On Jacobians of dimension $2g$ that decompose into Jacobians of dimension g

by

Avinash Kulkarni
B.Math (Hons.),University of Waterloo, 2012

Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2014

APPROVAL

Name: Avinash Kulkarni

Degree: Master of Science

Title of Thesis: On Jacobians of dimension $2g$ that decompose into Jacobians of dimension g.

Examining Committee: Dr. Ralf Wittenberg, Associate Professor
Chair

Dr. Nils Bruin
Senior Supervisor
Associate Professor

Dr. Imin Chen
Supervisor
Associate Professor

Dr. Petr Lisonek
Internal Examiner
Associate Professor

Date Defended/Approved: August 12th, 2014

Partial Copyright Licence

Abstract

In this thesis we describe a family of Jacobian varieties of non-hyperelliptic genus $2g$ curves that are isogenous to a product of Jacobians of genus g curves in a specific way. For any hyperelliptic genus g curve C we construct a 2-parameter family of hyperelliptic genus g curves H with $J(H)[2]$ isomorphic to $J(C)[2]$, and a generically non-hyperelliptic curve A such that there is an isogeny from $J(C) \times J(H)$ to $J(A)$ whose kernel is the graph of the isomorphism taking $J(H)[2]$ to $J(C)[2]$. This is accomplished by first showing that C can be considered as a subcover of a Galois cover of a $\mathbb{P}^1$ that has A and H naturally arising as subcovers and then showing the naturally occurring isogeny relations have the desired kernel. We also list some corollaries to the main result and provide a magma script to generate non-hyperelliptic genus 4 curves that have curious automorphism groups.

Keywords: Jacobian variety; decomposition

Acknowledgements

I would like to thank my family for the many years they have supported and encouraged my study of mathematics. To my fellow students Navid Alaei, Steve Melczer, Ryan McMahon, and Brett Nasserden I thank you for the many good times and for the helpful advice in learning the nuances of algebraic geometry. I owe many thanks to Colin Weir for his helpful discussions and insight into my research project, particularly regarding possible generalizations of the main result. Thanks to Imin Chen for pointing out the connection to Kani and Rosen's work. I would like to thank Bjorn Poonen for his very insightful comments regarding the future directions section. I would like to thank Diane Pogue for helping me with the administrative aspects of the writing process. Finally, I am deeply grateful to my senior supervisor Nils Bruin for his enduring patience, wise advice, vigilant editing, and warm guidance.

Contents

List of Figures

Chapter 1

Introduction

An abelian variety is a projective variety together with a morphism $+\colon A \times A \to A$ and a distinguished point O such that its point set is a commutative group with the operation given by "$+$". The group structure on an abelian variety can sometimes be used to recover arithmetic information about the subvarieties that exist within it. Considering curves inside their Jacobian varieties lead to Faltings' famous (revised) proof of Mordell's conjecture [10, Section E.1].

Theorem 1.0.1 (Faltings)**.** *A curve of genus $g \geq 2$ defined over a number field k has finitely many k-rational points.*

There are a number of ways in which abelian varieties can decompose into a product of abelian varieties of smaller dimension. It can be a product itself or it can admit a finite morphism onto such a product. Such a morphism is called an "isogeny". The factors of a decomposable abelian variety can be analyzed to understand the original object much like other algebraic structures. Decomposability of abelian varieties has a long history in mathematics that goes back at least to the computation of abelian and elliptic integrals in the late 19th century [1, 17].

The modern study of the subject has led to a number of interesting geometric and arithmetic results. There is a large body of work finding g-dimensional Jacobian varieties that are isogenous to the product of g copies of one elliptic curve. Jacobians of this type are interesting for a number of reasons, one reason of interest to number theorists and cryptographers is that over a finite field Jacobian varieties of this type are closely related to Jacobians that have a maximal number of rational points [11]. A paper by Ekedahl and Serre [6] shows that Jacobians of this type exist for many values of g. Related work by Jennifer Paulhus [16] classifies the other isogeny types of Jacobian varieties

of small genus. Her work also has applications to the computation of rank bounds on elliptic curves, which is a topic of much interest in modern mathematics.

All abelian varieties can be assigned something called a polarization, which is not in general preserved by isogeny. It is a natural and useful question to ask when a decomposition does respect the polarization. Nils Bruin and Victor Flynn give an example of how such a decomposition can aid in determining the existence of rational points on curves of genus ≤ 2, see [2, 3].

In this thesis we show how an explicitly described family of hyperelliptic curves can be related to Jacobian varieties that decompose in a way that respects polarizations. We prove

Theorem (Main Result)**.** *Let k be a field of characteristic not equal to 2. Let C_f be a hyperelliptic genus g curve defined over k, and $J(C_f)$ its Jacobian. Then there exists a two parameter family of explicitly determined curves C_F of genus g and A of genus $2g$ such that*

1. *C_F is hyperelliptic and there is an isomorphism of finite algebraic sets $\psi\colon J(C_F)[2] \to J(C_f)[2]$.*
2. *A is a double cover of C_F.*
3. *$J(A) \cong J(C_f) \times J(C_F)/\Delta$ as polarized abelian varieties, where Δ is the (anti)-diagonally embedded 2-torsion of $J(C_f)$.*

Our work was largely inspired by Everett Howe's [11, Section 4] classification of genus 4 double covers of genus 2 curves with a rational point since the decomposition type studied in this thesis arises when a genus 4 curve is a double cover of a genus 2 curve. We remark that any genus 4 curve that can be constructed from Howe's technique can also be produced from our construction with the right choice of C_f and μ but not vice-versa. We differ from [16] since we allow non-elliptic factors in the decomposition but we restrict the kernel of the isogeny from the product variety. We also draw inspiration from the construction of Legendre [1]. Our construction generalizes [1] since we do not require curves with a rational Weierstrass point. The techniques used in this thesis have also been applied by Recillas [18] and Donagi [4] to find correspondences between Jacobian varieties and Prym varieties.

In Chapter 2 of this thesis we provide an exposition of the necessary language required to state and prove the main result. In Chapter 3 we prove the main result and then state some immediate consequences. We also provide a small magma script that constructs one of the decomposition types

in [16] explicitly. Finally in Chapter 4 we posit a future statement related to the main result that can serve as a future direction of research.

Chapter 2

Background material

2.1 Prelude

In this chapter we present a terse review to the arithmetic geometry of curves and their Jacobians. This chapter shall serve the purpose of refreshing the reader on the definitions. The chapter as a whole serves to exposit on the language of arithmetic geometry to a point where the main question can be well formulated as well as provide the necessary tools needed to prove it. Those interested in the details are encouraged to refer to [9, 10, 19, 20], and Milne's course notes [14].

2.2 Notation and persistent assumptions

This section serves as a shorthand glossary and establishes the conventions and notations in case the reader should want to refer back to it.

If X is a set with finite cardinality then we denote the number of elements by $\#X$ or by $|X|$. The Klein 4-group, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, is denoted by V_4. The dihedral group of order 8 is denoted by D_4. We let k denote an arbitrary field with characteristic not 2. We shall always denote its algebraic closure as $\bar{k}$.

We define *affine n-space* over k, denoted $\mathbb{A}^n_k$, to be the set of all n-tuples of elements of k. An element $P \in \mathbb{A}^n_k$ will be called a point. We define *projective n-space* over k, denoted $\mathbb{P}^n_k$ to be the set of $(n+1)$-tuples of k, excluding the all-zero tuple, modulo the relation $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n), \lambda \in k^*$. A point $P \in \mathbb{P}^n_k$ is one of these equivalence classes and is denoted $P = (a_0 : \ldots : a_n)$.

For polynomials $f_i \in k[x_1, \ldots, x_n]$ we let $V(f_1, \ldots, f_r) \subseteq \mathbb{A}^n_{\bar{k}}$ denote their common zero locus and call this an *affine algebraic set defined over* k. Similarly we let $V(f_1, \ldots, f_r) \subseteq \mathbb{P}^n_{\bar{k}}$ denote the common zero locus of homogeneous polynomials f_i with coefficients in k and call this a *projective algebraic set defined over* k. Any affine or projective algebraic set defined over k is also defined over $\bar{k}$. As a shorthand we emphasize that an affine algebraic set $X \subseteq \mathbb{A}^n_{\bar{k}}$ is defined over k by writing $X \subseteq \mathbb{A}^n_k$ and we use a similar shorthand for projective algebraic sets. Henceforth if we make a statement regarding affine algebraic sets that has an analogue for projective algebraic sets we shall use the term *algebraic set*. We denote the set of points of an algebraic set X by $X(\bar{k})$.

An algebraic set X defined over $\bar{k}$ is said to be *geometrically reducible* if we can find non-empty algebraic sets Y, Z defined over $\bar{k}$ such that $X = Y \cup Z$ and both $Y \not\subseteq Z, Z \not\subseteq Y$. Otherwise X is said to be *geometrically irreducible* or more commonly, we call X a *variety*. Since every variety in this thesis is either an affine variety or a projective variety we identify a variety with its point set over $\bar{k}$.

Let X and Y be varieties defined over k. Fix a choice of co-ordinates $x_1, \ldots, x_n$ for X and $y_1, \ldots y_r$ for Y. We may describe any morphism $\varphi\colon X \to Y$ by polynomial functions $f_1, \ldots, f_r$ in the co-ordinates of X. A *morphism of varieties defined over* k is a morphism $\varphi := (f_1, \ldots, f_r)\colon X \to Y$ such that each f_i is a polynomial with coefficients in k. Similarly, a *rational map defined over* k is a map $\varphi := (f_1, \ldots, f_r)\colon X \to Y$ such that each f_i is a rational function that has coefficients in k. A rational map $\phi\colon X \to Y$ is said to be *dominant* if there is are open sets $U_X \subseteq X$ and $U_Y \subseteq Y$ such that $\phi(U_X) = U_Y$. A *function* on a variety X defined over k is a rational map $\varphi\colon X \to \mathbb{A}^1_k$ defined over k. The *ring of rational functions on* X *defined over* k, also called the *function field* of X, is denoted by $k(X)$. We also call $\bar{k}(X)$ the function field of X. We denote the identity map on X by $\mathbb{1}_X$ and when it is clear from context we will drop the subscript. The identity map is always defined over k.

The *absolute galois group* $G_k := \mathrm{Gal}(\bar{k}/k)$ is the group of automorphisms of $\bar{k}$ that fix k. Let X be a projective variety defined over k and let $P := (w_0 : \ldots : w_n) \in X(\bar{k})$. We say P is a *k-rational point* if there is a $\lambda \in \bar{k}$ such that each $\lambda w_i \in k$. If X is an affine variety defined over k and $P := (w_0, \ldots, w_n) \in X(\bar{k})$ we say P is a rational point if each $w_i \in k$. The rational points of a variety X defined over k are denoted $X(k)$.

We say that a *curve defined over* k is a birational isomorphism (defined over k) class of varieties defined over k of dimension 1. We call a particular representative a *model* of a curve. We call a

model projective or affine if the representing variety is projective or affine respectively. Theorem 2.3.9 shows that any such class contains smooth projective models and any two such models are isomorphic. Therefore we will often identify a curve with its smooth model.

Let X and Y be projective curves defined over k and let $\phi\colon Y \to X$ be a surjective morphism of curves defined over k. There is a corresponding morphism of function fields $\phi^*\colon k(X) \to k(Y)$ given by $\phi^*(f) := f \circ \phi$.

Definition 2.2.1. Let $\phi\colon X \to Y$ be a surjective morphism of curves defined over k. If $[k(Y) : \phi^*k(X)]$ is a finite extension of fields then we call this quantity the *degree* of ϕ and ϕ is said to be *separable* if $[k(Y) : \phi^*k(X)]$ is separable.

Let $\phi : C_1 \to C_2$ be a surjective morphism of models of curves and let $P \in C_2(\bar{k})$. We shall see by a later result (Proposition 2.3.6) this automatically ensures ϕ is of finite degree. Then we call the set $\phi^{-1}(P)$ the *fibre over* P. We also say that C_1 is a *cover* of C_2 and that ϕ is the covering map. A double cover is a cover of degree 2.

We denote the group of automorphisms of a variety X by $\mathrm{Aut}(X)$. If $\pi\colon \widetilde{C} \to C$ is a non-constant morphism of curves then we denote the subgroup of automorphisms $\sigma \in \mathrm{Aut}(\widetilde{C})$ such that $\pi \circ \sigma = \pi$ by $\mathrm{Aut}(\widetilde{C}/C)$. An *involution* of a variety X is an automorphism μ such that $\mu \circ \mu = \mathbb{1}_X$.

2.3 Theorems regarding curves

In this section when we refer to a point on a curve we mean $P \in C(\bar{k})$. We shall also assume that every curve is defined over k.

Definition 2.3.1. Let $P \in C$ be a point. Then the *local ring at* P is defined by

$$\mathcal{O}_{C,P} := \{f \in k(C) : \exists U \subseteq C \text{ Zariski open such that } P \in U \text{ and } f \text{ is regular on } U\}.$$

Proposition 2.3.2. *If P is a smooth point of C then $\mathcal{O}_{C,P}$ is a discrete valuation ring.*

Proof. See [20, Proposition II.1.1]. □

Recall that a generator for the unique maximal ideal of a discrete valuation ring is called a *uniformizing parameter* or a *uniformizer*.

Definition 2.3.3. Let $f \in \bar{k}(C)$ and let t be a uniformizing parameter at P. We define

$$\operatorname{ord}_P f := \sup \left\{ d \in \mathbb{Z} : f \cdot t^{-d} \in \mathcal{O}_{C,P} \right\}.$$

Definition 2.3.4. Let $f \in k(C)$ be a rational function of C. A *zero* of f is a point P such that $\operatorname{ord}_P f > 0$. Similarly a *pole* of f is a point P such that $\operatorname{ord}_P f < 0$.

Proposition 2.3.5. *Let C be a non-singular projective model of a curve. Then any $f \in k(C)$ has finitely many poles and zeros. Moreover $\sum_{P \in C} \operatorname{ord}_P(f) = 0$.*

Proof. See [20, Proposition II.1.2] for the first statement and [20, Proposition II.3.1] for the second. □

We conclude this section with some general theorems about curves which will come in handy later.

