easily with the full set of Richelot isogenies from J_X, rather than restricting our attention to a single Richelot isogeny as in [5] and [11]; we will make use of this in the next chapter, where we study part of the graph of Richelot isogenies.

8.1 $(2,2)$-subgroups and $(2,2)$-isogenies

In this section, we will describe the isogenies whose kernel are contained in the two-torsion subgroup $J_X[2]$.

Lemma 8.1.1. *Let R be a proper, nontrivial subgroup of $J_X[2]$. If R is the kernel of an isogeny of principally polarised abelian surfaces, then R is a maximal 2-Weil-isotropic subgroup of $J_X[2]$ (that is, the 2-Weil pairing restricts trivially to R, and R is not properly contained in any other such subgroup).*

Proof. The statement follows from Milne [45, Proposition 16.8]; see the footnote on page 88 of Cassels & Flynn [11]. □

It follows from the nondegeneracy of the Weil pairing that the maximal 2-Weil isotropic subgroups of $J_X[2]$ are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Lemma 8.1.1 therefore implies that if A is a principally polarised abelian surface, and if $\phi : J_X \to A$ is an isogeny respecting the polarisations such that the kernel of ϕ is a proper, nontrivial subgroup of $J_X[2]$, then ϕ is a $(2,2)$-isogeny. We call the kernels of $(2,2)$-isogenies $(2,2)$-*subgroups*.

Remark 8.1.2. The homomorphism induced by a $(2,2)$-correspondence may not be a $(2,2)$-isogeny. For example, $2\Delta_X$ is a $(2,2)$-correspondence, but $\phi_{2\Delta_X} = [2]_{J_X}$, which is a $(2,2,2,2)$-isogeny.

Lemma 8.1.3. *Each nonzero element of $J_X[2]$ may be uniquely represented by a pair of distinct Weierstrass points of X.*

Proof. (Cf. Cassels & Flynn [11, §1.2, §8.1].) Let $P_{i,j} = (\alpha_i, 0) - (\alpha_j, 0)$. Now, $P_{i,j}$ is not the divisor of a function on X, so its image in J_X is nonzero; but $2P_{i,j} = \operatorname{div}((u-\alpha_i)/(u-\alpha_j))$, so $[2P_{i,j}] = 2[P_{i,j}] = 0$, and thus the image of $P_{i,j}$ in J_X is a nonzero element of $J_X[2]$. Now $P_{i,j} = -P_{i,j}$ by definition, and by the above $-[P_{i,j}] = [P_{j,i}]$; so $[P_{i,j}]$ is determined by the unordered pair $\{i,j\}$. It is easily verified that $P_{i,j} + P_{k,l}$ is principal if and only if $\{i,j\} = \{k,l\}$; so each pair $\{i,j\}$ uniquely specifies an element of $J_X[2]$. Indeed, there are $2^{2g_X} - 1 = 15$ nonzero elements of $J_X[2]$, and there are

$\binom{6}{2} = 15$ pairs of distinct Weierstrass points of X; so every nonzero element of $J_X[2]$ is specified by a pair $\{i, j\}$. □

Every rational linear factor $a(u-\alpha_i)$ of f_X specifies a rational Weierstrass point ω_i of X. Each rational quadratic factor $a(u-\alpha_i)(u-\alpha_j)$ of f_X specifies a rational pair[1] of Weierstrass points, ω_i and ω_j, and hence a rational element $[P_{i,j}]$ of $J_X[2]$. Therefore, subsets of $J_X[2]$ may be represented by sets of quadratic factors of f_X. To determine which sets of quadratic factors correspond to $(2,2)$-subgroups of $J_X[2]$, we must first express the 2-Weil pairing of points of $J_X[2]$ in terms of their quadratic representatives.

Lemma 8.1.4. *Let P and Q be distinct nonzero elements of $J_X[2]$, represented by quadratic factors G_P and G_Q of f_X, respectively. Then the 2-Weil pairing $e_2(P,Q)$ of P and Q is trivial if and only if G_P and G_Q are coprime.*

Proof. Suppose $P = (\alpha_i, 0) - (\alpha_j, 0)$ and $Q = (\alpha_k, 0) - (\alpha_l, 0)$, with $i \neq j$ and $k \neq l$. Then $G_P = (u-\alpha_i)(u-\alpha_j)$ and $G_Q = (u-\alpha_k)(u-\alpha_l)$. Now, $2P = \mathrm{div}(f_P)$ and $2Q = \mathrm{div}(f_Q)$, where $f_P = (u-\alpha_i)/(u-\alpha_j)$ and $f_Q = (u-\alpha_k)/(u-\alpha_l)$. We have

$$e_2(P,Q) = f_P(Q)/f_Q(P) = \frac{(\alpha_k-\alpha_i)}{(\alpha_k-\alpha_j)}\frac{(\alpha_l-\alpha_j)}{(\alpha_l-\alpha_i)}\frac{(\alpha_i-\alpha_l)}{(\alpha_i-\alpha_k)}\frac{(\alpha_j-\alpha_k)}{(\alpha_j-\alpha_l)}.$$

If G_P and G_Q are coprime, then i, j, k and l are all distinct, and the expression above reduces to $e_2(P,Q) = 1$. On the other hand, if G_P and G_Q are not coprime, then without loss of generality we may take $l = j$; we assumed $P \neq Q$, so we also take $i \neq k$. The expression above then becomes

$$e_2(P,Q) = \frac{(\alpha_k-\alpha_i)(\alpha_i-\alpha_j)(\alpha_j-\alpha_k)}{(\alpha_j-\alpha_i)(\alpha_i-\alpha_k)(\alpha_k-\alpha_j)} = -1.$$

□

Lemma 8.1.4 implies that the $(2,2)$-subgroups of $J_X[2]$ may be repre-

[1]Recall that a rational pair of points is a Galois-stable pair of points; the points need not be rational themselves. Similarly, α_i and α_j need not elements of k for the quadratic polynomial $a(u-\alpha_i)(u-\alpha_j)$ to be k-rational.

sented by sets of three pairwise coprime quadratic factors of f_X. We introduce *quadratic splittings* to formalise this connection.

8.2 Quadratic splittings

Let $k[u]_2$ denote the k-vector space of polynomials of degree at most two, with a Lie algebra structure given by the bracket

$$[f, g] := \frac{df}{du} \cdot g - \frac{dg}{du} \cdot f.$$

Observe that $[f, g] = -[g, f]$, and $[\alpha f + \beta g, h] = \alpha[f, h] + \beta[g, h]$ for all f, g and h in $k[u]_2$ and all α and β in k.

We define a map $\det : k[u]_2^3 \longrightarrow k$ as follows: if $G = (G_1, G_2, G_3)$ is an element of $k[u]_2^3$, with $G_i = g_{i,3}u^2 + g_{i,2}u + g_{i,1}$ for $1 \leq i \leq 3$, then we set

$$\det(G) := \det(g_{i,j}).$$

We also define a map $\Pi : k[u]_2^3 \longrightarrow k[u]$ by

$$\Pi(G_1, G_2, G_3) := G_1 G_2 G_3.$$

If f_X is the hyperelliptic polynomial of a curve X of genus two, then $\Pi^{-1}(f_X)$ is the set of ordered factorizations of f_X into three polynomials of degree at most two. Note that every such factorization is comprised of either three quadratics or two quadratics and one linear polynomial. Henceforward, we adopt the convention that linear polynomials are viewed as quadratics with one root "at infinity". Each element of $\Pi^{-1}(f_X)$ therefore represents a partition of the Weierstrass points of X into pairs, and hence specifies a $(2, 2)$-subgroup of $J_X[2]$.

Definition 8.2.1. Let $\mathcal{H}$ denote the set of all hyperelliptic polynomials of genus two curves over k:

$$\mathcal{H} := \{f \in k[u] : \deg f \in \{5, 6\}, f \text{ is squarefree } \}.$$

We define the set of *quadratic splittings* to be

$$\mathcal{S} := (\Pi^{-1}(\mathcal{H}))/\sim,$$

where $\sim$ is the equivalence relation defined by

$$(G_1, G_2, G_3) \sim (G_2, G_3, G_1) \sim (G_3, G_1, G_2)$$

and

$$(G_1, G_2, G_3) \sim (\alpha G_1, \beta G_2, \gamma G_3)$$

for all α, β and γ in $k^\times$ such that $\alpha\beta\gamma = 1$. We denote the image of an element G in $\mathcal{S}$ by $[G]$.

Proposition 8.2.2. *The maps* $\Pi : k[u]_2^3 \to k[u]$ *and* $\det : k[u]_2^3 \to k$ *induce well-defined maps*

$$\Pi : \mathcal{S} \longrightarrow \mathcal{H}$$

and

$$\det : \mathcal{S} \longrightarrow k.$$

Proof. Checking the compatibility of Π and det with the equivalence relations for quadratic splittings is an exercise in elementary algebra. □

For each polynomial f in $\mathcal{H}$, we define the set of *quadratic splittings of* f to be $\mathcal{S}_f := \Pi^{-1}(f)$. Each quadratic splitting G is an element of $\mathcal{S}_{\Pi(G)}$; thus the set $\mathcal{S}$ of all quadratic splittings may be viewed as a family of disjoint sets $\mathcal{S}_f$ parametrised by $\mathcal{H}$.

We define an involution $\nu : \mathcal{S} \to \mathcal{S}$ called *negation* by

$$\nu([(G_1, G_2, G_3)]) = [(G_1, G_3, G_2)];$$

we call $\nu(G)$ the *negative* of G. Clearly $\Pi(\nu(G)) = \Pi(G)$, so negation stabilises each subset $\mathcal{S}_f$ of $\mathcal{S}$. The quotient of $\mathcal{S}_f$ by $\langle\nu\rangle$ is denoted $|\mathcal{S}_f|$. If G is a quadratic splitting of f, then we denote its image in $|\mathcal{S}_f|$ by $|G|$, and call $|G|$ an *unsigned quadratic splitting* of f. No quadratic splitting is its own

negative, so every unsigned quadratic splitting corresponds to precisely two quadratic splittings.

Quadratic splittings, signed and unsigned, are the fundamental data structures of the remainder of this document. We will see that the unsigned quadratic splittings of f_X are in bijection with the rational $(2,2)$-subgroups of $J_X[2]$, while the quadratic splittings of f_X specify rational $(2,2)$-isogenies from J_X to principally polarised abelian surfaces.

Proposition 8.2.3. *Let $X : v^2 = f_X(u)$ be a curve of genus two. The rational $(2,2)$-subgroups of $J_X[2]$ are in bijection with the unsigned quadratic splittings of f_X.*

Proof. Each $(2,2)$-subgroup R of $J_X[2]$ has three nonzero elements P_1, P_2 and P_3; each element P_i corresponds to a quadratic factor G_{P_i} of f_X, which is unique up to scalar multiples. Lemma 8.1.4 implies R is 2-Weil isotropic if and only if the polynomials G_{P_i} are pairwise coprime, if and only if $G_{P_1}G_{P_2}G_{P_3} = cf_X$ for some c in $k^\times$; taking $c = 1$ (or dividing G_{P_3} by c), we have a uniquely determined pair $[(G_{P_1}, G_{P_2}, G_{P_3})]$, $[(G_{P_1}, G_{P_3}, G_{P_2})]$ of quadratic splittings of f_X, which are each other's negatives; that is, we have a uniquely determined unsigned quadratic splitting $|[(G_{P_1}, G_{P_2}, G_{P_3})]|$. □

Each quadratic splitting therefore specifies the kernel of an isogeny to a principally polarised abelian surface, which may be either the Jacobian of a genus two curve or the product of two elliptic curves. In fact, the type of the codomain of the isogeny may be deduced from the determinant of the quadratic splitting.

Definition 8.2.4. Suppose G is a quadratic splitting. If $\det(G) = 0$, then we say G is *singular*; otherwise, we say G is *nonsingular*. We denote the set of nonsingular quadratic splittings by $\mathcal{S}^{\mathrm{ns}}$, and the set of nonsingular quadratic splittings of f by $\mathcal{S}_f^{\mathrm{ns}}$.

We will see in §8.3 that singular quadratic splittings specify isogenies to products of elliptic curves. In §8.4, we show that nonsingular quadratic splittings specify $(2,2)$-isogenies to Jacobians.

It is easily verified that $\mathcal{S}^{\mathrm{ns}}$ is closed under negation: for all quadratic splittings G we have $\det(\nu(G)) = -(\det(G))$, so $\det(G) \neq 0$ if and only if $\det(\nu(G)) \neq 0$. Further, $\Pi(\nu(G)) = \Pi(G)$, so $\mathcal{S}_f^{\mathrm{ns}}$ is closed under negation for each f in $\mathcal{H}$.

Example 8.2.5. Let $k = \mathbb{F}_{83}$, and let X be the curve of genus two over k defined by

$$X : v^2 = f_X(u) = 24u^6 + 61u^5 + 48u^4 + 64u^3 + 14u^2 + 65u + 21.$$

Let

$$\begin{aligned}
g_1 &= 24u^2 + 52u + 74 \\
g_2 &= u^2 + 6u + 5 = (u+1)(u+5) \\
g_3 &= u^2 + 23u + 22 = (u+1)(u+22) \\
g_4 &= u^2 + 46u + 45 = (u+1)(u+45) \\
g_5 &= u^2 + 27u + 27 = (u+5)(u+22) \\
g_6 &= u^2 + 50u + 59 = (u+5)(u+45), \text{ and} \\
g_7 &= u^2 + 67u + 77 = (u+22)(u+45).
\end{aligned}$$

The set of quadratic splittings of f_X is

$$\mathcal{S}_{f_X} = \left\{ \begin{array}{c} [(g_1, g_2, g_7)], [(g_1, g_7, g_2)], \\ [(g_1, g_3, g_6)], [(g_1, g_6, g_3)], \\ [(g_1, g_4, g_5)], [(g_1, g_5, g_4)] \end{array} \right\}.$$

Computing determinants, we find

$$\begin{aligned}
&\det([(g_1, g_2, g_7)]) = 0, \quad &&\det([(g_1, g_7, g_2)]) = 0, \\
&\det([(g_1, g_3, g_6)]) = 66, \quad &&\det([(g_1, g_6, g_3)]) = -66, \\
&\det([(g_1, g_4, g_5)]) = 71, \quad &&\det([(g_1, g_5, g_4)]) = -71.
\end{aligned}$$

Therefore $[(g_1, g_2, g_7)]$ and $[(g_1, g_7, g_2)]$ are singular, and

$$\mathcal{S}_{f_X}^{\mathrm{ns}} = \{[(g_1, g_3, g_6)], [(g_1, g_6, g_3)], [(g_1, g_4, g_5)], [(g_1, g_5, g_4)]\}.$$

8.3 Singular quadratic splittings

By definition, the determinant of a quadratic splitting $G = [(G_1, G_2, G_3)]$ vanishes precisely when the polynomials G_1, G_2 and G_3 are k-linearly dependent. As this is a rather special situation, it is natural to ask is what this implies for the $(2,2)$-subgroup specified by G. We will see that G is singular precisely when G specifies the kernel of a $(2,2)$-isogeny to a product of elliptic curves. Further, a linear dependency between G_1, G_2 and G_3 allows us to explicitly construct the elliptic curves (cf. Flynn and Cassels [11, §14.1]).

Let X be a curve of genus two with an affine plane model $X : v^2 = f_X(u)$, and suppose $G = [(G_1, G_2, G_3)]$ is a singular quadratic splitting of f_X. Since $\det(G) = 0$, the polynomials G_1, G_2 and G_3 are k-linearly dependent.

Since G_1 and G_2 are elements of $k[u]_2$, we may construct a pair of linear polynomials $x_1 = (u - s_1)$ and $x_2 = (u - s_2)$, together with elements $a_{1,1}$, $a_{1,2}$, $a_{2,1}$ and $a_{2,2}$ of k such that $G_1 = a_{1,1}x_1^2 + a_{1,2}x_2^2$ and $G_2 = a_{2,1}x_1^2 + a_{2,2}x_2^2$. To see that x_1 and x_2 exist, consider the polynomial $g_\alpha = G_1 + \alpha G_2$, for α in k: the discriminant of g_α is a quadratic in α, with two distinct roots α_1 and α_2. Up to units, we have $x_1^2 = G_1 + \alpha_1 G_2$ and $x_2^2 = G_1 + \alpha_2 G_2$. Now G_3 is a linear combination of G_1 and G_2, hence a linear combination of x_1^2 and x_2^2; so there exist $a_{3,1}$ and $a_{3,2}$ in k such that $G_3 = a_{3,1}x_1^2 + a_{3,2}x_2^2$.

Given these expressions for G_1, G_2 and G_3 in terms of x_1 and x_2, we may write our model of X in the form

$$X : v^2 = G_1 G_2 G_3 = \prod_{i=1}^{3} (a_{i,1}x_1^2 + a_{i,2}x_2^2).$$

If E_1 and E_2 are the two (possibly identical) curves of genus one defined by

$$E_1 : v^2 = \prod_{i=1}^{3} (a_{i,1}u + a_{i,2}) \quad \text{and} \quad E_2 : v^2 = \prod_{i=1}^{3} (a_{i,1} + a_{i,2}u),$$

then there are distinct coverings $\psi_1 : X \to E_1$ and $\psi_2 : X \to E_2$ of degree two, defined by

$$\psi_:(u, v) \mapsto ((x_1/x_2)^2, v/x_2^3) \quad \text{and} \quad \psi_2 : (u, v) \mapsto ((x_2/x_1)^2, v/x_1^3),$$

respectively. The following proposition shows that J_X is isogenous to the product $J_{E_1} \times J_{E_2}$.

Proposition 8.3.1. *Let X be a curve of genus two. If there exists a singular quadratic splitting G of f_X, then J_X is $(2,2)$-isogenous to a product of elliptic curves.*

Proof. Given X and G, construct the curves E_1 and E_2 and covers $\psi_1 : X \to E_1$ and $\psi_2 : X \to E_2$ as in the discussion above. The abelian surface J_X has one-dimensional abelian subvarieties $\psi_1^*(J_{E_1})$ and $\psi_2^*(J_{E_2})$, so J_X is not simple; therefore, J_X is a product of elliptic curves.

We have homomorphisms $(\psi_1)_* : J_X \to J_{E_1}$ and $(\psi_2)_* : J_X \to J_{E_2}$, so the elliptic curves J_{E_1} and J_{E_2} are isogeny factors of J_X. The two-torsion subgroup $J_{E_1}[2]$ of E_1 is generated by differences of the points $P_i = (-a_{i,2}/a_{i,1}, 0)$ for $1 \leq i \leq 3$. Now, $\psi_1^{-1}(P_i) = \{(r_i, 0), (r_i', 0)\}$, where r_i and r_i' are the roots of the polynomial G_i. Therefore, the element $[(r_i, 0) - (r_j, 0)]$ of $J_X[2]$ maps to $[P_i - P_j]$ in $J_{E_1}[2]$; this image is zero if and only if $i = j$. The same argument holds for $(\psi_2)_*$; so the kernel of the map $(\psi_1)_* \times (\psi_2)_* : J_X \to E_1 \times E_2$ is precisely the subgroup specified by $|G|$. □

The $(2,2)$-subgroup of $J_X[2]$ specified by $|G|$ is the image in J_X of both $J_{E_1}[2]$ and $J_{E_2}[2]$. Therefore, J_X is the product of J_{E_1} and J_{E_2}, glued along their two-torsion subgroups — which are necessarily isomorphic.

Example 8.3.2. Let k and X be as in Example 8.2.5: that is, $k = \mathbb{F}_{83}$, and

$$X : v^2 = f_X(u) = 24u^6 + 61u^5 + 48u^4 + 64u^3 + 14u^2 + 65u + 21.$$

Recall that the splitting

$$G := [(g_1, g_2, g_7)] = \left[(24u^2 + 52u + 74, u^2 + 6u + 5, u^2 + 67u + 77)\right]$$

of f_X is singular; we find $g_1 = -33g_6 - 26g_7$. Let $x_1 := (u - 1)$ and $x_2 := (u + 2)$; then $g_2 = 55x_1^2 + 29x_2^2$ and $g_7 = 31x_1^2 + 53x_2^2$, so $g_1 = 35x_1^2 + 72x_2^2$.

Therefore, let E_1 and E_2 be the curves of genus one defined by

$$\begin{aligned} E_1 : v^2 &= (72+35u)(29+55u)(53+31u) \\ &= 81u^3 + 29u^2 + 55u + 25 \end{aligned}$$

and

$$\begin{aligned} E_2 : v^2 &= (35+72u)(55+29u)(31+53u) \\ &= 25u^3 + 55u^2 + 29u + 81; \end{aligned}$$

we have covers $\psi_1 : X \to E_1$ and $\psi_2 : X \to E_2$ defined by

$$\psi_1(u,v) = (((u-1)/(u+2))^2, v/(u+2))$$

and

$$\psi_2(u,v) = (((u+2)/(u-1))^2, v/(u-1)),$$

and hence an isogeny $(\psi_1 \times \psi_2)_* : J_X \to J_{E_1} \times J_{E_2}$.

8.4 Richelot correspondences

We now turn our attention to nonsingular quadratic splittings. For every nonsingular quadratic splitting, we construct a $(2,2)$-isogeny of Jacobians of genus two curves. The construction of the isogenous Jacobian is due to Richelot [51, 50]. To express Richelot's construction in terms of quadratic splittings, we define the *Richelot operator*.

Definition 8.4.1. We define the *Richelot operator*

$$\mathcal{R} : \{G \in k[u]_2^3 : \det(G) \neq 0\} \longrightarrow k[u]_2^3$$

by

$$\mathcal{R}((G_1, G_2, G_3)) := (\delta[G_2, G_3], \delta[G_3, G_1], \delta[G_1, G_2]),$$

where $\delta = (\det(G_1, G_2, G_3))^{-1}$.

The following series of results shows that our Richelot operator induces an involution on nonsingular quadratic splittings.