Proposition 2.3.6. *Let $\pi \colon \widetilde{C} \to C$ be a non-constant morphism of curves. Then π is surjective and of finite degree.*

Proof. See [20, Theorems II.2.3, II.2.4]. □

Definition 2.3.7. If $\pi \colon \widetilde{C} \to C$ is a surjective morphism of curves then we refer to $\widetilde{C}$ as a *cover* of C.

Proposition 2.3.8. *Let $\phi : C \to C'$ be a birational map. Then $k(C) \cong k(C')$.*

Proof. See [20, Theorem II.2.4]. □

Theorem 2.3.9. *Let C be a curve.*

1. *Then there is a smooth projective curve X such that X is birationally equivalent to C.*
2. *If X and X' are smooth projective curves birationally equivalent to C then X' is isomorphic to X.*

We say X is a desingularization *of C.*

Proof. See [8, 7.5 Theorem 3]. □

Proposition 2.3.10. *Let $\phi \colon C_1 \to C_2$ be a rational map of projective curves and let C_1 be smooth. Then ϕ can be extended to a morphism on all of C_1.*

Proof. See [20, Proposition II.2.1]. □

Corollary 2.3.11. *Let C_1, C_2 be projective curves and let $\widetilde{C}_1, \widetilde{C}_2$ be their respective desingularizations. If $\phi\colon C_1 \to C_2$ is a birational morphism then there is a morphism $\widetilde{\phi}\colon \widetilde{C}_1 \to \widetilde{C}_2$.*

Proof. We notice that by definition $\widetilde{C}_1, \widetilde{C}_2$ are birational to C_1, C_2 respectively and that by assumption C_1 is birational to C_2. Hence there is a birational morphism $\widetilde{\phi}\colon \widetilde{C}_1 \to \widetilde{C}_2$. By the preceeding proposition $\widetilde{\phi}$ extends to a morphism.

□

2.4 Divisors

The following is a very brief treatment of Weil divisors. This is all we need since we only work with smooth curves. We introduce the Picard group of a curve and survey some useful properties. We also provide a couple of computational lemmas at the end of the section for use later. The reader interested in this subject is encouraged to refer to [10] for a more complete reference.

Definition 2.4.1. Let X be a variety. A subvariety Y is said to be of *co-dimension 1* if for every variety $Y \subseteq Z \subseteq X$ we have $Z = Y$ or $Z = X$.

Definition 2.4.2. Let X be a smooth projective variety. A *(Weil) divisor of X* is a formal $\mathbb{Z}$-linear combination $D = \sum_{Y \subseteq X} a_Y Y$ such that all but finitely many of the a_Y are zero and each Y is a codimension 1 subvariety of X. The free abelian group generated by the Y is denoted $\mathrm{Div}(X)$.

In other words, $\mathrm{Div}(X)$ is the group of divisors of X over $\bar{k}$. In this thesis we exclusively focus on divisors of curves, however it is possible to extend this notion to arbitrary projective varieties as in [10]. We observe that since every codimension 1 subvariety of a curve must be a point that every divisor on a curve can be written as the formal linear combination of $\bar{k}$-points on the curve. Throughout let C be a smooth projective curve.

Definition 2.4.3. Let $D = \sum_{P \in C} a_P P$ be a divisor of C. Then the *multiplicity of a point P in D* is the integer a_P.

Definition 2.4.4. A divisor $D = \sum_{P \in C} a_P P$ is said to be *effective* if each $a_P \geq 0$.

Definition 2.4.5. For a divisor $D = \sum_{P \in C} a_P P$ on a curve X we define the *degree* to be $\sum_{P \in C} a_P$. This is denoted $\deg(D)$.

Definition 2.4.6. The degree map $\deg\colon \mathrm{Div}(C) \to \mathbb{Z}$ is a morphism of groups, the kernel of which are the degree 0 divisors. The *subgroup of degree 0 divisors* on C is denoted $\mathrm{Div}^0(C)$.

Definition 2.4.7. Let $\pi\colon \widetilde{C} \to C$ be a cover of degree d of curves defined over k and let $P \in C$. Then we have an induced inclusion of function fields $\pi^*\colon k(C) \to k(\widetilde{C})$. We define the *ramification index* of π at P by

$$e_{\pi,P} := \mathrm{ord}_P(\pi^*(t))$$

where t is a uniformizer of $\pi(P)$. We say that π is ramified at P if $e_{\pi,P} > 1$ and unramified at P otherwise. We say that π is ramified if there is a ramified point $P \in \widetilde{C}$ and is unramified otherwise. If the map π is clear from context then we use the notation e_P.

Proposition 2.4.8. *Let $\pi\colon \widetilde{C} \to C$ be a cover of curves. Then:*

(a) For all $Q \in C$ we have

$$\sum_{P \in \pi^{-1}(Q)} e_P = \deg(\pi).$$

(b) For all but finitely many P we have $e_P = 1$.

Proof. See [20, Proposition II.2.6]. □

By Proposition 2.4.8 (b) we define the following.

Definition 2.4.9. The *ramification divisor* of a cover $\pi\colon \widetilde{C} \to C$ is

$$\mathcal{R}_\pi := \sum_{P \in \widetilde{C}} (e_P - 1)P.$$

Definition 2.4.10. For any function $f \in \bar{k}(C)$ we define

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

By Proposition 2.3.5 this is well defined and degree 0. A divisor of the form $\mathrm{div}\, f$ is called a *principal divisor*.

Proposition 2.4.11. *Let $f, g \in k(C)$ and $c \in k^*$. Then since each* ord_P *is a valuation trivial on the constant functions we have:*

$$\begin{aligned} \mathrm{div}(fg) &= \mathrm{div}(f) + \mathrm{div}(g) \\ \mathrm{div}\left(\frac{1}{f}\right) &= -\mathrm{div}(f) \\ \mathrm{div}(c) &= 0. \end{aligned}$$

The above proposition allows us to give the following definition.

Definition 2.4.12. We denote by $\mathrm{Princ}(C)$ the subgroup of principal divisors in $\mathrm{Div}^0(C)$.

Definition 2.4.13. We define the *Picard group* $\mathrm{Pic}(C)$ by the exact sequence

$$0 \longrightarrow \mathrm{Princ}(C) \longrightarrow \mathrm{Div}(C) \longrightarrow \mathrm{Pic}(C) \longrightarrow 0$$

Similarly, define $\mathrm{Pic}^0(C)$ by the exact sequence

$$0 \longrightarrow \mathrm{Princ}(C) \longrightarrow \mathrm{Div}^0(C) \xrightarrow{[\cdot]} \mathrm{Pic}^0(C) \longrightarrow 0$$

The group $\mathrm{Pic}(C)$ is the divisor class group of C. We represent elements in $\mathrm{Pic}(C)$ by $[D]$ and call this the *divisor class* of D.

Definition 2.4.14. Let $\widetilde{C}, C$ be smooth projective curves and let $\pi\colon \widetilde{C} \to C$ be a cover. Let $D = \sum_{P \in C} n_P P$ be a divisor of C. We define the *pullback of* D, denoted $\pi^*(D)$, as

$$\pi^*(D) = \sum_{P \in D} \sum_{\pi(Q)=P} e_Q n_P Q$$

where e_Q is the ramification index of Q.

Lemma 2.4.15. *There is an induced morphism*

$$\pi^*\colon \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(\widetilde{C}).$$

Proof. It is straightforward to verify the claim that

$$\pi^*(\mathrm{div}(f)) = \mathrm{div}(f \circ \pi) = \mathrm{div}(\pi^*(f))$$

and hence the pullback of a principal divisor is again principal. Hence we get the induced map from the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Princ}(C) & \longrightarrow & \mathrm{Div}^0(C) & \longrightarrow & \mathrm{Pic}^0(C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \pi^*} & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Princ}(\widetilde{C}) & \longrightarrow & \mathrm{Div}^0(\widetilde{C}) & \longrightarrow & \mathrm{Pic}^0(\widetilde{C}) & \longrightarrow & 0 \end{array}$$

□

Definition 2.4.16. Let $\pi\colon \widetilde{C} \to C$ be a cover of curves. Then we define the map $\pi_*\colon \mathrm{Div}^0(\widetilde{C}) \to \mathrm{Div}^0(C)$ by

$$\pi_* \left(\sum_{P \in \widetilde{C}} n_P P \right) = \sum_{P \in \widetilde{C}} n_P \pi(P).$$

We call π_* the *norm*.

Definition 2.4.17. If $\sigma \in \mathrm{Aut}(\widetilde{C}/C)$ and $D = \sum_{P \in \widetilde{C}} a_P P$ is a divisor then we have the group action

$$\sigma_*(D) = \sum_{P \in \widetilde{C}} a_P \sigma(P).$$

The following appears as an exercise in [9] but proves to be useful to us later.

Lemma 2.4.18. *Let $\widetilde{C}, C, \pi$ be as before and let $P \in C$. If $\widetilde{C}/C$ is Galois then $\mathrm{Gal}(\widetilde{C}/C)$ acts transitively on the set*

$$\textit{fibre over } P := \left\{ Q \in \widetilde{C}(\bar{k}) : \pi(Q) = P \right\}.$$

Proof. Label the points in the fibre over P by $Q_1, \ldots, Q_n$. By [19, Theorem III.2.3] we find $t_i \in k(C)$ such that $\mathrm{ord}_{Q_j} t_i = \delta_{ij}$ where δ is the Kronecker delta. Since

$$\mathrm{Nm}_{\widetilde{C}/C}(t_1)(Q) = \prod_{\sigma \in \mathrm{Gal}(\widetilde{C}/C)} t_1(\sigma(Q))$$

is invariant under Galois action and vanishes at Q_1, it must vanish at each Q. That is, for every point such that $\pi(Q) = P$ there is a σ such that $t_1(\sigma(Q)) = 0$. Since t_1 had a unique root among the Q we are done. □

Remark 2.4.19. Our blanket assumption that $\mathrm{char}\, k \neq 2$ guarantees that a double cover of curves is always separable.

Lemma 2.4.20. *Let $\pi\colon \widetilde{C} \to C$ be a Galois cover of smooth projective curves of degree n. Let D be a divisor on C and $\widetilde{D}$ a divisor on $\widetilde{C}$. Then*

(i) $(\pi_* \circ \pi^*)(D) = nD$

(ii) $(\pi^* \circ \pi_*)(\widetilde{D}) = \sum_{\sigma \in \mathrm{Gal}(\widetilde{C}/C)} \sigma(\widetilde{D})$.

Proof.

(i) Let $P \in C(\bar{k})$. Then

$$\pi^*(P) = \sum_{\pi(Q)=P} e_Q Q$$

$$\pi_* \left(\sum_{\pi(Q)=P} e_Q Q \right) = \sum_{\pi(Q)=P} e_Q P = nP.$$

Now let $D = a_0 P_0 + \ldots + a_r P_r \in \mathrm{Div}(C)$. Then

$$\begin{aligned} \pi_*\pi^*(D) &= \pi_*\pi^*(a_0 P_0 + \ldots + a_r P_r) = a_0 \pi_*\pi^*(P_0) + \ldots + a_r \pi_*\pi^*(P_r) \\ &= nD. \end{aligned}$$

(ii) Let $Q \in \widetilde{C}(\bar{k})$ and let $\pi(Q) = P$. Then

$$\pi^*\pi_*(Q) = \sum_{\pi(Q')=P} e_{Q'} Q'.$$

Since $\widetilde{C}/C$ is Galois, the automorphisms act transitively on the fibre over P. Thus

$$\sum_{\sigma \in \mathrm{Gal}(\widetilde{C}/C)} \sigma(Q) = \sum_{Q' \in \mathrm{Orb}(Q)} |\mathrm{Stab}(Q)|\, Q' = \sum_{\pi(Q')=P} e_{Q'} Q'.$$

Now let $\widetilde{D} = a_0 P_0 + \ldots + a_r P_r \in \mathrm{Div}(C)$. Applying the same trick as before we obtain the result.

□

Lemma 2.4.21. *Let $\pi\colon \widetilde{C} \to C$ be a Galois cover of curves of degree n. Then there is an induced*

morphism of Picard groups $\pi_*\colon \operatorname{Pic}^0(\widetilde{C}) \to \operatorname{Pic}^0(C)$ *given by*

$$\pi_*\left(\left[\sum n_{P_i} P_i\right]\right) = \left[\sum n_{P_i} \pi(P_i)\right].$$

Proof. First we show that π_* takes principal divisors to principal divisors. By the morphism π there is an induced inclusion of function fields π^*. There is also the standard norm map $\operatorname{Nm}\colon k(\widetilde{C})^* \to k(C)^*$. We claim that

$$\begin{array}{ccc} k(\widetilde{C})^* & \xrightarrow{\text{div}} & \operatorname{Princ}(\widetilde{C}) \\ \downarrow{\scriptstyle \operatorname{Nm}} & & \downarrow{\scriptstyle \pi_*} \\ k(C)^* & \xrightarrow{\text{div}} & \operatorname{Princ}(C) \end{array}$$

commutes. First we show this for functions $g \in \pi^*(k(C)) \subseteq k(\widetilde{C})$. We see by Lemma 2.4.20 that

$$\pi_* \operatorname{div}_{\widetilde{C}}(g \circ \pi) = n \operatorname{div}_C g = \operatorname{div}_C \operatorname{Nm}(g).$$

Now let $\widetilde{g} \in k(\widetilde{C})^*$ and let $g = \operatorname{Nm}(\widetilde{g})$. Then since $\pi_*(\widetilde{g}) = \pi_*(\widetilde{g}^\sigma)$ for all $\sigma \in \operatorname{Aut}(\widetilde{C}/C)$ we have

$$n \cdot \pi_* \operatorname{div}_{\widetilde{C}}(\widetilde{g}) = \sum_{\sigma \in \operatorname{Aut}(\widetilde{C}/C)} \pi_* \operatorname{div}_{\widetilde{C}} \widetilde{g}^\sigma = \pi_* \operatorname{div}_{\widetilde{C}} \operatorname{Nm}(\widetilde{g}) = n \cdot \operatorname{div}_C g.$$

So π_* of principal divisors are still principal. Now consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Princ}(\widetilde{C}) & \longrightarrow & \operatorname{Div}^0(\widetilde{C}) & \longrightarrow & \operatorname{Pic}^0(\widetilde{C}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle \pi_*} & & \downarrow & & \\ 0 & \longrightarrow & \operatorname{Princ}(C) & \longrightarrow & \operatorname{Div}^0(C) & \longrightarrow & \operatorname{Pic}^0(C) & \longrightarrow & 0 \end{array}$$

We get an induced map between Picard groups. □

2.4.1 Riemann-Roch and Riemann-Hurwitz Theorems

We introduce the standard results for working with projective curves and in particular also define the genus of a curve. To that end we introduce a differential on a curve. At the end of this section we provide some explicit computational tools that allow us to determine the data used in these formulae.