Lemma 8.4.2. *Suppose G_1, G_2, and G_3 are polynomials in $k[u]_2$, such that $\det(G_1, G_2, G_3) \neq 0$ and $\Pi(G_1, G_2, G_3)$ is a polynomial of degree five or six. Then $\Pi(\mathcal{R}((G_1, G_2, G_3)))$ is a squarefree polynomial of degree five or six.*

Proof. Let $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. Comparing the discriminant of H_1 with the resultant of G_2 and G_3, we find that H_1 is squarefree; similarly, H_2 and H_3 are squarefree. Comparing the resultant of H_1 and H_2 with the discriminant of G_3, we find that H_1 and H_2 are coprime; similarly, H_3 is coprime to H_2 and H_1. Hence $\Pi(\mathcal{R}((G_1, G_2, G_3))) = H_1H_2H_3$ is squarefree. It remains to check that the degree of $H_1H_2H_3$ is five or six — that is, that at most one of the H_i has degree less than two. It is easy to see that $[G_1, G_2]$ is constant if and only if $G_1 = G_2$, which contradicts $\det(G_1, G_2, G_3) \neq 0$. Thus we must show that at most one of the H_i is linear. The bracket is k-bilinear, so it is enough to check the case where G_1, G_2 and G_3 are monic. If one of the G_i is linear, then two of the H_j are brackets of linear and quadratic polynomials, which must be quadratic: $[u+c, u^2+au+b] = u^2+2cu+(ac-b)$. Therefore, we may suppose that G_1, G_2 and G_3 are monic quadratics. If a_i denotes the coefficient of u in G_i, then the coefficients of u^2 in H_1 and H_2 are $a_3 - a_2$ and $a_1 - a_3$ respectively. Therefore, if H_1 and H_2 are both linear, then $a_1 = a_2 = a_3$; but this contradicts $\det(G_1, G_2, G_3) \neq 0$. Hence $H_1H_2H_3$ is a squarefree polynomial of degree five or six. □

Lemma 8.4.3. *Suppose G_1, G_2, and G_3 are polynomials in $k[u]_2$, such that $\det(G_1, G_2, G_3) \neq 0$ and $\Pi(G_1, G_2, G_3)$ is a polynomial of degree five or six. Let $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. The following identities hold:*

1. *$\mathcal{R}((\alpha G_1, \beta G_2, \gamma G_3)) = (\alpha^{-1}H_1, \beta^{-1}H_2, \gamma^{-1}H_3)$ for all $\alpha, \beta, \gamma \in k^\times$;*
2. *$\mathcal{R}((G_2, G_3, G_1)) = (H_2, H_3, H_1)$ and $\mathcal{R}((G_3, G_1, G_2)) = (H_3, H_1, H_2)$;*
3. *$\mathcal{R}((H_1, H_2, H_3)) = (G_1, G_2, G_3)$;*
4. *$\det(H_1, H_2, H_3) = 2/\det(G_1, G_2, G_3)$; and*
5. *$\sum_{i=1}^{3} G_i(u_1)H_i(u_2) + (u_1 - u_2)^2 = 0$.*

Proof. Each identity is readily verified by explicit computation. □

We are now ready to prove that the Richelot operator induces an involution on the set of nonsingular quadratic splittings.

Proposition 8.4.4. *The Richelot operator induces a well-defined involution*

$$\mathcal{R}(\cdot) : \mathcal{S}^{\text{ns}} \longrightarrow \mathcal{S}^{\text{ns}}$$

on nonsingular quadratic splittings.

Proof. Suppose G is a nonsingular quadratic splitting; choose a representative (G_1, G_2, G_3) in $k[u]_2^3$ for G. By Lemma 8.4.2, $\Pi(\mathcal{R}((G_1, G_2, G_3)))$ is in $\mathcal{H}$, so $[\mathcal{R}((G_1, G_2, G_3))]$ is a quadratic splitting. We check that $[\mathcal{R}((G_1, G_2, G_3))]$ is independent of the choice of representative (G_1, G_2, G_3) for G. For notational convenience, set $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. Identity (1) of Lemma 8.4.3 imples that for all α, β and γ in k such that $\alpha\beta\gamma = 1$, we have

$$\begin{aligned}[\mathcal{R}((\alpha G_1, \beta G_2, \gamma G_3))] &= [(\alpha^{-1}H_1, \beta^{-1}H_2, \gamma^{-1}H_3)] \\ &= [(H_1, H_2, H_3)] \\ &= [\mathcal{R}((G_1, G_2, G_3))],\end{aligned}$$

since $\det(\alpha^{-1}H_1, \beta^{-1}H_2, \gamma^{-1}H_3) = \det(H_1, H_2, H_3)$; identity (2) of Lemma 8.4.3 implies $[\mathcal{R}((G_2, G_3, G_1))] = [\mathcal{R}((G_1, G_2, G_3))]$. Hence the Richelot operator takes representatives of the same splitting to representatives of the same splitting. Identity (4) of Lemma 8.4.3 shows that $[\mathcal{R}((G_1, G_2, G_3))]$ is nonsingular, so we have a well-defined map $\mathcal{R}(\cdot) : \mathcal{S}^{\text{ns}} \longrightarrow \mathcal{S}^{\text{ns}}$; identity (3) of Lemma 8.4.3 shows that $\mathcal{R}(\mathcal{R}(G)) = G$, so $\mathcal{R}(\cdot)$ is in fact an involution on $\mathcal{S}^{\text{ns}}$. □

Remark 8.4.5. The Richelot operator does *not* induce a well-defined map on singular quadratic splittings, since it is not defined for their representatives in $k[u]_2^3$.

Definition 8.4.6. Let $X : v^2 = f_X(u)$ be a curve of genus two. For each nonsingular quadratic splitting G of f_X, we define X_G to be the curve given by

$$X_G : v^2 = f_{X_G}(u) := \Pi(\mathcal{R}(G)).$$

Lemma 8.4.2 implies that X_G is a curve of genus two. Observe that $\mathcal{R}(G)$ is a nonsingular quadratic splitting of f_{X_G}, and that $(X_G)_{\mathcal{R}(G)} = X$.

We may combine Lemma 8.4.2 with the fifth identity of Lemma 8.4.3 to produce a correspondence on $X \times X_G$. Let (G_1, G_2, G_3) be a representative in $k[u]_2^3$ for G, let $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$, and let $F = G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2)$. The last identity of Lemma 8.4.3 implies

$$f_X(u_1)f_{X_G}(u_2) \equiv G_1(u_1)^2 H_1(u_2)^2 (u_1 - u_2)^2 \pmod{F}.$$

Thus on $X \times X_G$ we have

$$\begin{aligned} V(F) &= V(F, v_1^2 v_2^2 - f_X(u_1)f_{X_G}(u_2)) \\ &= V(F, v_1^2 v_2^2 - G_1(u_1)^2 H_1(u_2)^2 (u_1 - u_2)^2) \\ &= C + C^-, \end{aligned}$$

where

$$C = V(F, v_1 v_2 - G_1(u_1)H_1(u_2)(u_1 - u_2))$$

and

$$C^- = V(F, v_1 v_2 + G_1(u_1)H_1(u_2)(u_1 - u_2)).$$

Note that $V(F) \approx 0$, since it is the pullback via $h_{X \times X_G}$ of the correspondence $V(F)$ on $\mathbb{P}^1 \times \mathbb{P}^1$; so $C^- \approx -C$.

Now, let us compute the correspondence pairing on C and C^-. First, $\langle C, C^- \rangle = 8 - C.C^-$, and direct calculation shows that $C.C^- = 16$, so

$$\left\langle C, C^- \right\rangle = -8.$$

Now $\langle C, C \rangle = -\langle C, C^- \rangle = \langle C^-, C^- \rangle$, so

$$\langle C, C \rangle = \left\langle C^-, C^- \right\rangle = 8.$$

These pairing values will be useful in distinguishing the homomorphic equivalence classes of correspondences on $X \times X_G$ constructed in such a way.

Definition 8.4.7. Let X be a curve of genus two, and let G be a nonsingular

quadratic splitting of f_X. For each representative (G_1, G_2, G_3) in $k[u]_2^3$ for G, we define a correspondence $C_{(G_1,G_2,G_3)}$ on $X \times X_G$ by

$$C_{(G_1,G_2,G_3)} := V\begin{pmatrix} G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2), \\ v_1v_2 - G_1(u_1)H_1(u_2)(u_1 - u_2) \end{pmatrix},$$

where $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. We say that $C_{(G_1,G_2,G_3)}$ is a *Richelot correspondence for* G.

Suppose $G = [(G_1, G_2, G_3)]$ is a nonsingular quadratic splitting. Now $C_{(G_1,G_2,G_3)} \neq C_{(G_2,G_3,G_1)}$, so we cannot associate a unique Richelot correspondence to G. The following proposition shows that all of the Richelot correspondences for G are in the same homomorphic equivalence class; hence we may associate to G a unique homomorphism from J_X to J_{X_G}.

Proposition 8.4.8. *If G is a nonsingular quadratic splitting, then all of the Richelot correspondences for G are homomorphically equivalent.*

Proof. Let (G_1, G_2, G_3) be a representative in $k[u]_2^3$ for G. The Richelot correspondence $C_{(G_1,G_2,G_3)}$ is defined by

$$C_{(G_1,G_2,G_3)} = V\begin{pmatrix} G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2), \\ v_1v_2 - G_1(u_1)H_1(u_2)(u_1 - u_2) \end{pmatrix}.$$

Take α, β and γ in k such that $\alpha\beta\gamma = 1$; then $[(\alpha G_1, \beta G_2, \gamma G_3)] = G$. Now $\mathcal{R}((\alpha G_1, \beta G_2, \gamma G_3)) = (\alpha^{-1}H_1, \beta^{-1}H_2, \gamma^{-1}H_3)$, by the first identity of Lemma 8.4.3, so

$$\begin{aligned} C_{(\alpha G_1,\beta G_2,\gamma G_3)} &= V\begin{pmatrix} \alpha G_1(u_1)\alpha^{-1}H_1(u_2) + \beta G_2(u_1)\beta^{-1}H_2(u_2), \\ v_1v_2 - \alpha G_1(u_1)\alpha^{-1}H_1(u_2)(u_1 - u_2) \end{pmatrix} \\ &= V\begin{pmatrix} G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2), \\ v_1v_2 - G_1(u_1)H_1(u_2)(u_1 - u_2) \end{pmatrix} \\ &= C_{(G_1,G_2,G_3)}. \end{aligned}$$

It remains to show that $C_{(G_1,G_2,G_3)} = C_{(G_2,G_3,G_1)} = C_{(G_3,G_1,G_2)}$. Recall that

$\left\langle C_{(G_1,G_2,G_3)}, C_{(G_1,G_2,G_3)} \right\rangle = 8$. Direct calculation shows that

$$\left\langle C_{(G_1,G_2,G_3)}, C_{(G_2,G_3,G_1)} \right\rangle = -8;$$

hence $\left\langle C_{(G_1,G_2,G_3)} - C_{(G_2,G_3,G_1)}, C_{(G_1,G_2,G_3)} - C_{(G_2,G_3,G_1)} \right\rangle = 0$, and therefore $C_{(G_1,G_2,G_3)} \approx C_{(G_2,G_3,G_1)}$. Similarly, $C_{(G_1,G_2,G_3)} \approx C_{(G_3,G_1,G_2)}$. □

Corollary 8.4.9. *There is a well-defined homomorphism $\rho_G : J_X \to J_{X_G}$ for every nonsingular quadratic splitting G of f_X. If $G = [(G_1, G_2, G_3)]$, then $\rho_G = \phi_{C_{(G_1,G_2,G_3)}}$.*

Definition 8.4.10. If G is a nonsingular quadratic splitting, then we call the homomorphism ρ_G of Corollary 8.4.9 the *Richelot isogeny* of G.