Definition 2.4.22. We define the $\bar{k}(C)$-module of *Kähler differentials* Ω_C as the free $\bar{k}(C)$ module

generated by the symbols df for each $f \in \bar{k}(C)$ modulo the relations:

$$\begin{aligned} &d(f+g) - df - dg = 0 \\ &dfg - fdg - gdf = 0 \\ &da = 0 \qquad\qquad\qquad\qquad \text{for all } a \in \bar{k}. \end{aligned}$$

Proposition 2.4.23. *Let C be a curve, let $P \in C$, and let $t \in \bar{k}(C)$ be a unformizer at P.*

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

$$\omega = g \cdot dt.$$

We denote g by ω/dt.

(b) Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity

$$\mathrm{ord}_P(\omega/dt)$$

depends only on ω and P, independent of the choice of uniformizer t.

Proof. See [20, Proposition II.4.3]. □

This motivates the following definition:

Definition 2.4.24. Let ω be a differential on a smooth projective curve C, let $P \in C$, and t be a uniformizer at P. Then we define

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\omega/dt).$$

Proposition 2.4.25. *For a non-zero $\omega \in \Omega_C$ we have $\mathrm{ord}_P\,\omega = 0$ for all but finitely many P.*

Proof. See [20, Proposition II.4.3]. □

Definition 2.4.26. Let ω be a differential. Then its divisor is defined by

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

which is a divisor by the above proposition. We call this a *canonical divisor*.

Remark 2.4.27. Since any two non-trivial differentials are $k(C)$-multiples of each other we see that their divisors are all linearly equivalent. Thus we see that for non-zero $\omega \in \Omega_C$ we have that $[\operatorname{div}\omega] = \kappa \in \operatorname{Pic}(C)$ is independent of ω. We call κ the *canonical divisor class* of C.

We now finally approach the Riemann-Roch Theorem.

Definition 2.4.28. To a divisor D on a curve X we associate a $\bar{k}$-vector space called the *Riemann-Roch space* of D defined by

$$\mathcal{L}(D) = \left\{ f \in \bar{k}(X) : \operatorname{div} f + D \text{ is effective} \right\} \cup \{0\}.$$

Proposition 2.4.29. *$\mathcal{L}(D)$ is a finite dimensional $\bar{k}$-vector space.*

Proof. See [20, Proposition II.5.2b]. □

Definition 2.4.30. For notational convenience we define

$$\ell(D) := \dim_{\bar{k}} \mathcal{L}(D).$$

Remark 2.4.31. Let D be a divisor on C and let f be a function. Then as vector spaces

$$\mathcal{L}(D) \cong \mathcal{L}(D + \operatorname{div} f).$$

We mention this to point out that the statement of the next theorem is independent of the choice of canonical divisor.

Theorem 2.4.32 (Riemann-Roch)**.** *Let D be a divisor on C and let κ denote a canonical divisor. Let $\ell(D) = \dim \mathcal{L}(D)$. Then there exists an integer $g \geq 0$ depending only on C such that*

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

Proof. See [20, Theorem II.5.4]. □

Definition 2.4.33. For a given C the integer g in the above theorem is called the *genus* of C.

By substituting $D = 0$ and then $D = \kappa$ into the above theorem and observing that $\mathcal{L}(0)$ is the $\bar{k}$ vector space of constant functions we obtain:

Proposition 2.4.34. *For ℓ, g, k as above,*

$$\ell(\kappa) = g$$
$$\deg(\kappa) = 2g - 2.$$

Theorem 2.4.35 (Riemann-Hurwitz)**.** *Let $\pi : \widetilde{C} \to C$ be a cover of degree d such that the extension of function fields $k(\widetilde{C})/k(C)$ is separable and let e_P be the ramification index of $P \in \widetilde{C}$. Then*

$$\kappa_{\widetilde{C}} = \pi^* \kappa_C + \mathcal{R}_\pi.$$

If in addition we know $\operatorname{char}(k) \nmid e_P$ for each P or $\operatorname{char}(k) = 0$ then we take degrees to see

$$2g(\widetilde{C}) - 2 = d(2g(C) - 2) + \sum_{P \in \widetilde{C}} (e_P - 1).$$

Proof. See [20, Theorem II.5.9] and [10, Proposition A.2.2.8]. □

2.4.2 Computing ramification

Computing ramification data from the function fields

In order to make use of the Hurwitz formula we shall require information about the ramification divisor. This section highlights a means to obtain this.

Definition 2.4.36. Let F be a field. A *discrete valuation* on F is a map $\nu \colon F \to \mathbb{Z} \cup \{+\infty\}$ such that

(i) $\nu(a) = +\infty$ if and only if $a = 0$,

(ii) $\nu(ab) = \nu(a) + \nu(b)$,

(iii) $\nu(a + b) \geq \min(\nu(a), \nu(b))$, and

(iv) there exists an element $t \in F^*$ such that $\nu(t) = 1$.

The pair (F, ν) is called a *discrete valuation field*.

Let C be a smooth projective curve and $k(C)$ its function field. Let $P \in C$ be a point and

$\mathcal{O}_{C,P} \subseteq k(C)$ the associated local ring. This gives rise to a discrete valuation on $k(C)$ by defining

$$\nu_P(f) := \operatorname{ord}_P f.$$

In the form of a proposition:

Proposition 2.4.37. *To each point $P \in C(\bar{k})$ on a smooth projective curve we can associate a discrete valuation ν_P of $\bar{k}(C)$ with $\nu_P(a) = 0$ for all $a \in k$. Additionally, we see that the associated discrete valuation ring $\mathcal{O}_{C,P}$ contains $\bar{k}$ and the fraction field of $\mathcal{O}_{C,P}$ is $\bar{k}(C)$.*

Proposition 2.4.38. *Let C be a smooth projective curve and let $\mathcal{O}_\nu$ be a discrete valuation subring of $\bar{k}(C)$ containing $\bar{k}$ such that the fraction field of $\mathcal{O}_\nu$ is $\bar{k}(C)$. Then there is a point $P \in C(\bar{k})$ such that $\nu = \operatorname{ord}_P f$.*

Proof. See [8, Corollary 7.1.4]. □

The main advantage of this is that we can compute ramification of a cover of curves directly from the associated function fields. We state a well known result which allows us to easily compute the ramified places of a separable double cover.

Corollary 2.4.39. *Let $\pi\colon \widetilde{C} \to C$ be a separable cover of smooth projective curves and let $k(\widetilde{C}) = k(C)(\sqrt{f})$ for some non-zero $f \in k(C)$. Then*

$$P \in \widetilde{C} \text{ is ramified } \iff \operatorname{ord}_{\pi(P)}(f) \text{ is odd.}$$

Proof. For notational convenience we write $\bar{k}(\widetilde{C})$ as an extension of $\bar{k}(C)$ since $\pi^*\bar{k}(C) \subseteq \bar{k}(\widetilde{C})$. Let $\widetilde{P} \in \widetilde{C}(\bar{k})$ be a point and $P := \pi(\widetilde{P})$. Since $\widetilde{C}$ is smooth $\mathcal{O}_{\widetilde{C},\widetilde{P}}$ is the integral closure of $\mathcal{O}_{C,P}$ in $\bar{k}(\widetilde{C})$. (See [8, Problem 7.20].)

First we assume that $\operatorname{ord}_{\widetilde{C},\widetilde{P}} f$ is either 0 or 1. Notice

$$p(T) := T^2 - f$$

is the minimal polynomial for $\sqrt{f}$ over $\mathcal{O}_{C,P}$. Let S be the free $\mathcal{O}_{C,P}$ module generated by $\left\{1, \sqrt{f}\right\}$ and note that $S \subseteq \mathcal{O}_{\widetilde{C},\widetilde{P}}$. By [7, I.4 Proposition 6ii] and [7, I.3 Proposition 4i] we have

$$\operatorname{Nm}_{k(\widetilde{C})/k(C)}\left(p'(\sqrt{f})\right)\mathcal{O}_{C,P} = (4f)\mathcal{O}_{C,P} \subseteq \operatorname{Disc}(S/\mathcal{O}_{C,P})$$

where $\mathrm{Disc}(C/\mathcal{O}_{C,P})$ is the discriminant of S over $\mathcal{O}_{C,P}$ (See [7, I.3 Equation 4]). If $\mathrm{ord}_{C,P} f = 0$ then $4f$ is a unit and the discriminant contains $\mathcal{O}_{C,P}$. Thus $\mathrm{Disc}(S/\mathcal{O}_{\widetilde{C},\widetilde{P}}) = \mathcal{O}_{C,P}$ and by [7, I.5 Theorem 1] the extension $\bar{k}(\widetilde{C})/\bar{k}(C)$, as discrete valuation fields with discrete valuations $\mathrm{ord}_{\widetilde{C},\widetilde{P}}$ and $\mathrm{ord}_{C,P}$ (respectively), is unramified. That is, for a uniformizer $t \in \mathcal{O}_{C,P}$ we have

$$\mathrm{ord}_{\widetilde{C},\widetilde{P}}\, t = 1.$$

Therefore $\widetilde{P}$ is an unramified point of π. Otherwise, if $\mathrm{ord}_{C,P} f = 1$ then f is a uniformizer for $\mathcal{O}_{C,P}$. We see that

$$2 \cdot \mathrm{ord}_{\widetilde{C},\widetilde{P}} \sqrt{f} = \mathrm{ord}_{\widetilde{C},\widetilde{P}} f \geq 1.$$

Since $\mathrm{ord}_{\widetilde{C}} \sqrt{f}$ is an integer we have that $\mathrm{ord}_{\widetilde{C},\widetilde{P}} f > 1$. Thus $\widetilde{P}$ is a ramified point of π.

We now address the general case. Let t be a uniformizer for $\mathcal{O}_{C,P}$ and write $f = ut^{2m+r}$ where $u \in \mathcal{O}^*_{C,P}$, $m \in \mathbb{Z}$, and $r \in \{0, 1\}$. Then since $f \cdot t^{-2m} \in \mathcal{O}_{C,P}$ and

$$\left(\sqrt{f} \cdot t^{-m}\right)^2 - f \cdot t^{-2m} = 0$$

we have that $\sqrt{f} \cdot t^{-m}$ is integral over $\mathcal{O}_{C,P}$. Hence it is in $\mathcal{O}_{\widetilde{C},\widetilde{P}}$. We replace f with $f \cdot t^{-2m}$ in the previous argument to complete the proof. □

Hyperelliptic curves

Definition 2.4.40. A curve C is called *hyperelliptic* if $g(C) > 0$ and there is a degree 2 map $\pi \colon C \to \mathbb{P}^1$.

Remark 2.4.41. If $g(C) > 1$ then π is determined up to an automorphism of $\mathbb{P}^1$. This is quite interesting but we do not require this result. The alert reader will notice that we refer to "the hyperelliptic involution" instead of "a hyperelliptic involution".

Remark 2.4.42. Recall the characteristic of k is not 2. Thus for any hyperelliptic curve C defined over k we can find a squarefree $f \in k[x]$ such that

$$X := V(y^2 - f) \subseteq \mathbb{A}^2_k$$

is an affine model of C.

Any separable double cover of curves is automatically Galois. In particular a hyperelliptic curve C is a double cover of the projective line, so there is an automorphism of C corresponding to changing the branches of this cover.

Definition 2.4.43. Let C be a hyperelliptic curve double covering $\mathbb{P}^1$. The involution of C over $\mathbb{P}^1$ is called the *hyperelliptic involution*.

Hyperelliptic curves are interesting because they are very easy to construct and it is very easy to find the ramification locus of the map $\pi\colon C \to \mathbb{P}^1$, as demonstrated by the corollary below.

Corollary 2.4.44. *The ramification index of a point $P \in H$ with respect to the quotient by hyperelliptic involution on a hyperelliptic curve is 2 if P is invariant under the hyperelliptic involution and is 1 otherwise.*

Proof. Since the degree of the quotient map is 2 that means the ramification index of each point is either 1 or 2. By Proposition 2.4.8 we see that the result is immediate. □

2.5 Abelian varieties

In this section we make precise what types of objects we are classifying and describe Jacobian varieties. For a deeper look into the theory of abelian varieties the reader is encouraged to refer to [13] or [14].

2.5.1 Definition and properties of abelian varieties

Definition 2.5.1. Let A be a smooth projective variety defined over k and O some distinguished point over k on A. Furthermore suppose there are morphisms

$$\begin{aligned} +\colon A \times A &\to A \\ [-1]\colon \quad A &\to A \end{aligned}$$

satisfying the usual associativity, inverse, and identity conditions. Then we call the quadruple $(A, O, +, [-1])$ an *abelian variety*. We will refer to this data by A when the group structure is clear from context.

We should point out that [14] begins with a different definition and then shows that the definition given here is equivalent.

Theorem 2.5.2. *The triple* $(A(\bar{k}), +, O)$ *defines a commutative group.*

Proof. See [14, Corollary I.1.4].

□

Definition 2.5.3. We say that a morphism $\phi\colon A \to B$ of varieties is a morphism of abelian varieties $(A, +_A, O_A, -1_A) \to (B, +_B, O_B, -1_B)$ provided that $\phi(O_A) = O_B$ and $\phi(P +_A Q) = \phi(P) +_B \phi(Q)$ for all $P, Q \in A$.