Of course, we must show that Richelot isogenies are indeed isogenies. The following theorem shows that the kernel of a Richelot isogeny ρ_G is in fact the $(2,2)$-subgroup specified by the unsigned quadratic splitting $|G|$.

Theorem 8.4.11. *Let $X : v^2 = f_X(u)$ be a curve of genus two. If G is a nonsingular quadratic splitting of f_X, then $\rho_G : J_X \to J_{X_G}$ is a $(2,2)$-isogeny, and the kernel of ρ_G is the $(2,2)$-subgroup specified by $|G|$. Further, $\rho_G(J_X[2])$ is the $(2,2)$-subgroup of J_{X_G} specified by $|\mathcal{R}(G)|$.*

Proof. Fix a representative (G_1, G_2, G_3) for G in $k[u]_2^3$, and let $i : X_G \to X'_G$ be the isomorphism defined by $i(u, v) = (u, \det(G)v)$. The homomorphism $i_* \circ \rho_G$ is identical to the classical Richelot isogeny of [11, §9.1, §9.2], and the Richelot correspondence $C_{(G_1,G_2,G_3)}$ is that of [11, §9.2] and [5, §3.3]. □

Proposition 8.4.12. *If G is a nonsingular quadratic splitting, then ${\rho_G}^\dagger = \rho_{\mathcal{R}(G)}$ and $\rho_{\nu(G)} = -\rho_G$.*

Proof. Suppose $G = [(G_1, G_2, G_3)]$, and set $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. Now $\mathcal{R}((H_1, H_2, H_3)) = (G_1, G_2, G_3)$ by the third identity of Lemma 8.4.3, so the Richelot correspondence for (H_1, H_2, H_3) is defined by

$$C_{(H_1,H_2,H_3)} = V \begin{pmatrix} H_1(u_1)G_1(u_2) + H_2(u_1)G_2(u_1), \\ v_1 v_2 - H_1(u_1)G_1(u_2)(u_1 - u_2) \end{pmatrix},$$

which is clearly the transpose of $C_{(G_1,G_2,G_3)}$; so $\rho_H = {\rho_G}^\dagger$ by Proposition 3.3.16. For the second assertion, note that $\nu(G) = [(G_2, G_1, G_3)]$. Direct calculation shows that $\left\langle C_{(G_1,G_2,G_3)}, C_{(G_2,G_1,G_3)} \right\rangle = -8$, which implies

$$\left\langle C_{(G_1,G_2,G_3)} + C_{(G_2,G_1,G_3)}, C_{(G_1,G_2,G_3)} + C_{(G_2,G_1,G_3)} \right\rangle = 0,$$

and thus $C_{(G_2,G_1,G_3)} \approx -C_{(G_1,G_2,G_3)}$; therefore $\rho_{\nu(G)} = -\rho_G$. Alternatively: $C_{(G_1,G_2,G_3)} + C_{(G_2,G_1,G_3)} = V(G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2))$, which is a homomorphically trivial correspondence, hence $\rho_{\nu(G)} = -\rho_G$. □

Example 8.4.13. As in Examples 8.2.5 and 8.3.2, let $k = \mathbb{F}_{83}$, and X the curve of genus two over k defined by

$$X : v^2 = f_X(u) = 24u^6 + 61u^5 + 48u^4 + 64u^3 + 14u^2 + 65u + 21.$$

Let

$$G = (24u^2 + 52u + 74, u^2 + 23u + 22, u^2 + 50u + 59);$$

we saw in Example 8.2.5 that $[G]$ is a nonsingular quadratic splitting of f_X. Set $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$; then

$$(H_1, H_2, H_3) = (26u^2 + 19u + 20, 35u^2 + 13u + 3, 5u^2 + 29u + 16).$$

If $X_{[G]}$ is the curve is defined by

$$X_{[G]} : v^2 = \Pi(\mathcal{R}(G)) = 68u^6 + 31u^5 + 51u^4 + 48u^3 + 80u^2 + 6u + 47,$$

then there is a Richelot isogeny $\rho_G : J_X \to J_{X_{[G]}}$ induced by the Richelot correspondence $C_{(G_1,G_2,G_3)}$ on $X \times X_G$. Note that $C_{(G_1,G_2,G_3)}$ is equal to

$$V\left(\begin{array}{c} u_1^2u_2^2 + 39u_1^2u_2 + 3u_1^2 + 50u_1u_2^2 + 58u_1u_2 + 77u_1 + 9u_2^2 + 60u_2 + 56, \\ v_1v_2 - 43(u_1^2 + 16u + 10)(u_2^2 + 55u + 71)(u_1 - u_2) \end{array} \right).$$

A particularly interesting feature of Richelot isogenies is that multiplication by two on Jacobians of genus two curves splits into a composition of Richelot isogenies. The following corollary makes this precise.

Corollary 8.4.14. *Let $\rho_G : J_X \to J_{X_G}$ be a Richelot isogeny. The isogenies ρ_G and ${\rho_G}^\dagger : J_{X_G} \to J_X$ factor multiplication-by-two:*

$$ {\rho_G}^\dagger \circ \rho_G = [2]_{J_X} \quad \textit{and} \quad \rho_G \circ {\rho_G}^\dagger = [2]_{J_{X_G}}. $$

Proof. The kernel of $\rho_G^\dagger$ is the image of the 2-torsion of J_X under ρ_G, by Theorem 8.4.11; so the kernel of ${\rho_G}^\dagger \circ \rho_G$ contains $J_X[2]$. On the other hand, ρ_G and ${\rho_G}^\dagger$ are both isogenies of degree four, so their composition is an isogeny of degree sixteen. But $J_X[2]$ is a group of order sixteen, so it must be the whole kernel; thus ${\rho_G}^\dagger \circ \rho_G = [2]_{J_X} \circ \alpha$, for some automorphism α of X. On the other hand, we know that ρ_G is the induced homomorphism of some Richelot correspondence C for G, and the self-pairing of C is 8. Therefore $\mathrm{Tr}({\rho_G}^\dagger \circ \rho_G) = 8$ by Theorem 5.3.3; but $\mathrm{Tr}(2\alpha) = 2\mathrm{Tr}(\alpha)$, so $\mathrm{Tr}(\alpha) = 4$. The norm $N_{\mathrm{End}(J_X)/\mathbb{Z}}(\alpha)$ of α is one, since α is an automorphism; we conclude that $\alpha = 1$. Therefore ${\rho_G}^\dagger \circ \rho_G = [2]_{J_X}$. Similarly, $\rho_G \circ \rho^\dagger = [2]_{J_{X_G}}$. □

The number of quadratic splittings of the hyperelliptic polynomial f_X of some curve X of genus two is determined by the number and the degree of the k-irreducible factors of f_X. If f_X has any irreducible factors of degree greater than two, then (by definition) there can be no quadratic splittings of f_X defined over k. Assume, then, that f_X is a product of linear and quadratic factors, with $2r$ linear factors over k. Then there are $(2r)!/(r!2^r)$ distinct factorizations of f_X into quadratics (up to units) over k, and so there are $(2r)!/(r!2^r)$ unsigned quadratic splittings. Every unsigned quadratic splitting corresponds to two quadratic splittings, so there must be $(2r)!/(r!2^{r-1})$ quadratic splittings of f_X. Table 8.1 describes the possible numbers of splittings.

8.5 Richelot endomorphisms

Suppose that we have a hyperelliptic curve X of genus two and a nonsingular quadratic splitting G of f_X such that there is an isomorphism $i : X_G \to X$. Corollary 8.4.14 tells us that the endomorphism $i_* \circ \rho_G$ splits multiplication-by-two on J_X; thus the subring $\mathbb{Z}[i_* \circ \rho_G]$ of $\mathrm{End}(J_X)$ is isomorphic to $\mathbb{Z}[\sqrt{2}]$.

Table 8.1: The number of quadratic splittings of f_X

Degrees of irreducible factors of f_X over k	$\#\mathcal{S}_{f_X}$	$\#\lvert\mathcal{S}_{f_X}\rvert$	$\#(2,2)$-subgroups of $J_X[2]$
$2,2,2$	2	1	1
$2,2,1,1$	2	1	1
$2,1,1,1,1$	6	3	3
$1,1,1,1,1,1$	30	15	15
(other)	0	0	0

The theory of Richelot endomorphisms has been thoroughly treated by Bending in his PhD thesis [3]. Bending constructs a family of curves of genus two such that the Jacobian of every member of the family has real multiplication by $\mathbb{Z}[\sqrt{2}]$. Further, he proves that every curve defined over the complex numbers whose Jacobian has real multiplication by $\mathbb{Z}[\sqrt{2}]$ is isomorphic to a member of this family. We state Bending's theorem below; see [3] for proof and applications.

Theorem 8.5.1 (Bending [3, Theorem 4.1]). *Let X be a curve of genus two over a subfield k of the complex numbers. Suppose that there exists an endomorphism ρ of J_X such that $\rho^\dagger = \rho$ and $\rho^2 - [2] = 0$. Then there exists some A and Q in k and P and Δ in $k^\times$, such that X is isomorphic over $\overline{k}$ to the curve $X_{P,Q,A,\Delta}$ defined by*

$$v^2 = \Delta \prod_{i=1}^{3} G_i(u)$$

with

$$G_i(u) := (u^2 - \alpha_i u + P\alpha_i^2 + Q\alpha_i + 4P),$$

where α_1, α_2 and α_3 are defined by

$$\prod_{i=1}^{3}(u - \alpha_i) = u^3 + Au^2 + \frac{Q(PA - Q) + 4P^2 + 1}{P^2}u + 4(A - \frac{Q}{P}).$$

Further, if $\psi : X \to X_{P,Q,A,\Delta}$ is the isomorphism and $G = [(G_1, G_2, G_3)]$,

then $\psi\rho\psi^{-1} = \pm\iota^{-1}\rho_G$*, where* $\iota : X_{P,Q,A,\Delta} \to (X_{P,Q,A,\Delta})_G$ *is the isomorphism defined by*

$$\iota(u, v) = \left(\frac{2}{u}, \frac{4\det(G)v}{u^3}\right).$$

Conversely, if k *is a field of characteristic not two, then for any* A *and* Q *in* k *and* P *and* Δ *in* $k^\times$ *the curve* $X_{P,Q,A,\Delta}$ *has an endomorphism acting as* $\sqrt{2}$*, given by* $\iota^{-1} \circ \rho_G$*.*

Cassels and Flynn give a brief construction of Richelot endomorphisms in [11]. If $G = [(G_1, G_2, G_3)]$ is a nonsingular quadratic splitting of f_X fixed by the Richelot operator (that is, $\mathcal{R}(G) = G$), then $X_G = X$, so ρ_G is an endomorphism of J_X splitting $[2]_{J_X}$; thus J_X has real multiplication by $\mathbb{Z}[\sqrt{2}]$. Cassels & Flynn derive conditions on the coefficients of G_1, G_2 and G_3 sufficient for this to occur: see [11, §15.1] for details.