Remark 2.5.4. The fibre over O_B characterizes the fibre structure of the map ϕ. For any point $P \in B$ choose a Q such that $\phi(Q) = P$. Then by additivity of ϕ we have that

$$\phi^{-1}(P) = \left\{Q' \in A : Q' +_A [-1]_A Q \in \phi^{-1}(O_B)\right\}.$$

Since ϕ is a morphism on the level of groups we call $\phi^{-1}(O_B)$ the *kernel*.

We highlight a particularly useful family of morphisms.

Definition 2.5.5. The *multiplication by* m *morphism*, denoted $[m]$, is defined by

$$[m]P := \underbrace{P + \ldots + P}_{m \text{ times}}.$$

Its kernel is called the m-torsion of A and is denoted $A[m]$.

Remark 2.5.6. Since $[m]$ is a morphism, $\{O_A\}$ is Zariski-closed, and the pullback of a Zariski-closed set by a morphism is also Zariski-closed, we see $A[m]$ can be given the structure of an algebraic set. By [14, Theorem I.7.2] $\#A[m]$ is finite.

We shall now proceed to define an important type of morphism of abelian varieties and show that this gives rise to a type of invariant known as the isogeny class. We then sharpen this informally so that we may frame our motivating classification question in the correct language.

Definition 2.5.7. An *isogeny* of abelian varieties $\phi : A \to B$ is a surjective morphism of abelian varieties with finite kernel. If an isogeny exists we say that A is *isogenous* to B, denoted $A \sim B$.

Lemma 2.5.8. *Let* $U \subseteq A$ *be a non-empty Zariski-open set. Then the collection of translates of* U

$$\bigcup_{P \in U} U_P := \{Q \in A : Q - P \in U\}$$

is an open cover of A.

Proof. It suffices to show that there is a translate U' of U containing the identity since $0 \in U'$ implies $Q \in U'_Q$. Observe that since $[-1]$ is an automorphism we have

$$U \cap [-1]U$$

is an open set. Since A is a variety, the intersection of any two non-empty open sets is again non-empty so we may pick a point $P \in U \cap [-1]U$. Immediately $0 \in U_P$ and the rest of the result follows. □

Lemma 2.5.9. *$A \sim B$ is an equivalence relation.*

Proof. See [14, Remark 8.6]. □

Lemma 2.5.10. *Let $\phi\colon A \to B$ and $\tau\colon A \to C$ be isogenies defined over k such that $\tau^*(k(C)) \subseteq \phi^*(k(B)) \subseteq k(A)$. Then there exists an isogeny $\psi\colon B \to C$ defined over k such that $\tau = \psi \circ \phi$.*

Proof. Since ϕ and τ are isogenies they are surjective (and hence dominant). So $\phi^*(k(B)) \cong k(B)$ and $\tau^*(k(C)) \cong k(C)$. Thus there exists a rational map $\psi\colon B \to C$ such that $\tau = \psi \circ \phi$ on the open set for which ψ is defined. In particular, this means that whenever $P, Q, P+Q \in U$ we have

$$\psi(P+Q) = \psi(\phi(P') + \phi(Q')) = \tau(P'+Q') = \psi(\phi(P')) + \psi(\phi(Q')) = \psi(P) + \psi(Q).$$

On each open set U_P we define ψ_P by

$$\psi_P(Q) := \psi(Q - P) + \psi(P)$$

and define

$$\widetilde{\psi} := (U_P, \psi_P)_{P \in U}.$$

To clarify the above definition, we mean for each U_P and each $Q \in U_P$ that

$$\widetilde{\psi}(Q) := \psi_P(Q).$$

We see this is well defined since $\widetilde{\psi}(Q)$ is independent of the choice of open set containing Q. By Lemma 2.5.8 the open sets are a cover of C. It is not much more work to show that $\widetilde{\psi}$ is a legitimate

morphism from B to C such that $\widetilde{\psi}\Big|_U = \psi$. Finally,

$$\widetilde{\psi}(0_B) = \widetilde{\psi}(0_B) + \widetilde{\psi}(0_B) \Rightarrow \widetilde{\psi}(0_B) = 0_C$$

and $\widetilde{\psi}$ is surjective since $\tau = \widetilde{\psi} \circ \phi$ is. Thus $\widetilde{\psi} : B \to C$ is an isogeny. □

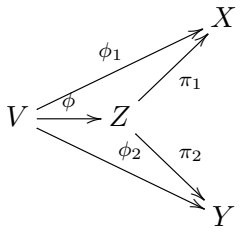
Definition 2.5.11. The *isogeny class* of A is the $(\sim)$-equivalence class of A.

Next we introduce the *product* abelian variety. We will need a couple of definitions before proceeding.

Proposition 2.5.12. *Let X, Y be projective varieties defined over k. Then there is a projective variety Z unique up to isomorphism such that*

(a) There are morphisms π_1, π_2 defined over k such that $\pi_1 \colon Z \to X$ and $\pi_2 \colon Z \to Y$ are surjective.

(b) For any projective variety V admitting morphisms ϕ_1, ϕ_2 into X and Y (respectively) there exists a unique morphism $\phi \colon V \to Z$ such that the following diagram commutes:



Proof. See [19, I.5.1] or [8, 6.4.6]. □

Definition 2.5.13. The Z produced by the above theorem is called the *product variety* of X and Y and we write $Z = X \times_k Y$.

Proposition 2.5.14. *Let $Z = X \times_k Y$. If $P \in X(\bar{k})$ and $Q \in Y(\bar{k})$ are smooth points then $(P, Q) \in Z(\bar{k})$ is a smooth point as well.*

Proof. It suffices to check smoothness locally so we choose affine open sets U_x, U_y containing P, Q respectively and notice that $U_x \times U_y$ is an affine open subset of Z containing P, Q. Then

$$\mathcal{O}_Z(U_x \times_{\bar{k}} U_y) \cong \mathcal{O}_X(U_x) \otimes_{\bar{k}} \mathcal{O}_Y(U_y).$$

(See [19, Examples I.2.1.5, I.2.2.4]). By $\mathcal{O}_X(U_x)$ we mean the affine co-ordinate ring of the affine variety U_x. We then verify that

$$\mathcal{O}_{Z,(P,Q)}(U_x \times_{\bar{k}} U_y) \cong \mathcal{O}_{X,P}(U_x) \otimes_{\bar{k}} \mathcal{O}_{Y,Q}(U_y).$$

and that for the associated maximal ideals

$$\dim_k \mathfrak{M}_{(P,Q)}/\mathfrak{M}^2_{(P,Q)} = \dim_{\bar{k}} \mathfrak{M}_P/\mathfrak{M}^2_P + \dim_{\bar{k}} \mathfrak{M}_Q/\mathfrak{M}^2_Q = \dim X + \dim Y = \dim Z$$

so smoothness is verified. □

Proposition 2.5.15. *Let $(A, O_A, +_A, [-1]_A), (B, O_B, +_B, [-1]_B)$ be abelian varieties. Let*

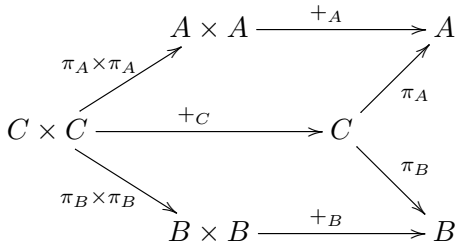
$$\begin{aligned} C &= A \times_k B \\ O_C &= (O_A, O_B) \in C \\ +_C &= (+_A, +_B) \\ [-1]_C &= ([-1]_A, [-1]_B). \end{aligned}$$

Then $(C, O_C, +_C, [-1]_C)$ is an abelian variety defined over k.

Proof. We remark that since A and B are smooth projective varieties defined over k then so is C. We need to show that

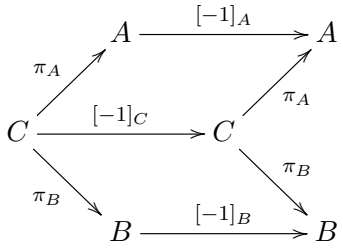
- $+_C$ is a morphism on the level of varieties.

  Since C is the product object, there is a map $+_C$ such that the following diagram commutes:



- $[-1]_C$ is a morphism.

As before we see commutativity of the diagram



gives us the result.

- O_C is the identity.

  First we show that $O_C +_C P = P +_C O_C = P$. By definition we have $\pi_A(O_C) = O_A$ and $\pi_B(O_C) = O_B$. Since

  $$\pi_A(P) + O_A = \pi_A(P)$$

  $$\pi_B(P) + O_B = \pi_B(P)$$

  and $C = A \times_k B$, we must have that

  $$P + O_C = P.$$

  A similar proof works for the other equality.

- $+_C$ is associative.

  Again we have for $P, Q, R \in C$ that

  $$\pi_A(P) + (\pi_A(Q) + \pi_A(R)) = (\pi_A(P) + \pi_A(Q)) + \pi_A(R)$$

  $$\pi_B(P) + (\pi_B(Q) + \pi_B(R)) = (\pi_B(P) + \pi_B(Q)) + \pi_B(R).$$

  Therefore $P + (Q + R) = (P + Q) + R$.

- $[-1]_C$ is inverse.

  Same trick.

□

Definition 2.5.16. A *k-isogeny factor* of an abelian variety C defined over k is a non-zero abelian variety A defined over k such that there exists an abelian variety B defined over k such that there is an isogeny $\phi\colon A \times B \to C$ defined over k.

2.5.2 Definition and properties of the Jacobian

In this section we will define the Jacobian variety of a curve as the abelian variety with the same group structure as the Picard group of the curve and discuss how maps of curves give rise to induced morphisms of their Jacobians. Again the interested reader is directed to [14, Section III].

Theorem 2.5.17. *Let C be a smooth projective curve. Then there is an abelian variety called the* Jacobian *of C such that in a natural way:*

$$J(C)(\bar{k}) \cong \mathrm{Pic}^0(C).$$

By natural we mean that given a surjective morphism of curves $\pi\colon \widetilde{C} \to C$ we have $\pi^*\colon J(C) \to J(\widetilde{C})$ and $\pi_*\colon J(\widetilde{C}) \to J(C)$ are morphisms as abelian varieties.

Proof. See [14, Theorem III.1.2, Remark III.1.4a]. □

Theorem 2.5.18. *If C is a smooth projective curve then* $\dim J(C) = g(C)$.

Proof. See [14, Proposition III.2.1]. □

2.5.3 Polarizations, principal polarizations, and polarized isogenies

The purpose of this section is to emphasize that the decompositions of Jacobian varieties as principally polarized abelian varieties are indeed quite stringent and worth pointing out whenever they occur. We only need formal properties of polarizations so the definitions we state here are incomplete. A proper treatment of polarizations and the definition of the dual abelian variety is beyond the scope of this thesis but can be found in [13] or [14].

Proposition 2.5.19. *If A is an abelian variety then there is a* dual abelian variety *denoted $A^\vee$. We also call $A^\vee$ the* Picard Variety *of A and denote it by* $\mathrm{Pic}(A)$.

Proposition 2.5.20. *Let A be an abelian variety and $A^\vee$ its dual. Then*

$$\dim A = \dim A^\vee.$$

Proof. See [14, Remark I.8.7e]. □

Proposition 2.5.21. *Let A, B be abelian varieties. Then $(A \times B)^\vee \cong A^\vee \times B^\vee$.*

Proof. See [13, Proposition IV.4.7]. □

Definition 2.5.22. A *polarization* is a special type of isogeny $\lambda\colon A \to A^\vee$. A polarization is said to be *principal* if $\#\ker\lambda = 1$. A pair consisting of an abelian variety and a specified (principal) polarization is called a *(principally) polarized abelian variety*.

Proposition 2.5.23. *If $\lambda \in \mathrm{Hom}(A, A^\vee)$ is a polarization and $n \in \mathbb{Z}$ is nonzero then $n\lambda \neq 0$.*

Proof. See [14, Lemma I.10.6] or [14, Lemma I.10.18]. □

Proposition 2.5.24. *If $\phi\colon A \to B$ is an isogeny of abelian varieties then there is an induced isogeny $\phi^\vee\colon B^\vee \to A^\vee$ of the same degree.*

Proof. See [14, Theorem I.9.1]. □

Definition 2.5.25. Let $(A, \lambda_A), (B, \lambda_B)$ be polarized abelian varieties. Then an isogeny $\phi\colon A \to B$ is said to *respect polarizations* if there are non-zero $n, m \in \mathbb{Z}$ such that the diagram

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

commutes. As it turns out $\frac{n}{m} = \pm\frac{\deg\lambda_B\cdot(\deg\phi)^2}{\deg\lambda_A}$. We say ϕ is a *polarized isogeny*.

Proposition 2.5.26. *The map $[n]\colon A \to A$ respects polarizations.*

Proof. Direct from definitions and the fact that $[n]_A^\vee = [n]_{A^\vee}$. □

Polarized abelian varieties, together with morphisms of abelian varieties respecting polarizations, define a category. We discuss some of the properties of this category in that there are products and the universal property of quotients.