Finally, Mestre gives a two-dimensional family of curves of genus two whose Jacobians have real multiplication by $\mathbb{Z}[\sqrt{2}]$ in [44, page 204]. These endomorphisms are not constructed as Richelot isogenies, but rather using the construction of §7.5 with an elliptic curve isogeny of degree 8.

8.6 Towards generalised Richelot isogenies

In his PhD thesis [36, §4.3], Kux describes a generalisation of the Richelot correspondence to hyperelliptic curves of higher genus. As in Richelot's construction, the starting point is a hyperelliptic curve X, defined by an affine plane model $v^2 = f_X(u)$, together with a factorization $f_X = G_1G_2G_3$ of the hyperelliptic polynomial of X, where the G_i are poloynomials of equal degree. For such a factorization to exist, we must have $\deg f_X \equiv 0 \pmod 3$; thus we immediately see that this construction only exists for curves X of genus $g_X \equiv 2 \pmod 3$. In particular, the first genus higher than two for which this construction might yield a generalised Richelot isogeny is five.

Kux derives a condition for the existence of a hyperelliptic curve X_G with an affine plane model $v^2 = f_{X_G}(u) = H_1H_2H_3(u)$ (where the H_i are polynomials of the same degree as the G_j), such that the correspondence

defined by

$$\overline{C} = V(G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2))$$

on $\mathbb{P}^1 \times \mathbb{P}^1$ lifts to a correspondence on $X \times X_G$ that has components that are not homomorphically trivial. Briefly, the condition is that there exist a polynomial P in $k[u_1, u_2]$ such that

$$G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2) + G_3(u_1)H_3(u_2) + P(u_1, u_2)^2 = 0;$$

this is an analogue of the final identity of Lemma 8.4.3. As in §8.4, we have $h^*_{X\times X_G}(\overline{C}) = C + C^-$, where C is the correspondence on $X \times X_G$ defined by

$$C = V\begin{pmatrix} G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2), \\ v_1v_2 - G_1(u_1)H_1(u_2)P_1(u_1, u_2), \end{pmatrix}$$

and $C^- \approx -C$.

On first inspection Kux's construction seems a natural generalisation of Richelot's. However, there is a crucial difference from the genus two case: the kernel of ϕ_C is *not* 2-Weil-isotropic, so ϕ_C is *not* an isogeny of principally polarised abelian varieties. The subgroup $J_X[2] \cap \ker \phi_C$ is generated by two elements (represented by the divisors cut out by G_1 and G_2, say.) If the genus of X is greater than two, then this subgroup cannot be maximally isotropic with respect to the 2-Weil pairing: it is simply not large enough. It follows that the homomorphism ϕ_C cannot split the multiplication-by-2 map on $\mathrm{End}(J_X)$ or $\mathrm{End}(J_{X_G})$. In fact, in the cases where Kux's criterion applies, J_X is reducible, with a factor isomorphic to the Jacobian $J_{\overline{X}}$ of some curve $\overline{X}$ of genus two. Kux's correspondence C on $X \times X_G$ induces a Richelot isogeny from $J_{\overline{X}}$ to $J_{\overline{X}_{\overline{G}}}$, for some quadratic splitting $\overline{G}$ of $f_{\overline{X}}$; the homomorphism ϕ_C extends this Richelot isogeny trivially to the rest of J_X.

As a first source of examples for this generalisation, Kux considers curves $X : v^2 = G_1G_2G_3(u)$ where the G_i are palindromic polynomials. These curves have an involution $\iota : X \to X$ defined by

$$iota : (u, v) \mapsto (1/u, v/u^{g_X+1}).$$

The Jacobian of any such X is reducible. The endomorphism ι_* is clearly not the identity, so $\iota_* - [1] \neq 0$; further, ι is not the hyperelliptic involution on X, so $\iota_* + [1] \neq 0$. However, $\iota_*^2 = [1]$, so $(\iota + [1])(\iota_* - [1]) = 0$. This implies that neither $(\iota + [1])$ nor $(\iota_* - [1])$ is an isogeny, so the connected components of their kernels are positive-dimensional abelian subvarieties of J_X; hence J_X is reducible.

A proper generalisation of Richelot correspondences to curves of higher genus should require the kernel of the induced homomorphism to be a maximal 2-Weil isotropic subgroup of the 2-torsion: then the induced homomorphism will split multiplication-by-two. In order to construct such homomorphisms from a hyperelliptic Jacobian J_X, one should consider factorizations

$$f_X = \prod_{i=1}^{g_X+1} G_i,$$

where each polynomial G_i is quadratic. Such a factorization specifies a maximal 2-Weil isotropic subgroup of $J_X[2]$, and hence the kernel of an isogeny to a principally polarised abelian variety of dimension g_X. However, when the genus of X is greater than three, there is no reason to expect the codomain of such an isogeny to be the Jacobian of a curve (see the footnote on page 104 of [11]); thus the isogeny may not be induced by any correspondence.

For generic curves of genus three, recent work of Lehavi and Ritzenthaler [41] provides an algorithm which, given a curve X and a maximal 2-Weil isotropic subgroup R of $J_X[2]$, constructs a curve Y such that there exists an isogeny $\rho : J_X \to J_Y$ with kernel R. However, the geometric arguments involved in the construction of [41] require a smooth plane quartic model of X, and so do not appear to carry over to hyperelliptic curves of genus three.

Chapter 9

Richelot isogeny cycle structures

In this chapter, we will use the theory of Richelot correspondences developed in Chapter 8 to construct explicit isogeny cycles of Jacobian surfaces. These generalise isogeny cycles of elliptic curves, which have a wide variety of applications. Satoh [53] and others have used them to compute canonical lifts of curves over finite fields. Kohel [35] uses isogeny cycles to determine elliptic curve endomorphism ring structure; Fouquet and Morain [20] use Kohel's techniques to improve the Schoof–Elkies–Atkin point counting algorithm described in [55], [54], [1], [2], [47], and [18].

9.1 Isogeny cycles and endomorphism rings

Consider a sequence of $n+1$ Jacobians, connected by a sequence of n isogenies, such that the last Jacobian is equal to the first:

$$J_0 \overset{\varphi_1}{\to} J_1 \overset{\varphi_2}{\to} J_2 \overset{\varphi_3}{\to} \cdots \overset{\varphi_{n-1}}{\to} J_{n-1} \overset{\varphi_n}{\to} J_n = J_0.$$

We call such a sequence an *isogeny cycle* of length n. Composing the isogenies in the cycle yields an endomorphism $\phi = \varphi_n \circ \cdots \circ \varphi_1$ of J_0. Similarly, we may compose the isogenies to obtain an endomorphism of each Jacobian in the cycle: $\varphi_{i+1} \circ \cdots \circ \varphi_n \circ \varphi_1 \circ \cdots \varphi_i$ is an endomorphism of J_i for $1 \leq i \leq n$.

For the remainder of this section, we fix a prime l. If each isogeny φ_i splits $[l]_{J_i}$, in the sense that ${\varphi_i}^\dagger \circ \varphi_i = [l]_{J_{i-1}}$, and if the kernel of $\varphi_{i+1} \circ \varphi_i$ is a maximal l^2-Weil isotropic subgroup of J_{i-1} for each i, then the kernel of ϕ is a maximal l^n-Weil isotropic subgroup of J_0, and ϕ splits $[l^n]_{J_0}$.

Each isogeny φ_i corresponds to an ideal $\mathfrak{L}$ over (l) in $\mathrm{End}(J_{i-1})$. If the image of $J_i[l]$ under φ_i intersects trivially with the kernel of φ_{i+1} for all i, then the endomorphism ϕ corresponds to the ideal $\mathfrak{L}^n$. On the other hand, endomorphisms correspond to principal ideals: thus $\mathfrak{L}^n$ is principal, and the order of $\mathfrak{L}$ in the ideal class group of $\mathrm{End}(J_0)$ divides n, where n is the length of the cycle. If n is minimal — that is, if the cycle does not contain a subsequence that is an isogeny cycle — then we may conclude that $\mathfrak{L}$ has order n in the ideal class group of $\mathrm{End}(J_0)$, and that $\mathrm{End}(J_0)$ contains the ideal $\mathfrak{L}^n$. We may use n, together with the splitting behaviour of (l) in $\mathrm{End}(J_0)$, to identify the identify the ideal $\mathfrak{L}^{\mathfrak{n}}$.

More generally, we may have a sequence of isogenous Jacobians J_i such that a cycle of length n appears, starting at J_d:

$$\begin{array}{ccccccccccc} & & & & & & & & & & \\ \cdots \to J_{d+n-1} & \xrightarrow{\varphi_{d+n}} & J_d & \xrightarrow{\varphi_{d+1}} & J_{d+1} & \xrightarrow{\varphi_{d+2}} & \cdots & \xrightarrow{\varphi_{d+n}} & J_{d+n} = J_d & \to \cdots & \\ & & \nearrow & & & & & & & & \\ J_0 \xrightarrow{\varphi_1} \cdots & \xrightarrow{\varphi_{d-1}} & J_{d-1} & & & & & & & & \end{array}$$

Composing the isogenies in the cycle, we obtain an endomorphism $\phi = \varphi_{d+n} \circ \cdots \circ \varphi_{d+1}$ dividing $[l^n]_{J_d}$ in $\mathrm{End}(J_d)$. We also have an endomorphism $\phi' = (\varphi_d \circ \cdots \circ \varphi_1)^\dagger \circ \phi \circ (\varphi_d \circ \cdots \circ \varphi_1)$ of $\mathrm{End}(J_0)$ such that the subring $\mathbb{Z}[\phi']$ of $\mathrm{End}(J_0)$ is isomorphic to the subring $\mathbb{Z}[m\phi]$ of $\mathrm{End}(J_d)$, and thus the index of $\mathrm{End}(J_0)$ in $\mathrm{End}(J_d)$ is divisible by m, where m is $\Pi_{i=1}^d \deg(\varphi_i) \deg({\varphi_i}^\dagger)$. In particular, if each J_i is a Jacobian surface, and each φ_i is a Richelot isogeny, then $\mathrm{End}(J_0)$ has index 16^d in $\mathrm{End}(J_d)$. In this way, we may compute the local structure of $\mathrm{End}(J_i)$ at l for $1 \leq i \leq d+n$. Combining this information over all primes l, we may determine the integral closure of $\mathbb{Z}[\mathfrak{F}]$ in $\mathrm{End}(J_0)$, where $\mathfrak{F}$ is the Frobenius endomorphism of J_0. In fact, it suffices examine the local structure at the (finite) set of primes dividing the conductor of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ in the maximal order of $\mathrm{End}^0(J_X)$.