Proposition 2.5.27. *Let $(A, \lambda_A), (B, \lambda_B)$ be polarized abelian varieties. Then $(A \times B, \lambda_A \oplus \lambda_B)$ is the product object in the category of polarized abelian varieties.*

Proof. This is immediate from the fact that $A \times B$ is the product object in the category of abelian varieties and the choice of polarization on $A \times B$. □

Proposition 2.5.28. *Let $\alpha\colon (A, \lambda_A) \to (B, \lambda_B)$ and $\beta\colon (A, \lambda_A) \to (C, \lambda_C)$ be isogenies of principally polarized abelian varieties such that $\beta^*(k(C)) \subseteq \alpha^*(k(B))$. Let $\gamma\colon B \to C$ be the unique morphism such that $\beta = \gamma \circ \alpha$. Then γ respects polarizations.*

Proof. Let $n_\alpha = \deg \alpha$ and $n_\beta = \deg \beta = \deg \gamma \cdot \deg \alpha$. Since $\deg \alpha$ divides $\deg \beta$ there is an $m \in \mathbb{Z}$ such that $n_\beta = mn_\alpha =: n$. Since α and β respect polarizations and $\beta^\vee = \alpha^\vee \circ \gamma^\vee$ we have that

$$\begin{aligned} n\lambda_A &= \alpha^\vee \circ m\lambda_B \circ \alpha \\ n\lambda_A &= \beta^\vee \circ \lambda_C \circ \beta \\ &= \alpha^\vee\gamma^\vee \circ \lambda_C \circ \gamma\alpha. \end{aligned}$$

So $\alpha^\vee(\gamma^\vee \circ \lambda_C \circ \gamma - m\lambda_B)\alpha = 0$. Since α is surjective we see that $\alpha^\vee(\gamma^\vee \circ \lambda_C \circ \gamma - m\lambda_B) = 0$ and hence $\operatorname{Im}(\gamma^\vee \circ \lambda_C \circ \gamma - m\lambda_B) \subseteq \ker \alpha^\vee$. But $\alpha^\vee$ is an isogeny of degree n_α (Proposition 2.5.24) so

$$0 = [n_\alpha](\gamma^\vee \circ \lambda_C \circ \gamma - m\lambda_B).$$

It follows that

$$\begin{array}{ccc} B & \xrightarrow{n_\alpha m\lambda_B} & B^\vee \\ {\scriptstyle\gamma}\downarrow & & \uparrow{\scriptstyle\gamma^\vee} \\ C & \xrightarrow{n_\alpha\lambda_C} & C^\vee \end{array}$$

commutes. □

We end this section by noting Jacobian varieties can be considered as polarized abelian varieties and state the some important results regarding polarizations on Jacobian varieties.

Proposition 2.5.29. *The Jacobian variety of a curve C admits a canonical principal polarization coming from C, denoted by λ_C.*

Proposition 2.5.30. *Let $\pi\colon \widetilde{C} \to C$ be a morphism of curves and $\pi^*\colon J(\widetilde{C}) \to J(C)$ the induced*

map on the Jacobians. Let $\lambda_{\widetilde{C}}, \lambda_C$ be the canonical polarizations on $J(\widetilde{C}), J(C)$ respectively. Then

$$\begin{array}{ccc} J(\widetilde{C}) & \xrightarrow{\lambda_{\widetilde{C}}} & J(\widetilde{C})^\vee \\ \downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle (\pi^*)^\vee} \\ J(C) & \xleftarrow{\lambda_C^{-1}} & J(C)^\vee \end{array}$$

commutes.

Proof. See [15, Section 1]. □

Proposition 2.5.31. *Let C be a curve defined over $\bar{k}$ and let $P \in C(\bar{k})$. Then there exists a morphism $j_P \colon C \to J(C)$ defined by*

$$j_P(Q) := [Q - P]$$

where $[Q-P]$ is the point on $J(C)$ corresponding to the element $[Q-P] \in \mathrm{Pic}^0(C)$. (See Theorem 2.5.17.)

Proof. See [10, Theorem A.8.1.1]. □

Theorem 2.5.32 (Torelli)**.** *Let C and C' be smooth projective curves over an algebraically closed field k, and let $j_P \colon C \to J$ and $j_{P'} \colon C' \to J'$ be the maps of C and C' into their Jacobians defined by points P and P' on C and C'. Let $\beta \colon (J, \lambda_C) \to (J', \lambda_{C'})$ be an isomorphism from the canonically polarized Jacobian of C to that of C'.*

(a) There exists an isomorphism $\alpha \colon C \to C'$ such that $j_{P'} \circ \alpha = \pm\beta \circ j_P + c$ for some c in $J'(k)$.

(b) Assume that C has genus ≥ 2. If C is not hyperelliptic, then the map α, the sign $\pm$; and c are uniquely determined by β, P, P'. If C is hyperelliptic, the sign can be chosen arbitrarily, and then α and c are uniquely determined.

Proof. See [14, Theorem III.12.1]. □

2.5.4 Decompositions of the Jacobian

Up until now we have merely treated the Jacobian variety as an abstract group and mentioned that the group aspects we had talked about correspond to geometric operations. We now discuss decompositions of Jacobian varieties *as abelian varieties*.

Definition 2.5.33. Let A, B and C be nontrivial principally polarized abelian varieties. We say that C *decomposes as polarized abelian varieties* into A and B if there exists a polarized isogeny ϕ such that

$$\phi\colon A \times B \to C.$$

We highlight the particular type of decomposition we are interested in.

Definition 2.5.34. Let $\phi\colon A \times B \to C$ be a decomposition as polarized abelian varieties of C into non-trivial principally polarized abelian varieties. Suppose that $\psi\colon A[n] \to B[n]$ is an isomorphism both as abstract groups and as algebraic sets. If

$$\ker \phi = \{(a, -\psi(a)) \in A[n] \times B[n] : a \in A[n]\}$$

we say that C is the principally polarized abelian variety obtained by *gluing A and B along their n-torsion*.

2.6 Endomorphisms of abelian varieties

Let A be an abelian variety.

Definition 2.6.1. An *endomorphism* of A is a morphism of abelian varieties $\phi\colon A \to A$ such that $\phi(0_A) = 0_A$ and $\phi(x + y) = \phi(x) + \phi(y)$.

- The identity morphism $\mathbb{1}$ is an endomorphism. It is defined over k.
- The trivial morphism 0 defined by $0(x) = 0_A$ is also a morphism defined over k.

Proposition 2.6.2. *If ϕ, ψ are endomorphisms of A then $\phi + \psi$, $\phi \circ \psi$ are also an endomorphisms.*

Proof. The ring criteria are straightforward to check and the composition of morphisms of abelian varieties is also a morphism of abelian varieties. Thus we conclude $\phi \circ \psi$ is an endomorphism of abelian varieties. All that is left to assert is that $\phi + \psi$ is a morphism as varieties. But we see by the diagram

$$A \xrightarrow{\text{diag}} A \times A \xrightarrow{\phi \oplus \psi} A \times A \xrightarrow{+} A$$

that $\phi + \psi$ is a composition of morphisms of varieties. On the level of groups we see that for $P, Q \in A$

$$(\phi + \psi)(O_A) = \phi(O_A) + \psi(O_A) = O_A$$

$$(\phi+\psi)(P+Q)=\phi(P)+\phi(Q)+\psi(P)+\psi(Q)=(\phi+\psi)(P)+(\phi+\psi)(Q).$$

□

Proposition 2.6.3. *There exists an endomorphism* $[-1]$ *which satisfies the inverse properties that one would expect. Namely for any endomorphism* ϕ *we have* $[-1]\circ\phi=\phi\circ[-1]$ *and* $\phi+[-1]\circ\phi=0$.

Proof. Since A is an abelian variety there is an inverse morphism $[-1]_A$. Let $P\in A$. Then

$$(\phi+[-1]_A\phi)(P)=\phi(P)+[-1]_A\phi(P)=0$$

$$\phi([-1]_AP)+\phi(P)=\phi(P+[-1]_AP)=\phi(0)=0.$$

□

These lead to the natural definition:

Definition 2.6.4. The *endomorphism ring* of an abelian variety $\mathrm{End}(A)$ is the ring with ring structure $(0,\mathbb{1},+,\circ)$ specified above.

$\mathrm{End}(A)$ gives us a lot of useful information about A. Since abelian varieties are projective we get the following lemma:

Lemma 2.6.5. *Let* $\phi\in\mathrm{End}(A)$. *Then* $\phi(A)$ *is a sub-abelian variety of* A.

Lemma 2.6.6. *Let* $\widetilde{C},C$ *be curves,* $\pi\colon\widetilde{C}\to C$, *and* $\sigma\in\mathrm{Aut}(\widetilde{C}/C)$. *Then the action of* σ_* *on* $\mathrm{Div}^0(\widetilde{C})$ *induces an endomorphism of* $J(\widetilde{C})$ *by*

$$\sigma_*([D])=[\sigma_*(D)].$$

Moreover, $\pi_*\circ\sigma_*=\pi_*$ *and* $\sigma_*\circ\pi^*=\pi^*$.

Proof. First we have to show that $\sigma_*(\mathrm{Princ}(\widetilde{C}))\subseteq\mathrm{Princ}(\widetilde{C})$. Let

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

be a principal divisor. Then

$$\sigma_*(D)=\sum_{P\in\widetilde{C}}a_P\sigma(P).$$

We see $\sigma_*(D)$ is exactly $\mathrm{div}(f \circ \sigma^{-1})$, which is a well defined function of C. Thus σ_* acts compatibly on divisor classes. We also infer that $\sigma_*([0]) = [0]$ and that $\sigma_*([D]+[D']) = \sigma_*([D])+\sigma_*([D'])$. Since $\sigma\colon \widetilde{C} \to \widetilde{C}$ by Theorem 2.5.17 we assert that σ_* is a morphism on the level of varieties. Since $\pi \circ \sigma = \pi$, we have that

$$\pi_* \circ \sigma_* \left(\sum_{P \in \widetilde{C}} a_P P \right) = \sum_{P \in \widetilde{C}} a_P \pi(\sigma P) = \pi_* \left(\sum_{P \in \widetilde{C}} a_P P \right).$$

We also see that

$$\begin{aligned} \sigma_* \circ \pi^* \left(\sum_{P \in C} a_P P \right) &= \sigma_* \left(\sum_{P \in C} \sum_{\pi(Q)=P} e_Q n_P Q \right) \\ &= \sum_{P \in C} \sum_{\pi(Q)=P} e_Q n_P \sigma(Q). \end{aligned}$$

But $\pi \circ \sigma = \pi$, so points in the fibre over P go to points in the fibre over P. Thus $\sigma_* \circ \pi^* = \pi^*$. □

Remark 2.6.7. The morphism in $\mathrm{End}(J(C))$ induced by σ is denoted by σ_*.

Definition 2.6.8. Let R be a (not necessarily commutative) ring. An *idempotent* of R is an element $\epsilon \in R$ such that $\epsilon^2 = \epsilon$.

Endomorphism rings give us all the information we need to determine the isogeny factors of an abelian variety. This is due to the classical result of Kani and Rosen [12], which we state with the aid of the following lemma.

Lemma 2.6.9. $\mathrm{End}(A)$ *is torsion-free. Equivalently, the map* $\mathrm{End}(A) \to \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *given by* $\phi \to \phi \otimes 1$ *is an injection.*

Proof. See [14, Lemma I.10.6]. □

Theorem 2.6.10 (Kani-Rosen)**.** *Let A be an abelian variety. Let $\epsilon_1, \ldots, \epsilon_n \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ be idempotents. Then idempotent relations correspond to isogeny relations between abelian varieties. In particular,*

(a) If $\epsilon \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an idempotent then we may find an $m \in \mathbb{Z}$ such that $m \cdot \epsilon \in \mathrm{End}(A)$. Moreover $m\epsilon(A)$ is also an abelian variety.

(b) if $\sum_i \epsilon_i = \mathbb{1}$ *then there is an integer* m *such that*

$$A \sim m\epsilon_1 A \times \ldots \times m\epsilon_n A$$

and conversely, if $A \sim B_1 \times \ldots \times B_n$ *then we may find idempotents* $\epsilon_1, \ldots, \epsilon_n$ *and integers* m_i *such that*

$$m_i\epsilon_i(A) \sim B_i$$

and

$$A \sim m_1\epsilon_1 A \times \ldots \times m_n\epsilon_n A.$$

2.7 Final preliminaries

This last section covers some technical lemmas and contextual results which we isolate here in order to improve readability of the next chapter.

2.7.1 Motivating facts for the case $g = 2$

The following results classify all principally polarized abelian varieties of dimension 2. This greatly simplifies the types of decompositions that we need to consider since we are only looking for Jacobian factors.

Proposition 2.7.1. *Every genus 2 curve is hyperelliptic.*

Proof. Observe that the Riemann-Roch space of the canonical divisor has dimension 2. Choosing a basis $\langle f, g\rangle$ we see that the map

$$(f, g) : C \to \mathbb{P}^1$$

$$P \to (f(P) : g(P))$$

is surjective and extends to a morphism on all of C. Both f and g are degree at most 2 since this is the degree of the canonical divisor so the map has degree at most 2. The map has degree greater than 1 since $g(C) > 0$. □

Theorem 2.7.2. *Every principally polarized 2-dimensional abelian variety is either the Jacobian variety of some hyperelliptic curve* C *or is a product of elliptic curves* $E_1 \times E_2$.

Proof. See [21, Satz 2]. □

2.7.2 Representing 2-torsion points on hyperelliptic Jacobians

In this section we shall provide a concrete specification of the 2-torsion of the Jacobian of a hyperelliptic curve. We will represent these 2-torsion classes by divisors supported on special points of the curve that are easy to identify.

Definition 2.7.3. A *Weierstrass point* on a genus 2 curve is a point P such that

$$\ell(2P) > 1.$$

This is a bit of an awkward definition for our purposes, so we provide a practical criterion

Theorem 2.7.4. *Let $\pi\colon C \to \mathbb{P}^1_x$ be a hyperelliptic curve with hyperelliptic involution ι. Then $P \in C$ is a Weierstrass point if and only if $e_P > 1$.*

Proof. Let t be a uniformizer for $\pi(P) \in \mathbb{P}^1_x$. The reverse direction is easy since $\langle 1, \frac{1}{t}\rangle \subseteq \mathcal{L}(2P)$. For the forward direction let $P \in C$ such that $P \neq \iota(P)$. Then

$$\mathcal{L}(2P), \mathcal{L}(2\iota(P)) \subseteq \mathcal{L}(2(P + \iota(P))).$$

So by the Riemann-Roch theorem

$$\ell(2(P + \iota(P))) = 3.$$

Clearly $\mathcal{L}(2(P + \iota(P))) = \langle 1, \frac{1}{t}, \frac{1}{t^2}\rangle$. Any $\bar{k}$-linear combination of these functions has equal valuations at P and $\iota(P)$ so

$$\mathcal{L}(2P) = \mathcal{L}(2P) \cap \mathcal{L}(2P + 2\iota(P)) = \langle 1\rangle.$$

□

Theorem 2.7.5 (Hilbert 90)**.** *Let L/K be a finite cyclic extension of fields with $Gal(L/K) = \langle\sigma\rangle$ and let $f \in L$. Then $\mathrm{Nm}_{L/K}(f) = 1$ if and only if there is a $g \in L$ such that $f = \frac{g}{g^\sigma}$.*

Proof. See [5, 14.2 Exercise 23]. □

Lemma 2.7.6. *Let $\pi : \widetilde{C} \to C$ be a double cover of curves with $\mathrm{Aut}(\widetilde{C}/C) = \langle\sigma\rangle$. Then for any divisor class $[D] \in J(\widetilde{C})$ with $\sigma_*[D] = [D]$ we may find a divisor D' of $\widetilde{C}$ (not necessarily defined over k) such that $\sigma_* D' = D'$ and $[D] = [D']$.*

Proof. Let D be a representative for $[D]$. Since $\sigma_*[D] = [D]$ we have that $\sigma_* D - D = \operatorname{div} f$ for some $f \in \bar{k}(\widetilde{C})$. Then

$$\operatorname{div} f^\sigma + \operatorname{div} f = 0$$

and in particular $f \cdot f^\sigma$ is a constant which we may assume to be 1. Since the Galois group is a finite cyclic extension and the norm of f is 1 we may apply Hilbert 90 to find $g \in k(\widetilde{C})$ such that

$$f = \frac{g}{g^\sigma}.$$

Now

$$\begin{aligned} \sigma D - D &= \operatorname{div}(g) - \operatorname{div}(g^\sigma) \\ \Rightarrow \sigma D + \operatorname{div}(g^\sigma) &= D + \operatorname{div}(g). \end{aligned}$$

Taking $D' = D + \operatorname{div}(g)$ completes the proof. □

Lemma 2.7.7. *Let C be a hyperelliptic curve and $[D] \in \operatorname{Pic}^0(C)[2]$. Then we can find a representative $D \in \operatorname{Div}^0(C)$ such that D is supported only on the Weierstrass points of C.*

Proof. Let σ be the hyperelliptic involution and observe that a 2-torsion class must satisfy $\sigma([D]) = -[D] = [D]$. Moreover the cover $\pi\colon C \to \mathbb{P}^1$ is finite and cyclic, so by the previous lemma we can find a divisor D' such that

$$D' = \sum_{\theta_i \text{ Weierstrass points}} a_i \theta_i + \pi^*(\mathfrak{a})$$

where $\mathfrak{a} \in \operatorname{Div}(\mathbb{P}^1)$. Since $\pi^*(\mathfrak{a}) \sim \deg(\mathfrak{a}) \cdot \theta_i$ we are done. □

Chapter 3

Curves of genus $2g$ with decomposable Jacobians

3.1 Introduction

In this chapter we shall make use of the terminology and machinery referenced in the previous chapter and prove the main result of this thesis.

Definition 3.1.1. Let G and H be finite abelian groups and let $\psi\colon G \to H$ be an isomorphism. We call the subgroup

$$\Delta := \left\{(g,h) \in G \times H : h = \psi(g)^{-1}\right\}$$

the *anti-diagonal* of $G \times H$.

Definition 3.1.2. Let S_2 be the symmetric group on 2 elements. Let V be a variety, let $\mathcal{M}$ be a set of varieties, and let $\mathcal{P}_2$ be the set of pairs in $\mathbb{P}^1_k(\bar{k}) \times \mathbb{P}^1_k(\bar{k})/S_2$ such that

(i) $P_1 \neq P_2$

(ii) either P_1, P_2 are both k-rational points or P_1 is the quadratic conjugate of P_2.

Then a *two parameter family* (associated to V) is the image of a map of sets $\varphi\colon \{V\} \times \mathcal{P}_2 \to \mathcal{M}$.

Remark 3.1.3. The definition we use for a two-parameter family is sufficient to state the main result but lacks the requirements for φ to be continuous and for independence of the parameters. It is beyond the scope of this thesis to provide a full treatment of parameter families.

Theorem (Main Result)**.** *Let k be a field of characteristic not equal to 2. Let C_f be a hyperelliptic genus g curve defined over k, and $J(C_f)$ its Jacobian. Then we may find a two parameter family of explicitly determined curves C_F of genus g and A of genus $2g$ such that*

1. *C_F is hyperelliptic and there is an isomorphism of finite algebraic sets $\psi\colon J(C_F)[2] \to J(C_f)[2]$.*
2. *A is a double cover of C_F.*
3. *$J(A) \cong J(C_f) \times J(C_F)/\Delta$ as polarized abelian varieties, where Δ is the (anti)-diagonal of $J(C_f)[2] \times J(C_F)[2]$.*

Proposition 3.1.4. *Let A be a genus $2g$ double cover of a hyperelliptic genus g curve C_F, which double covers $\mathbb{P}^1_x$. Let Ω be the Galois closure of $A/\mathbb{P}^1_x$ and assume that $A \neq \Omega$. Then $\mathrm{Gal}(\Omega/\mathbb{P}^1_x) \cong D_4$. Moreover, there is a choice of C_f and parameters as in the above theorem where we recover A and C_F.*

It is useful to know when this occurs for a number of reasons since $J(A)$ decomposing in this way may allow us to say something interesting about either A or one of the component Jacobians. We list some potential applications:

- The endomorphism ring of $J(A)$ can inherit special properties of the endomorphism rings of $J(C_F)$ and $J(C_f)$.
- We can show any principally polarized abelian of dimension 2 arises as an isogeny factor (defined over k) of a Jacobian of a genus 4 curve. More generally, we can show any hyperelliptic g-dimensional Jacobian arises as an isogeny factor defined over k of some Jacobian of a genus $2g$-curve.

The proof of the main result will proceed as follows. First we shall review the historical literature both to show the inspiration for the main construction and to show potential applications for it. We then provide the main construction for the curves A and C_F and calculate some necessary information. We will prove the main result and finally list some of its corollaries and potential future directions.

3.2 Construction 1: Legendre

The identification of Jacobian varieties that are gluings of smaller Jacobian varieties has seen a number of historical uses. See for example [1, 3]. One hopes with a generalized construction the techniques already present in the literature can be considerably extended. Out of historic respect and conceptual insight we review the classical construction to show the origin of the method employed by this thesis.

For $f \in k[x]$ a square-free quintic, $a \in k$ such that $f(a) \neq 0$, and $d \in k$ non-zero we let

$$C_1 : y^2 = f(x)$$
$$C_2 : z^2 = d(x-a)f(x).$$

Proposition 3.2.1. *Let $L = k(x)(\sqrt{f}, \sqrt{d(x-a)})$. Then $L/k(x)$ is Galois with Galois group V_4.*

Proof. Since $d(x-a)$ is not a square multiple of $f(x)$ we have

$$\sqrt{d(x-a)} \notin k(x)(\sqrt{f}).$$

Thus $[L : k(C_1)] = [L : k(C_2)] = 2$ and $[L : k(x)] = 4$. Since every separable extension of degree 2 is Galois, we see that $L/k(C_1)$ and $L/k(C_2)$ are both Galois. Hence L is Galois over $k(C_1) \cap k(C_2) = k(x)$. Finally, since $k(C_1) \neq k(C_2)$ we see that L does not have a unique subfield of index 2. Thus $\mathrm{Gal}(L/k(x))$ is not cyclic and so $\mathrm{Gal}(L/k(x)) \cong V_4$. □

Let Ω be the curve corresponding to the composite field of $k(C_1)$ and $k(C_2)$. By Proposition 3.2.1 we have the familiar diagram of Figure 3.1.

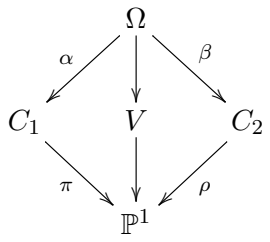


Figure 3.1: Subcover structure of $\Omega/\mathbb{P}^1$.

Lemma 3.2.2. *Let V and Ω be as in Figure 3.1. Then $g(V) = 0, g(\Omega) = 4$.*

Proof. From function fields we see $k(V) = k(x)(yz) = k(x)(\sqrt{d(x-a)f(x)^2})$ is ramified at two points, a and ∞. Since this is a degree 2 extension we have that $V \cong \mathbb{P}^1_k$.

Notice that there is a single Weierstrass point P on C_1 lying over ∞ and that there are two points on C_2 lying over infinity. Thus there are at least two points on Ω lying over ∞ since Ω is a cover of C_2. Thus $\alpha^{-1}(P) = \beta^{-1}\rho^{-1}(\{\infty\})$ contains at least two points, so no points over P are ramified. Hence $k(\Omega) = k(C_1)(\sqrt{d(x-a)})$ is ramified at only two points. Thus from the Riemann-Hurwitz formula $g(\Omega) = 4$.

□

Lemma 3.2.3. *Let Ω, C_1, C_2 be as in Figure 3.1. Then $J(C_1)[2] \cong J(C_2)[2]$. Moreover, if Δ is the anti-diagonal of $J(C_1)[2] \times J(C_2)[2]$ then $J(\Omega) \cong J(C_1) \times J(C_2)/\Delta$.*

Proof. Let $\alpha\colon \Omega \to J(C_1)$, $\beta\colon \Omega \to J(C_2)$, τ be the nontrivial automorphism of Ω/C_1, and σ be the non-trivial automorphism of Ω/C_2. By Lemma 2.6.6 there are endomorphisms $\tau_*, \sigma_* \in \mathrm{End}(J(\Omega))$. By Lemma 2.6.6 we see that $\alpha_* \circ \tau = \alpha_*$. Hence $\mathrm{Im}(\mathbb{1} - \tau_*) \subseteq \ker(\alpha_*)$ and

$$\mathbb{1} - \tau_* = \mathbb{1} - \tau_* + (\mathbb{1} + \tau_* + \sigma_* + \sigma_*\tau_*) - (\mathbb{1} + \sigma_*\tau_*) = \mathbb{1} + \sigma_* \in \mathrm{End}(\Omega).$$

We see $\ker(\alpha_*) \subseteq \mathrm{Im}(\mathbb{1} + \sigma_*) = \mathrm{Im}(\beta^*)$. Similarly $\ker(\beta_*) \subseteq \mathrm{Im}(\alpha^*)$. Therefore

$$\begin{array}{ccc} J(C_1) \times J(C_2) & & \\ \downarrow{\scriptstyle [2]} & \searrow^{\alpha^* + \beta^*} & \\ & & J(\Omega) \\ & \swarrow_{(\alpha_*, \beta_*)} & \\ J(C_1) \times J(C_2) & & \end{array}$$

commutes.

We now proceed to compute the kernel which must be contained in $J(C_1)[2] \times J(C_2)[2]$. Notice that $f \in k(\mathbb{P}^1_x)$ has a divisor of the form

$$\mathrm{div}\, f = \theta_1 + \ldots + \theta_5 - 5\infty$$

where the θ_i are the points corresponding to the roots of $f(x)$ on $\mathbb{P}^1_x$. Let $D := \theta_i + \theta_j - \theta_k - \theta_l \in \mathrm{Div}^0(\mathbb{P}^1_x)$ for arbitrary $i, j, k, l \in \{1, \ldots, 5\}$. Since all of these points lie under ramification points

of both π and ρ we see that the divisors

$$D_1 := \frac{1}{2}\pi^*(D) = \frac{1}{2}\left(2\pi^{-1}(\theta_i) + 2\pi^{-1}(\theta_j) - 2\pi^{-1}(\theta_k) - 2\pi^{-1}(\theta_l)\right)$$

$$D_2 := \frac{1}{2}\rho^*(D) = \frac{1}{2}\left(2\rho^{-1}(\theta_i) + 2\rho^{-1}(\theta_j) - 2\rho^{-1}(\theta_k) - 2\rho^{-1}(\theta_l)\right)$$

are well defined. It is also clear that for the map $\gamma : \Omega \to \mathbb{P}^1_x$ that

$$\alpha^*([D_1]) + \beta^*([D_2]) = \gamma^*([D]) = [0].$$

Thus it is immediate that $\ker(\alpha^* + \beta^*)$ is the anti-diagonally embedded 2-torsion since the D_1, D_2 generate $J(C_1)[2], J(C_2)[2]$ respectively.

□

We intend to produce a generalization of this construction. One particular restriction of Legendre's construction is that we insist both C_1 and C_2 have a rational Weierstrass point (over ∞ and over α respectively). Not every genus 2 curve has to have a rational Weierstrass point.

3.3 Diagrams associated to a Galois covering

The main technique we will use to construct Jacobians of genus $2g$ curves that arise as a gluing of Jacobians of genus g curves is to construct Galois covers which have these objects as isogeny factors and see if these can be recognized as isomorphisms. If $A/\mathbb{P}^1_x$ is not already Galois then the Galois closure (Ω) of the tower of double covers $A \to H \to \mathbb{P}^1_x$ over $\mathbb{P}^1_x$ will have $\mathrm{Gal}(\Omega/\mathbb{P}^1) \cong D_4$. We give names to the automorphisms and the curves arising from Ω.

Lemma 3.3.1. *Let K, L, M be fields and let M/K and L/M be Galois extensions of degree 2. If L/K is not Galois then there is a degree 2 extension $\hat{L}/L$ such that $\hat{L}/K$ is Galois and* $\mathrm{Gal}(\hat{L}/K) \cong D_4$.

Proof. Let $L = M(\alpha)$ and let p be the minimal polynomial of α over M. Let σ be the nontrivial automorphism of M/K. Then σ acts on p by acting on the coefficients of p. Let β be a roots of p^σ and define $L' := M(\beta)$.

If $L' = L$ this is a contradiction, since then both $\langle\sigma\rangle$ and $\mathrm{Aut}(L/M)$ are subgroups of $\mathrm{Aut}(L/K)$. This would imply $\sigma \in \mathrm{Aut}(L/M)$ and so fixes M, a contradiction.