Suppose that we are given a Jacobian J, and that we wish to determine the endomorphism ring structure of J. First, we must compute $\mathrm{End}^0(J)$; if $J = J_X$ for some hyperelliptic curve X over a finite field, then this is done by computing the zeta function of X. Next, we must compute the factorization of the conductor of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ in the maximal order of $\mathrm{End}^0(J_X)$, to obtain the set of primes l to be checked.[1] For each l, we must then construct the directed graph whose vertices are Jacobians J, with an edge from J to J' if there is an isogeny $\varphi : J \to J'$ that splits $[l]_J$. Finally, we search for cycles in the graph, and deduce information about the l-structure of $\mathrm{End}(J)$ from the cycles.

Constructing this isogeny graph requires that we be able to construct the full set of isogenies splitting $[l]_J$ for any Jacobian J. For isogeny graphs of elliptic curves, we may use the modular l-division polynomials $\Phi_l(j, j')$ to construct l-isogenous elliptic curves — see [17] for a discussion of these polynomials and their construction. The l-isogenies themselves may be constructed using the formulae of Vélu [63]; see also [18]. These methods are generally not available for Jacobians of higher genus curves. However, for Jacobians of curves of genus two, the theory of Richelot correspondences allows us to compute the local information at the prime 2, giving a partial determination of endomorphism ring structure.

9.2 Extensions of Richelot isogenies

Let $\rho_G : J_X \to J_{X_G}$ be a Richelot isogeny. The dual isogeny ${\rho_G}^\dagger : J_{X_G} \to J_X$ of ρ_G is also a Richelot isogeny: by Proposition 8.4.12, we have ${\rho_G}^\dagger = \rho_{\mathcal{R}(G)}$. We also know that ${\rho_G}^\dagger \circ \rho_{\mathcal{R}(G)} = [2]_{J_X}$, a $(2,2,2,2)$-isogeny. Now, $\mathcal{R}(G)$ may not be the only nonsingular splitting of f_{X_G} over k: according to Table 8.1, there are up to thirty distinct quadratic splittings of f_{X_G} over k, each corresponding to a distict Richelot isogeny from J_{X_G} to another Jacobian surface. We classify the Richelot isogenies from J_{X_G} according to the abelian invariants of the kernels of their compositions with ρ_G.

[1] Depending on the sizes of the discriminants of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ and $\mathcal{O}_{\mathrm{End}^0(J_X)}$, this step may be a nontrivial exercise.

Definition 9.2.1. Let $\rho : J_{X_1} \to J_{X_2}$ and $\phi : J_{X_2} \to J_{X_3}$ be Richelot isogenies, where X_1, X_2 and X_3 are curves of genus two. Then $\phi \circ \rho$ is either a $(4,4)$-isogeny, a $(4,2,2)$-isogeny or a $(2,2,2,2)$-isogeny.

- If $\phi \circ \rho$ is a $(2,2,2,2)$-isogeny, then we say ϕ is a *dual extension* of ρ.
- If $\phi \circ \rho$ is a $(4,2,2)$-isogeny, then we say ϕ is an *acyclic extension* of ρ.
- If $\phi \circ \rho$ is a $(4,4)$-isogeny, then we say ϕ is a *cyclic extension* of ρ.

It is instructive to compare composition of Richelot isogenies with composition of 2-isogenies of elliptic curves. Suppose $\phi_1 : E_0 \to E_1$ and $\phi_2 : E_1 \to E_2$ are 2-isogenies of elliptic curves: $\phi_2 \circ \phi_1$ is either a $(2,2)$-isogeny or a 4-isogeny. If $\phi_2 \circ \phi_1$ is a $(2,2)$-isogeny, then its kernel is the whole of $E_0[2]$; thus $\phi_2 \circ \phi_1$ is isomorphic to $[2]_{E_0}$, and ϕ_2 is isomorphic to ${\phi_1}^\dagger$. Hence ϕ_2 is a "dual" extension of ϕ_1. If, on the other hand, $\phi_2 \circ \phi_1$ is a 4-isogeny, then its kernel is a cyclic subgroup of $E_0[4]$. The isogeny $\phi_2 \circ \phi_1$ splits multiplication-by-4, since $(\phi_2 \circ \phi_1)^\dagger \circ (\phi_2 \circ \phi_1) = [4]_{E_0}$.

If ϕ is a cylic extension of ρ, then the kernel of $\phi \circ \rho$ is a $(4,4)$-subgroup of $J_X[4]$ — that is, a maximal 4-Weil isotropic subgroup. Similarly, composing a cyclic extension of ϕ with $\phi \circ \rho$ gives an $(8,8)$-isogeny, and a chain of n cyclic extensions gives a $(2^n, 2^n)$-isogeny.

We can describe the extension types for Richelot isogenies in terms of quadratic splittings. Suppose that we have Richelot isogenies

$$J_X \xrightarrow{\rho_G} J_{X_G} \xrightarrow{\rho_E} J_Y,$$

where $G = [(G_1, G_2, G_3)]$ and and $E = [(E_1, E_2, E_3)]$ are nonsingular splittings of f_X and f_{X_G}, respectively. Suppose also that $\mathcal{R}(G) = [(H_1, H_2, H_3)]$.

If ρ_E is a dual extension of ρ_G, then $\ker \phi = \rho(J_X[2])$, so $|E| = |\mathcal{R}(G)|$; hence $\Pi(\mathcal{R}(E)) = \Pi(G) = f_X$, so $Y = X$. Therefore, either $E = \mathcal{R}(G)$ and $\rho_E = {\rho_G}^\dagger$ (so $\rho_E \circ \rho_G = [2]_{J_X}$) or $E = \nu(\mathcal{R}(G))$ and $\rho_E = -{\rho_G}^\dagger$ (so $\rho_E \circ \rho_G = [-2]_{J_X}$).

If ρ_E is an acyclic extension of ρ_G, then $(\ker \rho_E) \cap \rho_G(J_X[2]) \cong \mathbb{Z}/2\mathbb{Z}$. The intersection is generated by a single element of $J_{X_G}[2]$, which is specified by

E_i and H_j for some pair of indices i and j; therefore $E_i = \alpha H_j$ for precisely one pair of indices i and j, and some α in $k^\times$. Note that there are six $(2,2)$-subgroups of $J_{X_G}[2]$ that intersect with $\rho_G(J_X[2])$ in this way, though they may not be k-rational.

If ρ_E is a cyclic extension of ρ_G, then $(\ker \rho_E) \cap \rho_G(J_X[2]) = 0_{J_X}$. There are eight $(2,2)$-subgroups of $J_{X_G}[2]$ that intersect trivially with $\ker \rho_E$, though they may not be k-rational. In terms of the splittings E and $\mathcal{R}(G)$, we have $E_i \neq \alpha H_j$ for all pairs of indices i and j, and all α in $k^\times$.

Note that given a Richelot isogeny $\rho_G : J_X \to J_{X_G}$ defined over k, the dual extensions $\phi = \pm\rho^\dagger$ are always defined over k, since they correspond to the splittings $\mathcal{R}(G)$ and $\nu(\mathcal{R}(G))$. According to Table 8.1, if there are any fewer than four linear factors of f_{X_G} over k then only the dual extensions of ρ_G are defined over k. If f_{X_G} has four linear factors, then we have six extensions of ρ_G over k: two are dual and four are acyclic. If f_{X_G} has six linear factors, then all thirty extensions are defined over k: two dual, twelve acyclic, and sixteen cyclic. In particular, k-rational cyclic extensions of ρ_G exist *only* when f_{X_G} is completely reducible over k.

Let $\rho_G : J_X \to J_{X_G}$ be the Richelot isogeny of some nonsingular splitting G of f_X; we will construct the set of cyclic extensions of ρ_G. Assume that $f_{X_G} = \Pi\mathcal{R}(G)$ splits completely over k — otherwise, there are no cyclic extensions of ρ_G over k. There is a factorization $f_{X_G} = \prod_{i=1}^{6} L_i$ of f_{X_G} over k, with each of the L_i linear[2], such that

$$\mathcal{R}(G) = [(L_1L_2, L_3L_4, L_5L_6)].$$

The symmetric group Sym_6 acts on the set $\{L_i : 1 \leq i \leq 6\}$ by $\sigma(L_i) := L_{\sigma(i)}$. Now, the polynomials in any quadratic splitting of f_{X_G} must must be formed from products of the L_i; therefore, if we set $\sigma(\alpha L_i L_j) = \alpha L_{\sigma(i)} L_{\sigma(j)}$ for all $i \neq j$ and α in $k^\times$, then set $\sigma([(H_1, H_2, H_3)]) := [(\sigma(H_1), \sigma(H_2), \sigma(H_3))]$, then the action extends naturally to $\mathcal{S}_{f_{X_G}}$. Clearly every quadratic splitting of f_{X_G} may be obtained by the action of some element of Sym_6 on $\mathcal{R}(G)$.

[2]If f_{X_G} is a quintic, then we let one of the L_i be a constant polynomial. By abuse of a notion, we say that the root of the constant L_i is ∞.

The stabiliser of $\mathcal{R}(G) = [(L_1L_2, L_3L_4, L_5L_6)]$ is generated by the permutations $(1,2)$, $(3,4)$ and $(5,6)$ (whose actions fix the polynomials L_1L_2, L_3L_4 and L_5L_6, respectively), together with $(1,3,5)(2,4,6)$ (which permutes L_1L_2, L_3L_4 and L_5L_6, but does not change the splitting $\mathcal{R}(G)$). Therefore, we let S denote the stabiliser of $\mathcal{R}(G)$:[3]

$$S = \langle (1,2), (3,4), (5,6), (1,3,5)(2,4,6) \rangle.$$

The quotient set Sym_6/S acts on $\mathcal{S}_{f_{X_G}}$, and therefore acts on the set of Richelot isogenies from J_{X_G}. The stabiliser S has order 24, so Sym_6/S is a set of 30 S-cosets. The extension type of $\rho_{\sigma(\mathcal{R}(G))}$ as an extension of ρ_G is completely determined by the S-coset of σ in Sym_6. Table 9.1 lists a representative σ of each S-coset, together with the type of $\rho_{\sigma(\mathcal{R}(G))}$ as an extension of ρ_G for any nonsingular quadratic splitting G. The coset representatives are arranged in rows of two: if σ and τ are in the same row of Table 9.1, then $\tau(\mathcal{R}(G)) = \nu(\sigma(\mathcal{R}(G)))$ and $\rho_{\sigma(\mathcal{R}(G))} = -\rho_{\tau(\mathcal{R}(G))}$.

We use Table 9.1 to construct an algorithm which, given a quadratic splitting representing some $(2,2)$-isogeny, constructs a set of quadratic splittings representing the cyclic extensions of that isogeny. For our applications, we need only one extension $J_{X_G} \to J_Y$ for each kernel $(2,2)$-subgroup of J_{X_G}; so if we have constructed an extension ρ_H, we may omit the construction of its negative $-\rho_H = \rho_{\nu(H)}$. Therefore, we let

$$\mathcal{C} := \left\{ \begin{array}{c} (1,2,3,4,5,6)\ ,\ (2,3,4,5,6)\ ,\ (1,3,6,4)(2,5)\ ,\ (1,3,6,4,2,5)\ , \\ (1,5,4,3,2)\ ,\ (1,4,3)(2,6,5)\ ,\ (1,5,3,2)\ ,\ (1,5,3) \end{array} \right\}.$$

The set $\mathcal{C}$ contains coset representatives to construct one of each positive-negative pair of cyclic extensions from $\mathcal{R}(G)$ — that is,

$$\{\sigma(\mathcal{R}(G)) : \sigma \in \mathcal{C}\} \cup \{\nu(\sigma(\mathcal{R}(G))) : \sigma \in \mathcal{C}\} = \mathcal{S}_{f_{X_G}},$$

and the union is disjoint.

[3]The reader familiar with wreath products may note that $S = \langle (1,2) \rangle \wr \langle (1,3,5)(2,4,6) \rangle$.

Table 9.1: S-cosets and extension types

Coset representative (negative)		Extension type
Id	$(3,5)(4,6)$	Dual
$(1,2,4,6,3,5)$	$(2,3,5)(4,6)$	Acyclic
$(2,4,6,3,5)$	$(1,2,3,5)(4,6)$	Acyclic
$(1,4,2,6,5,3)$	$(1,3)(2,5,4)$	Acyclic
$(1,6,2)$	$(1,5,6)$	Acyclic
$(1,3)(2,6,5,4)$	$(1,6,2,3,4,5)$	Acyclic
$(1,6)$	$(1,5,6,2)$	Acyclic
$(1,2,3,4,5,6)$	$(1,6,3,4,5,2)$	Cyclic
$(2,3,4,5,6)$	$(1,6,3,4,5)$	Cyclic
$(1,3,6,4)(2,5)$	$(1,4)(3,6,5)$	Cyclic
$(1,3,6,4,2,5)$	$(1,4,2)(3,6,5)$	Cyclic
$(1,5,4,3,2)$	$(1,4,3,2,6,5)$	Cyclic
$(1,4,3)(2,6,5)$	$(1,5,4,3)$	Cyclic
$(1,5,3,2)$	$(1,2,4)(3,5,6)$	Cyclic
$(1,5,3)$	$(2,4)(3,5,6)$	Cyclic

Algorithm 9.2.2. Given a nonsingular quadratic splitting G, computes a representative for each of the cyclic extensions of ρ_G, up to sign.

procedure CyclicExtensions(G)
  $[(H_1, H_2, H_3)] := \mathcal{R}(G)$;
  if H_1, H_2 or H_3 is irreducible **then**
    return {};
  end if;
  $\alpha_1, \alpha_2 :=$ Roots(H_1, k);
  $\alpha_3, \alpha_4 :=$ Roots(H_2, k);
  $\alpha_5, \alpha_6 :=$ Roots(H_3, k);
  $c := \prod_{i=1}^{3}$ LeadingCoefficient(H_i);
  $E := \{\}$;
  for σ **in** $\mathcal{C}$ **do**
    $H_1' := (u - \alpha_{\sigma(1)})(u - \alpha_{\sigma(2)})$;
    $H_2' := (u - \alpha_{\sigma(3)})(u - \alpha_{\sigma(4)})$;
    $H_3' := (u - \alpha_{\sigma(5)})(u - \alpha_{\sigma(6)})$;

```
        E := E ∪ {[(cH'_1, H'_2, H'_3)]};
    end for;
    return E;
end procedure;
```

Example 9.2.3. As in Examples 8.2.5, 8.3.2, and 8.4.13, suppose $k = \mathbb{F}_{83}$, and let X be the curve of genus two over k defined by

$$X : v^2 = f_X(u) = 24u^6 + 61u^5 + 48u^4 + 64u^3 + 14u^2 + 65u + 21.$$

In Example 8.2.5, we noted that the splittings

$$\begin{aligned} G &= [(24u^2 + 52u + 74, u^2 + 23u + 22, u^2 + 50u + 59)] \quad \text{and} \\ G' &= [(24u^2 + 52u + 74, u^2 + 46u + 45, u^2 + 27u + 27)], \end{aligned}$$

together with $\nu(G)$ and $\nu(G')$, are nonsingular. Now, $\Pi(\mathcal{R}(G)) = f_{X_G}$ is not completely reducible over k, so ρ_G has no rational cyclic extensions over k. On the other hand, the polynomials of

$$\mathcal{R}(G') = \left[(33u^2 + 80u + 23, 61u^2 + 15u + 8, 60u^2 + 57u + 22)\right]$$

are all completely reducible over k, so $\rho_{G'}$ has cyclic extensions defined over k. Applying Algorithm 9.2.2 (CyclicExtensions) to G', we find that the quadratic splittings

$$\begin{aligned} &[(15u^2 + 9u + 29, u^2 + 49u + 24, u^2 + 2)], \\ &[(15u^2 + 58u + 31, u^2 + 7u + 76, u^2 + 2)], \\ &[(15u^2 + 56u + 36, u^2 + 61u + 34, u^2 + 7u + 76)], \\ &[(15u^2 + 9u + 29, u^2 + 79u + 49, u^2 + 53u + 23)], \\ &[(15u^2 + 48u + 13, u^2 + 37u + 3, u^2 + 26u + 74)], \\ &[(15u^2 + 23u + 71, u^2 + 18u + 11, u^2 + 19u + 80)], \\ &[(15u^2 + 57u + 45, u^2 + 18u + 11, u^2 + 61u + 34)], \text{ and} \\ &[(15u^2 + 56u + 36, u^2 + 19u + 80, u^2 + 49u + 24)], \end{aligned}$$

together with their negatives, specify all of the cyclic extensions of $\rho_{G'}$.

9.3 Explicit isogeny cycles

Let X be a curve of genus two and J_X its Jacobian. We will apply the theory of Richelot isogenies and isogeny cycles to determine the structure of $\mathrm{End}(J_X)$ at the prime 2, by looking for cycles in its $(2,2)$-isogeny graph. For each Richelot isogeny ρ from J_X, we conduct a breadth-first search [14, §22.2] in the graph of cyclic extensions originating from ρ. We generate cyclic extensions by recursively applying Algorithm 9.2.2 (CyclicExtensions); as we traverse the graph, we keep a list of the absolute Igusa invariants [43, page 325] of all of the Jacobians that we encounter. If we ever construct a codomain Jacobian with invariants already in our list, then we have detected a cycle.

Algorithm 9.3.1. Given a curve X of genus two over k, computes a sequence L of sets of absolute Igusa invariants corresponding to Jacobians connected by Richelot isogenies over k, with each isogeny a cyclic extension of its predecessor, such that the sequence begins with the invariants of X and contains a cycle (if no such sequence exists, then an empty sequence is returned). The algorithm returns L, together with integers n and d, where n is the length of the cycle and d is the index in the sequence (counting from zero) at which the cycle begins.

procedure RichelotIsogenyCycles(X)
  for $G \in \mathcal{S}_{f_X}^{\mathrm{ns}}$ **do**
    $Q :=$ [(G, [AbsoluteIgusaInvariants(X)])];
    while $Q \neq$ [ ] **do**
      Let (G, L) be the first item of Q, and remove this item from Q;
      $I :=$ AbsoluteIgusaInvariants(Curve($v^2 - \Pi(\mathcal{R}(G))$));
      if $I \in L$ **then** // we have detected a cycle.
        $d :=$ index of I in L (counting from zero);
        $n := \#L - d$;
        return L, n, d;
      end if;
      append I to L;
      for H in CyclicExtensions(G) **do**

```
            if det(H) ≠ 0 then                    // if H is nonsingular
                append [(H, L)] to Q;
            end if;
        end for;
    end while;
end for;
return [ ], 0, 0;                                // No rational cycle exists.
end procedure;
```

Example 9.3.2. As in Examples 8.2.5, 8.3.2, 8.4.13 and 9.2.3, let $k = \mathbb{F}_{83}$, and let X be the curve of genus two over k defined by

$$X : v^2 = f_X(u) = 24u^6 + 61u^5 + 48u^4 + 64u^3 + 14u^2 + 65u + 21.$$

Applied to X, Algorithm 9.3.1 (RichelotIsogenyCycles) detects a cycle of length five, one Richelot isogeny away from J_X. The Richelot isogeny leading us to the cycle is $\rho_{G'} : J_X \to J_{X_{G'}}$, where G' is defined in Example 9.2.3.

Example 9.3.3. Let $k := \mathbb{F}_{5^4}$, and let w be a primitive element of k with minimal polynomial $x^4 - x^2 - x + 2$. Let X be the curve of genus two defined by

$$X : v^2 = f_X(u) = u^6 + w^{524}u^5 + w^{258}u^4 + w^{28}u^3 + w^{611}u^2 + w^{507}u + w^{505}.$$

Computing the zeta function of X, we deduce that the characteristic polynomial of the Frobenius endomorphism is $\chi(x) = x^4 + 32x^3 + 1166x^2 + 20000x + 390625$. The discriminant of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ is $2^{16} \cdot 3 \cdot 5^2 \cdot 17^3 \cdot 251$. Let $K = \mathrm{End}^0(J_X) \cong \mathbb{Q}[x]/(\chi(x))$, and let K_0 be the real subfield of K. Let $\mathcal{O}_K$ and $\mathcal{O}_{K_0}$ denote the maximal orders of K and K_0, respectively. The discriminant of $\mathcal{O}_K$ is $3 \cdot 5^2 \cdot 17^3 \cdot 251$, so the conductor of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ in $\mathcal{O}_K$ is $256 = 2^{16}$: we need only check the prime 2, so the Richelot isogeny cycle graph will completely determine the endomorphism ring of J_X. The ideal (2) remains prime in $\mathcal{O}_{K_0}$; however, in $\mathcal{O}_K$ we have $(2) = \mathfrak{P}_1\mathfrak{P}_2$, where each prime $\mathfrak{P}_i$ has order 40 in the class group of $\mathcal{O}_K$. Applied to X, Algo-

rithm 9.3.1 (RichelotIsogenyCycles) detects a Richelot isogeny cycle of length 40, two Richelot isogenies away from J_X. The Richelot isogeny from J_X leading to the cycle is ρ_G, where

$$G = \left[(u^2 + w^{586}u + w^{91}, u^2 + w^{586}u + w^{499}, u^2 + w^2u + w^{539})\right].$$

The endomorphism ring of the Jacobians in the cycle is isomorphic to $\mathcal{O}_K$, and J_X is two Richelot isogenies away from the cycle; therefore the index of $\mathrm{End}(J_X)$ in $\mathcal{O}_K$ is $16^2 = 256$. Hence $\mathrm{End}(J_X) = \mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$: the endomorphism ring of J_X is minimal.