Define $\hat{L} := M(\alpha, \beta)$. We see that $[\hat{L} : M(\alpha)] = 2$ and that $\hat{L}$ is the splitting field of the polynomial $p \cdot p^\sigma$ whose coefficients are in M. Thus $\hat{L}/M$ is Galois and there are two distinct degree 2 sub-extensions of $\hat{L}/K$, $M(\alpha)$ and $M(\beta)$. Therefore $\mathrm{Gal}(\hat{L}/M) \cong V_4$. But $p \cdot p^\sigma$ is σ invariant and so has coefficients in K. We conclude $\hat{L}/K$ is Galois and furthermore:

(i) $\left|\mathrm{Gal}(\hat{L}/K)\right| = 8$,

(ii) $\mathrm{Gal}(\hat{L}/K)$ has a V_4 subgroup,

(iii) $\mathrm{Gal}(\hat{L}/K)$ is non-abelian since L/K is not Galois.

Therefore $\mathrm{Gal}(\hat{L}/K) \cong D_4$. □

3.3.1 Models

The following are affine models for the curves corresponding to Ω and its subcovers. By Theorem 2.3.9 we may find a smooth projective model in place of these objects and note that since the Jacobian is determined by the function field that we can use the information provided by these models.

$$\begin{aligned}
C_F :&\quad V(y^2 - F(x)) \subseteq \mathbb{A}^2_k(x, y)\\
A_1 :&\quad V(y^2 - F(x), z_1^2 - r + y) \subseteq \mathbb{A}^3_k(x, y, z_1)\\
A_2 :&\quad V(y^2 - F(x), z_2^2 - r - y) \subseteq \mathbb{A}^3_k(x, y, z_2)\\
\Omega :&\quad V(y^2 - F(x), z_1^2 - r + y, z_2^2 - r - y) \subseteq \mathbb{A}^4_k(x, y, z_1, z_2).
\end{aligned}$$

We remark that the given affine model of C_F is a double cover of $\mathbb{A}^1_k$ by the map $\phi\colon (x, y) \to (x)$. Let $\mathbb{P}^1_x$ be the corresponding $\mathbb{P}^1_k$ double covered by C_F. If A_1 is not Galois over $\mathbb{P}^1_k$ then, by Lemma 3.3.1, the curve Ω is Galois over $\mathbb{P}^1_k$ with Galois group isomorphic to D_4. The automorphisms of Ω over $\mathbb{P}^1_k$ are generated by

$$\begin{aligned}
\iota :=&\quad (y, z_1, z_2) \to (-y, z_2, z_1)\\
\rho :=&\quad (y, z_1, z_2) \to (y, -z_1, z_2)\\
\tau :=&\quad (y, z_1, z_2) \to (y, z_1, -z_2)\\
\tau\iota =&\quad (y, z_1, z_2) \to (-y, z_2, -z_1)
\end{aligned}$$

where $y^2 = F, z_1^2 = r - y, z_2^2 = r + y$. Observe

$$(\tau\iota)^2(y, z_1, z_2) = \tau\iota(-y, z_2, -z_1) = (y, -z_1, -z_2) = \rho\tau(y, z_1, z_2).$$

Since $(\tau\iota)^2$ is an element of order 2, $\tau\iota$ is of order 4. We also note that ρ and τ commute. We also note that $\iota\rho = \tau\iota$.

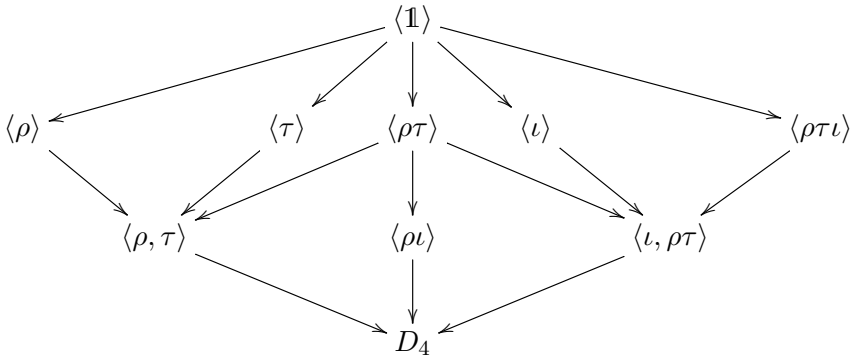


Figure 3.2: Subgroup structure of $\mathrm{Aut}(\Omega/\mathbb{P}^1)$. Arrows denote inclusion.

We relate the subgroups in Figure 3.2 to their quotient curves (and corresponding fixed fields) in Figure 3.3 through the usual correspondence of Galois theory.

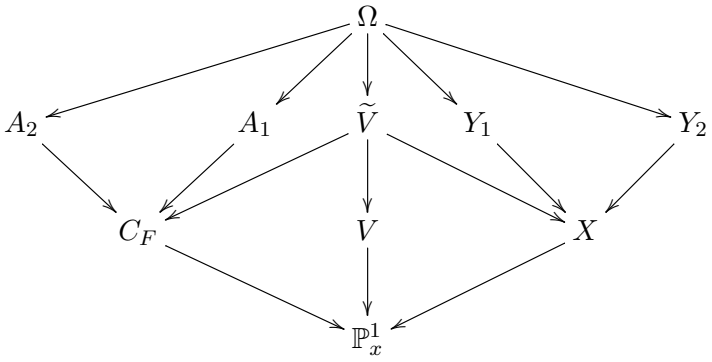


Figure 3.3: Subcover structure of Ω.

We compute the genera of Y_1 and X.

Lemma 3.3.2. *Let $\Omega, C_F, A_1, Y_1, X, \mathbb{P}^1_x$ be as in Figure 3.3 and let $g = g(C_F)$. Let $\pi\colon A_1 \to C_F$, $\phi\colon C_F \to \mathbb{P}^1_x$, $\xi\colon Y_1 \to X$, and $\eta\colon X \to \mathbb{P}^1_x$ be the covering morphisms as in Figure 3.3. If π is ramified at two points P_1, P_2 such that $\phi(\pi(P_1)), \phi(\pi(P_2)) \in \mathbb{P}^1_x$ are distinct points which are not zeros or poles of F, then $g(A_1) = 2g, g(Y_1) = g$ and $g(X) = 0$.*

Proof. By the Riemann-Hurwitz formula we have

$$2g(A_1) - 2 = 2(2g(C_F) - 2) + \sum_{P \in A_1} (e_P - 1) = 4g(C_F) - 2.$$

Thus $g(A_1) = 2g$. The function $z_1 z_2 \in k(\Omega)$ is invariant under both ι and $\rho\tau$ and not invariant under τ. Thus $z_1 z_2 \in k(X)$ and $z_1 z_2 \notin k(x)$. But

$$z_1 z_2 = \sqrt{(r-y)(r+y)} = \sqrt{r^2 - F}.$$

By Corollary 2.4.39 we have that $\mathrm{div}_{C_F}(r-y) = n_{P_1} P_1 + n_{P_2} P_2 + 2D$ where both n_{P_1} and n_{P_2} are odd. Since $r^2 - F = \mathrm{Nm}_{k(C_F)/k(x)}(r-y)$ we have

$$\mathrm{div}_{\mathbb{P}^1_x}(r^2 - F) = n_{P_1}\phi(P_1) + n_{P_2}\phi(P_2) + 2D.$$

Since $k(X) = k(x)(\sqrt{r^2 - F})$ it follows from Corollary 2.4.39 that the cover η is ramified at two points. By the Riemann-Hurwitz formula

$$2g(X) - 2 = 2(2g(\mathbb{P}^1_x) - 2) + 2 = -2.$$

Thus $g(X) = 0$.

The function $w := z_1 + z_2 \in k(\Omega)$ is invariant under ι but not under $\rho\tau$. Thus $k(Y_1) = k(X)(w)$. Observe that

$$w^2 = 2(r + z_1 z_2).$$

Let $D = \mathrm{div}_X(r + z_1 z_2)$. Since $\tau(z_1 z_2) = -z_1 z_2$ we have

$$\pi_*(D) = \mathrm{div}_{\mathbb{P}^1_x} \mathrm{Nm}_{k(X)/k(x)}(r + z_1 z_2) = \mathrm{div}_{\mathbb{P}^1_x} F.$$

Thus the number of points of odd multiplicity in D is at least the number of points of odd multiplicity in $\mathrm{div}_{\mathbb{P}^1_x} F$. Since all of the ramification points of $\Omega \to \mathbb{P}^1_x$ lie over points of odd multiplicity in $\mathrm{div}_{\mathbb{P}^1_x} F$, $\phi(\pi(P_1))$, or $\phi(\pi(P_2))$, the number of points of odd multiplicity in $\mathrm{div}_X D$ is equal to the number of points of odd multiplicity of $\mathrm{div}_{\mathbb{P}^1_x} F$. Therefore by Corollary 2.4.39 the number of ramification points of ϕ and ξ are equal. By the Riemann-Hurwitz formula we conclude $g(Y_1) = g$. □

Lemma 3.3.3. *Let Y_1, X be as in Lemma 3.3.2. Then X has a rational point and is isomorphic to $\mathbb{P}^1_k$.*

Proof. See [10, Exercise A.4.12b]. □

3.4 Construction of a dihedral cover of $\mathbb{P}^1_k$

Lemma 3.4.1. *For each genus g curve C separably double covered by a genus $2g$ curve A there exists a function $z \in k(A)$ such that $k(A) = k(C)(\sqrt{z})$ and the divisor of z is of the form*

$$\operatorname{div}(z) = 1 \cdot P_1 + 1 \cdot P_2 + 2(D^+ - D^-)$$

where D^+, D^- are effective and $P_1, P_2 \in C(\bar{k})$.

Proof. Let z be a function such that $k(A) = k(C_F)(\sqrt{z})$. By the Riemann-Hurwitz formula the cover is ramified at two points so we write

$$\operatorname{div}(z) = P_1 + P_2 + 2(D^+ - D^-)$$

with D^+ and D^- effective.

□

Remark 3.4.2. The divisor $D^- - D^+$ is both degree 1 and defined over k.

3.4.1 Norm construction

In this section we provide a construction that shows how, given hyperelliptic genus g curve C_f, to obtain pairs (A, C_F) of curves defined over k such that A is a double cover of C_F ramified at 2 points and C_F is a hyperelliptic genus g curve. The primary utility of this lemma is the principle given by Kani-Rosen (2.6.10) that a common Galois cover Ω of C_f, C_F and A will give rise to isogeny relations between $J(C_f), J(C_F)$ and $J(A)$. We will proceed with a careful computation to determine the exact isogeny relations.

Lemma 3.4.3. *Let $P_1, P_2 \in \mathbb{P}^1_{\bar{k}}$ be points such that $P_1 \neq P_2$. Assume either P_1 and P_2 are k-rational points or P_1 is the quadratic conjugate of P_2. Then there is an involution $\mu\colon \mathbb{P}^1_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ defined over k that fixes P_1 and P_2.*

Proof. Fix a choice of co-ordinates $(x : z)$ for $\mathbb{P}^1_{\bar{k}}$. We may assume up to translation that P_1, P_2 are in the set

$$\left\{(x : z) \in \mathbb{P}^1_k : z \neq 0\right\}$$

so we let $P_1 = (a : 1), P_2 = (b : 1)$ for some $a, b \in \bar{k}$. If P_1 and P_2 are rational then $a + b, ab \in k$. If P_1 and P_2 are quadratic conjugates then a and b are conjugate, that is

$$(t - a)(t - b) \in k[t].$$

So $a + b, ab \in k$. We see the morphism $\mu\colon \mathbb{P}^1_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ defined by

$$\mu(x : z) := (x : z) \begin{bmatrix} a + b & 2 \\ -2ab & -a - b \end{bmatrix}$$

is defined over k. A simple calculation shows that μ fixes P_1 and P_2 and is an involution. □

Lemma 3.4.4. *Let $\mathcal{R}_\pi = P_1 + P_2 \in \mathrm{Div}(\mathbb{P}^1_k)$ be a degree 2 divisor such that P_1 and P_2 fulfil the conditions of Lemma 3.4.3. Let μ be the involution fixing P_1 and P_2. Then we may find $\pi\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ such that*

(i) there is an element $x \in k(\mathbb{P}^1_k)$ such that $k[t, \mu^*(t)]$ is an integral extension of $k[x]$,

(ii) $\pi^*(k(\mathbb{P}^1_k)) = k(x)$, π has degree 2, and $\mathcal{R}_\pi$ is the ramification divisor of π.

Proof. If μ fixes ∞ then $\mu^*(t) = c - t$ for some $c \in k$. Define the rational map

$$\begin{aligned} \pi\colon \mathbb{P}^1_k &\to \mathbb{P}^1_k \\ (t : 1) &\to (t\mu^*(t) : 1). \end{aligned}$$

By Theorem 2.3.10 we see that π extends to a double cover. Let $x := \pi^*(t) = t(c - t)$ and notice that both $t, \mu^*(t)$ are roots of

$$p(T) = T^2 - cT + x \in k[x][T].$$

So (i) is satisfied in this case. If μ does not fix ∞ then we define the rational map

$$\begin{aligned} \pi\colon \mathbb{P}^1_k &\to \mathbb{P}^1_k \\ (t:1) &\to \left(\frac{t+\mu^*(t)}{2} : 1\right). \end{aligned}$$

By Theorem 2.3.10 we see that π extends to a double cover. Let $x := \pi^*(t) = \left(\frac{t+\mu^*(t)}{2}\right)$. If $c \in k$ we see that

$$\begin{aligned} \mathrm{div}_{\mathbb{P}^1_k}(t-c) &= (c:1) - \infty \\ \mathrm{div}_{\mathbb{P}^1_k}\mu^*(t) &= \mu(0) - \mu(\infty). \end{aligned}$$

Since μ does not fix ∞ we may choose c such that $(c:1) = \mu(\infty)$. If $\mu(0) \neq \infty$ then

$$\mathrm{div}_{\mathbb{P}^1_k}(t-c)\mu^*(t) = \mu(0) - \infty = \mathrm{div}_{\mathbb{P}^1_k}((t-c)+\alpha)$$

for some $\alpha \in k$. Since $t, \mu^*(t) \in k(t)$ we can find $d \in k$ such that

$$(t-c)\mu^*(t) = d[(t-c)+\alpha].$$

So $(t-c)(\mu^*(t)-d) = d\alpha \in k$. Both $(t-c)$ and $(\mu^*(t)-d)$ are roots of

$$p(T) = T^2 - xT - d\alpha \in k[x][T].$$

If $\mu(0) = \infty$ then $t\mu^*(t) \in k$ and both $t, \mu^*(t)$ are roots of

$$p(T) = T^2 - xT - t\mu^*(t) \in k[x][T].$$

In each case we have satisfied (i).