Example 9.3.4. Let $k = \mathbb{F}_{5^4}$, and suppose w is a primitive element of k. Let X be the curve of genus two over k defined by

$$X : v^2 = f_X(u) = u^6 + w^{233}u^5 + w^{470}u^4 + w^{173}u^3 + w^{200}u^2 + w^{379}u + w^{383}.$$

Computing the zeta function of X, we deduce that the characteristic polynomial of the Frobenius endomorphism is $\chi(x) = x^4 - 32x^3 + 718x^2 - 20000x + 390625$. The discriminant of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ is $2^{16} \cdot 23 \cdot 197^2 \cdot 223$. Let $K = \mathrm{End}^0(J_X) \cong \mathbb{Q}[x]/(\chi(x))$, and let K_0 be the real subfield of K. Let $\mathcal{O}_K$ and $\mathcal{O}_{K_0}$ denote the maximal orders of K and K_0, respectively. The discriminant of $\mathcal{O}_K$ is $23 \cdot 197^2 \cdot 223$, so the conductor of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ in $\mathcal{O}_K$ is $256 = 2^{16}$: we need only check the prime 2, so the Richelot isogeny cycle graph will completely determine the endomorphism ring of J_X. The prime (2) is inert in K_0, and splits in K: we have $(2) = \mathfrak{P}_1\mathfrak{P}_2$ in $\mathcal{O}_K$, where the order of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ in the class group of K is 26. Applied to X, Algorithm 9.3.1 (RichelotIsogenyCycles) detects a Richelot isogeny cycle of length 26, one Richelot isogeny away from J_X. The Richelot isogeny leading us to the cycle is ρ_G, where

$$G = \left[(u^2 + w^{393}u + w^{367}, u^2 + w^{393}u + w^{459}, u^2 + w^{115}u + w^{181})\right]$$

The endomorphism ring of the Jacobians in the cycle is isomorphic to $\mathcal{O}_K$, and J_X is one Richelot isogeny away from the cycle; therefore the index of $\mathrm{End}(J_X)$ in $\mathcal{O}_K$ is 16, and the index of $\mathbb{Z}[\mathfrak{F}, \mathfrak{F}^\dagger]$ in $\mathrm{End}(J_X)$ is also 16.

Bibliography

[1] A. O. L. Atkin, The number of points on an elliptic curve modulo a prime, *preprint*, 1988.

[2] A. O. L. Atkin, The number of points on an elliptic curve modulo a prime (II), *preprint*, 1992.

[3] P. R. Bending, *Curves of genus* 2 *with* $\sqrt{2}$ *multiplication*, Ph.D. thesis, University of Oxford, 1998. Summary article available from `http://front.math.ucdavis.edu/ANT/0213/`

[4] D. J. Bernstein, Pippenger's Exponentiation Algorithm, *preprint, 2002.* Available from `http://cr.yp.to/papers.html#pippenger`

[5] J.-B. Bost and J.-F. Mestre, Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math. Soc. France* **38** (1988), 36–64.

[6] A. Brumer, *Curves with real multiplication*, in preparation.

[7] J. Buhler and N. Koblitz, Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, *Bull. Aust. Math. Soc.* **58** (1998), no. 1, 147-54.

[8] J. Cannon et. al., The MAGMA computational algebra system, `http://magma.maths.usyd.edu.au/`

[9] D. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), 95–101.

[10] J. W. S. Cassels, Factorization of polynomials in several variables, *Proceedings of the 15th Scandinavian Congress, Oslo 1968* Lecture Notes in Mathematics **118**, Springer, 1970, 1–17.

[11] J.W.S. Cassels and E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, *London Mathematical Society Lecture Note Series* 230, Cambridge University Press, 1996.

[12] P. Cassou–Nogues and J.-M. Couveignes, Factorisations explicities de $g(y) - h(z)$, *Acta Arithmetica* **87** (1999), no. 4, 291-317.

[13] M. Ciet, T. Lange, F. Sica and J.-J. Quisquater, Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms, *Advances in Cryptology—EUROCRYPT 2003*, 387–400, LNCS **2656**, Springer, Berlin, 2003.

[14] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms* (second edition), MIT Press and McGraw-Hill, 2001.

[15] M. Deuring, Arithmetische Theorie der Korrespondenzen algebraischer Functionenkörper (Tiel I), *J. Reine Angew. Math.* **177** (1937), 161–191.

[16] M. Deuring, Arithmetische Theorie der Korrespondenzen algebraischer Functionenkörper (Tiel II), *J. Reine Angew. Math.* **183** (1940), 25–36.

[17] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, *Computational perspectives on number theory: proceedings of a conference in honor of A. O. L. Atkin*, (D. A. Buell and J. T. Teitelbaum, eds), AMS, 1997, 21–76.

[18] N. D. Elkies, Explicit isogenies, *preprint*, 1991.

[19] J. Ellenberg, Endomorphism Algebras of Jacobians, *Advances in Mathematics* **162** (2001), 243–271.

[20] M. Fouquet and F. Morain, Isogeny volcanoes and the SEA algorithm, *Algorithmic number theory — ANTS-V 2002 (Sydney)*, 276–291, LNCS **2369**, Springer, 2002.

[21] M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

[22] W. Fulton, *Intersection Theory* (second edition), Springer, 1998.

[23] R. Gallant, R. Lambert and S. Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms, *Advances in Cryptology—CRYPTO 2001*, 190–200, LNCS **2139**, Springer, 2001.

[24] P. Gaudry and N. Gürel, Counting points in medium characteristic using Kedlaya's algorithm, *Experiment. Math.* **12** (2003), no. 4, 395–402.

[25] D. Gorenstein, The enormous theorem, *Scientific American* **253** (1985), 104–115, 150.

[26] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups*, Mathematical surveys and monographs **40.1**, American Mathematical Society, 1994.

[27] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Wiley, 1978.

[28] C. Günter, T. Lange and A. Stein, Speeding up the arithmetic on Koblitz curves of genus two, *Selected areas in cryptography: SAC 2001*, LNCS **2012**, Springer, 2001, 106–117.

[29] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag New York, 1977.

[30] K. Hashimoto, On Brumer's family of RM-curves of genus two, *Tohoku Math. J.* **52** (2000), 475–488.

[31] M. Hindry and J. H. Silverman, *Diophantine Geometry : An Introduction*, Graduate Texts in Mathematics **201**, Springer, 2000.

[32] K. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), no. 4, 323–338.

[33] D. Kim and S. Lim, Integer decomposition for fast scalar multiplication on elliptic curves, *Selected areas in cryptography: SAC 2002*, LNCS **2595**, Springer, 2003, 13–20.

[34] N. Koblitz, CM-curves with good cryptographic properties. *Advances in Cryptology—CRYPTO '91*, 279–287, LNCS **576**, Springer, 1992.

[35] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

[36] G. Kux, *Construction of algebraic correspondences between hyperelliptic function fields using Deuring's theory*, Ph.D. thesis, Universitat Kaiserslautern, 2004.

[37] S. Lang, *Abelian Varieties*, Springer, 1983.

[38] S. Lang, *Algebra* (third edition), Graduate Texts in Mathematics **211**, Springer, 2002.

[39] H. Lange and C. Birkenhake, *Complex Abelian Varieties* (second edition), Grundlehren der mathematischen Wissenschaften 302, Springer-Verlag Berlin, 2004.

[40] T. Lange, *Efficient arithmetic on hyperelliptic Koblitz curves*, Ph.D. thesis, Universität Duisburg–Essen, 2001.

[41] D. Lehavi and C. Ritzenthaler, An explicit formula for the arithmetic geometric mean in genus 3, *preprint, 2005*, available from `http://arxiv.org/abs/math.AG/0403182`.

[42] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman monographs and surveys in pure and applied mathematics **65**, Longman Scientific & Technical, 1993.

[43] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, *Effective methods in algebraic geometry*, 131–334, Progress in Math. **94**, Birkhäuser, Boston 1991.

[44] J.-F. Mestre, Familles de courbes hyperelliptiques à multiplications réelles, in *Arithmetic algebraic geometry (Texel, 1989)*, 193–208, Progress in Math. **89**, Birkhäuser, Boston 1991.

[45] J. S. Milne, *Abelian Varieties*, in G. Cornell and J. H. Silverman (eds), *Arithmetic Geometry (Proc. Conference on Arithmetic Geometry, Storrs, August 1984)*, Springer, 1986.

[46] J. S. Milne, *Jacobian Varieties*, in G. Cornell and J. H. Silverman (eds), *Arithmetic Geometry (Proc. Conference on Arithmetic Geometry, Storrs, August 1984)*, Springer, 1986.

[47] F. Morain, Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques, *J. Théor. Nombres Bordeaux* **7** (1995), 255–282.

[48] D. Mumford, *Tata lectures on Theta II*, Birkhäuser, Boston, 1984.

[49] Y.-H. Park, S. Jeong and J. Lim, Speeding up point multiplication on hyperelliptic curves with efficiently-computable endomorphisms, *Advances in cryptology—EUROCRYPT 2002 (Amsterdam)*, 197–208, LNCS **2332**, Springer, 2002.

[50] F. Richelot, De transformatione integralium Abelianorum primi ordinis commentatio, *J. Reine Angew. Math.* **16** (1837), 221–341.

[51] F. Richelot, Essai sur une méthode générale pour déterminer les valeurs des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes, *C. R. Acad. Sci. Paris.* **2** (1836), 622–627.

[52] T. J. Rivlin, *Chebyshev polynomials*, Wiley, 1990.

[53] T. Satoh, On p-adic point counting algorithms for elliptic curves over finite fields, *Algorithmic number theory — ANTS-V 2002 (Sydney)*, 43–66, LNCS **2369**, Springer, 2002.

[54] R. Schoof, Counting points on elliptic curves over finite fields, *J. Théor. Nombres Bordeaux* **7** (1995), 219–254.

[55] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494.

[56] J.-P. Serre, *Algebraic groups and class fields* (corrected second printing), Graduate Texts in Mathematics **117**, Springer, 1997.

[57] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton University Press, 1998. ,

[58] F. Sica, M. Ciet and J.-J. Quisquater, Analysis of the Gallant–Lambert–Vanstone method based on efficient endomorphisms: elliptic and hyperelliptic curves, *Selected areas in cryptography: SAC 2002*, LNCS **2595**, Springer, 2003.

[59] J. A. Solinas, Efficient arithmetic on Koblitz curves, *Des. Codes Cryptogr.* **19** (2000), no. 2-3, 195–249.

[60] R. Solomon, On finite simple groups and their classification, *Notices of the American Mathematical Society* **42** (1995), no. 2, 231–239.

[61] K. Takashima, A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application, *preprint* (work presented at ISISC, Seoul, Korea 2004).

[62] W. Tautz, J. Top, A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials, *Canad. J. Math.* **43** (1991), no. 5, 1055–1064.

[63] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris, Séries A* **273** (1971), 305–347.

[64] A. Weil, *Sur les courbes algébriques et les variétes qui s'en déduisent*, Hermann & Cie., Paris, 1948.

[65] A. Weil, *Variétes abéliennes et courbes algébriques*, Hermann & Cie., Paris, 1948.