Observe that $k(x)$ is contained in the subfield fixed by μ^*. Hence since $[k(t):k(x)] = 2$ we see $k(x)$ is the fixed field of μ^*. Since the quotient map π is ramified at its fixed points and μ has order 2, we are done. □

Lemma 3.4.5 (Norm construction)**.** *Let $C_f\colon w^2 - f(t)$ be an affine model of a hyperelliptic genus g curve where f is a squarefree polynomial in t. Let $\mathcal{R}_\pi = P_1 + P_2 \in \mathrm{Div}(\mathbb{P}^1_k)$ be a degree 2 divisor such that P_1 and P_2 fulfil the conditions of Lemma 3.4.3. Let μ, π be as in Lemma 3.4.4. Denote the preimage of π by $\mathbb{P}^1_t$ and denote the image of π by $\mathbb{P}^1_x$ whose function fields are denoted*

by $k(t), k(x)$ respectively. If the points of odd degree multiplicity in $\operatorname{div}_{\mathbb{P}^1_t} f$ and the points of odd degree multiplicity in $\operatorname{div}_{\mathbb{P}^1_t} f^\mu$ are disjoint then:

(i) The hyperelliptic curve defined by the affine model $C_F := V(y^2 - 4\operatorname{Nm}_{k(t)/k(x)}(f)) \subseteq \mathbb{A}^2_k$ has genus g.

(ii) Let $\beta\colon C_F \to \mathbb{P}^1_x$ be the cover extending the rational map $\beta(x,y) = (x:1)$. There is a double cover $\alpha\colon A \to C_F$ such that A has genus $2g$ and the ramification divisor of α, denoted $\mathcal{R}_\alpha$, satisfies

$$\beta_*\alpha_*(\mathcal{R}_\alpha) = \pi_*(\mathcal{R}_\pi).$$

Proof. Let

$$r := \frac{f + f\circ\mu}{2}, \quad q := \frac{f - f\circ\mu}{2}.$$

In particular $\mu(r) = r$, $\mu(q) = -q$, and $f = r+q$. Since $[k(t) : k(x)] = 2$ and q is not fixed by μ we see that $k(t) = k(x)(q)$. Since q vanishes at both P_1 and P_2 we write $\operatorname{div}_{\mathbb{P}^1_t}(q) = n_{P_1}P_1 + n_{P_2}P_2 + D$ with D not supported at P_1 or P_2. Hence since $\operatorname{div}_{\mathbb{P}^1_t} q$ is invariant under μ we have that

$$\begin{aligned}\operatorname{div}_{\mathbb{P}^1_x}\operatorname{Nm}_{k(t)/k(x)}(q) = \operatorname{div}_{\mathbb{P}^1_x}(-q^2) &= n_{P_1}\pi_*(P_1) + n_{P_2}\pi_*(P_2) + 2D' \\ &= \pi_*(P_1) + \pi_*(P_2) - 2\infty + 2(D' + \infty).\end{aligned}$$

We infer from Corollary 2.4.39 and the fact $k(t) = k(x)(\sqrt{q^2(x)})$ that both n_{P_1} and n_{P_2} are odd. Since the divisor class group of $\mathbb{P}^1$ is $\mathbb{Z}$ we rewrite this as

$$\operatorname{div}_{\mathbb{P}^1_x}(h(x)) + 2\operatorname{div}_{\mathbb{P}^1_x}(\widetilde{q}(x))$$

where $h, \tilde{q} \in k(x)$. In light of this we rewrite $\operatorname{Nm}_{k(t)/k(x)}(q) = d \cdot h(x)\tilde{q}(x)^2$ with $d \in k$. We may assume that $d = 1$ by setting $\tilde{h}(x) := d \cdot h(x)$. Now define

$$F(x) := 4\operatorname{Nm}_{k(t)/k(x)}(f) = 4 \cdot f \cdot (f^\mu) = 4r(x)^2 - 4\tilde{h}(x)\tilde{q}(x)^2.$$

Recall there are no points with odd multiplicity in both $\operatorname{div}_{\mathbb{P}^1_t} f$ and $\operatorname{div}_{\mathbb{P}^1_t} f^\mu$. In particular since P_1 and P_2 are fixed by μ they have multiplicity zero in $\operatorname{div}_{\mathbb{P}^1_t} f$. Moreover for each point $P \in \mathbb{P}^1_t(\bar{k})$ at most one of $\{P, \mu(P)\}$ can occur in $\operatorname{div}_{\mathbb{P}^1_t} f$ with odd multiplicity. Since $\operatorname{div}_{\mathbb{P}^1_x} F = \pi_* \operatorname{div}_{\mathbb{P}^1_t} f$ we see the number of squarefree roots of F and f is the same, so the hyperelliptic curve $C_F : y^2 - F(x)$ also has genus g.

All that is left to do is to show that (ii) is satisfied. Let

$$w^2 := 2r(x) - y.$$

Define A by the affine model

$$A = \left\{(x, y, w) \in \mathbb{A}^3_k : (x, y) \in C_F \text{ and } w^2 = 2r(x) - y\right\}$$

and notice that $k(A) = k(C_F)(w)$. Proceeding we have

$$\mathrm{Nm}_{k(C_F)/k(x)}(w^2) = 4r(x)^2 - F = 4\tilde{h}(x)\tilde{q}(x)^2$$

so $\mathrm{div}_{\mathbb{P}^1_x} \mathrm{Nm}_{k(C_F)/k(x)}(w^2) = \pi_*(\mathcal{R}_\pi) + 2D'$. Since $k(A) = k(C_F)(w)$ we note that

$$\alpha_*(\mathcal{R}_\alpha) = \text{odd multiplicity terms of } \mathrm{div}_{C_F}(w^2),$$

so this cover is ramified at 2 points. We now compute the genus $g(A)$. By Riemann-Hurwitz

$$2g(A) - 2 = 2(2g(C_F) - 2) + 2$$

and so $g(A) = 2$, $g(C_F) = 2g$. □

Lemma 3.4.6. *Let $A, C_f, C_F, \mathbb{P}^1_t, \mathbb{P}^1_x, q, f, w$ be as in Lemma 3.4.5. Let Ω be the Galois closure of C_f over $\mathbb{P}^1_x$. Then $\mathrm{Gal}(\Omega/\mathbb{P}^1_x) \cong D_4$ and $k(A) \subseteq k(\Omega)$.*

Proof. By Lemma 3.3.1 we have that $\mathrm{Gal}(\Omega/\mathbb{P}^1_x) \cong D_4$. Let

$$p(T) := (T^2 - f(t))(T^2 - f^\mu(t)) \in k(\Omega)[T].$$

We see that $f(t) + f^\mu(t) = 2r(x) \in k(x)$,

$$p(T) = T^4 - (f(t) + f^\mu(t))T^2 + F(x) \in k(x)[T],$$

and $p(T)$ is irreducible over $k(x)$. But $p(\sqrt{f(t)}) = 0$, so $p(T)$ splits in $k(\Omega)$. Let $w_1 = \sqrt{f(t)}, w_2 = \sqrt{f^\mu(t)}$ and observe these are roots of $p(T)$. We have that $w_1 w_2 = \sqrt{f \cdot f^\mu} = y$ and so $k(C_F) \subseteq k(\Omega)$. Finally, let

$$\hat{p}(T) = T^2 - (2r(x) - y) \in k(\Omega)[T].$$

We see that

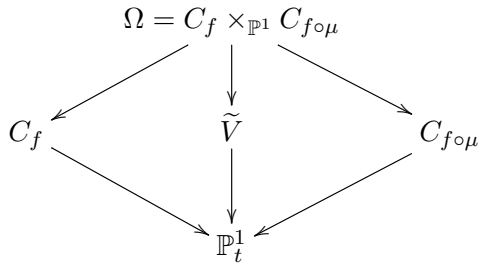
$$\hat{p}(w_1 - w_2) = w_1^2 + w_2^2 - w_1 w_2 - (2r(x) - y) = 0,$$

so any root of $\hat{p}$ lies in $k(\Omega)$. But by definition $\hat{p}(w) = 0$, so it follows that $k(A) \subseteq k(\Omega)$. □

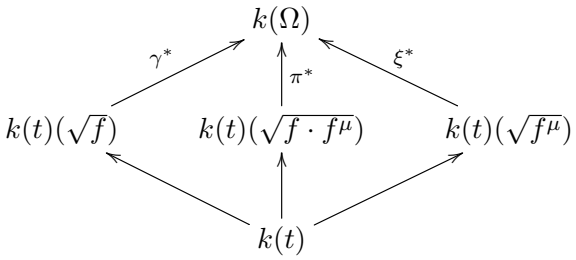
It turns out that ramification divisors of covers give us slightly more information about the associated Jacobians than just their dimensions. We make a few useful observations here before proceeding.

Proposition 3.4.7. *Let Ω, A, and C_f be as in Lemma 3.4.6. Then the covers $\Omega \to C_f$ and $\Omega \to A$ are ramified.*

Proof. First consider



and looking at the corresponding function fields we have the following diagram



Since we chose μ such that there are no points of odd multiplicity in both $\mathrm{div}_{\mathbb{P}^1_t} f$ and $\mathrm{div}_{\mathbb{P}^1_t} f^\mu$ we have that $\mathrm{div}_{\mathbb{P}^1_t}(f \cdot f^\mu)$ has $4g + 4$ points with odd multiplicity. Hence $\widetilde{V} \to \mathbb{P}^1_t$ is ramified at $4g + 4$ points so $g(\widetilde{V}) = 2g + 1$. By symmetry the ramification divisors of γ and ξ have the same degree. Now by Riemann-Hurwitz

$$\kappa_\Omega = \kappa_{\widetilde{V}} + \mathcal{R}_\pi$$
$$\kappa_\Omega = \kappa_{C_f} + \mathcal{R}_\gamma$$
$$\kappa_\Omega = \kappa_{C_{f^\mu}} + \mathcal{R}_\xi.$$

Taking degrees and solving the resulting linear system we find that π is unramified and γ, η are each ramified at $2g+2$ points. Let $\alpha\colon \Omega \to A$ be the double cover in Lemma 3.4.6. By the Riemann-Hurwitz formula

$$2g(\Omega) - 2 = 2(2g(\widetilde{V}) - 2)$$
$$(2g(\Omega) - 2) - 2(2g(A) - 2) = \sum_{P \in \Omega} (e_{\alpha,P} - 1).$$

Since $g(A) = 2g$ we conclude $g(\Omega) = 4g+1$ and α is ramified. □

Corollary 3.4.8. *For Ω and $\widetilde{V}$ as in Proposition 3.4.7 we have that $g(\Omega) = 4g+1$ and $g(\widetilde{V}) = 2g+1$.*

Remark 3.4.9. The technical conditions of Lemma 3.4.5 ensure that quotienting by μ creates a squarefree polynomial and thus C_F has exactly the ramification data needed to have genus g.

3.5 Verifying $J(C_F) \times J(C_f)/\Delta \cong J(A)$

3.5.1 Computing with endomorphisms of $J(\Omega)$

The following helpful lemma appears in [15, section 3]. Since we only need the double cover version we prove this directly.

Lemma 3.5.1 (Mumford)**.** *If $\pi : \widetilde{C} \to C$ is a ramified cover of prime degree then $\pi^*\colon J(C) \to J(\widetilde{C})$ is an embedding.*

proof for degree 2. Observe that since $\pi_* \circ \pi^* = [2]$ that

$$\ker \pi^* \subseteq J(C)[2].$$

Suppose for non-zero $[D] \in J(C)[2]$ that $\pi^*([D]) = [0]$. Then by definition there is a function $f \in \bar{k}(\widetilde{C})$ such that

$$\operatorname{div} f = \pi^*(D)$$

and in particular

$$\operatorname{div} \mathrm{Nm}(f) = \pi_*\pi^*(D) = 2D$$

since D was a non-principal divisor $f \notin \bar{k}(C)$. Hence because $[k(\widetilde{C}) : k(C)] = 2$ is prime we have

$$k(\widetilde{C}) = k(C)(\sqrt{f})$$

Thus the ramification divisor of π is given by

$$\pi_*(\mathcal{R}_\pi) = \text{odd multiplicity terms in } \operatorname{div}\operatorname{Nm}(\sqrt{f})$$

of which there are none, so the ramification divisor is trivial. □

We notice in our diagram that each of $J(C_f), J(D), J(C_F)$ must all embed into $J(\Omega)$. This means that we can use endomorphisms of $J(\Omega)$ to construct maps explicitly between these objects. We first show how to identify each of these in $J(\Omega)$ and then proceed with the main result. The following lemma will aid in this process.

Lemma 3.5.2. *Let $\pi\colon \widetilde{C} \to C$ be a double cover with Galois group $Gal(\widetilde{C}/C) = \langle\sigma\rangle$. Then $\pi^*J(C) = \operatorname{Im}(\mathbb{1}+\sigma) \subseteq J(\widetilde{C})$. Moreover if π is ramified the map $\pi^*\colon J(C) \to \operatorname{Im}(\mathbb{1}+\sigma)$ is an isomorphism.*

Proof. The first equality is the definition of π^* and the containment $\pi^*(J(C)) \subseteq J(\widetilde{C})$ is also straight from the definition. That the map is injective follows from Lemma 3.5.1. By definition of π^* the map is also an isogeny onto its image. By the proof of Lemma 2.5.9 we see π^* factors through multiplication by 1 so it is an isomorphism. □

Lemma 3.5.3. *Let $\pi\colon \widetilde{C} \to C$ be a ramified double cover with Galois group $\operatorname{Gal}(\widetilde{C}/C) = \langle\sigma\rangle$. Then*

$$\mathbb{1}+\sigma = \pi^* \circ \pi_* \in \operatorname{End}(J(\widetilde{C})).$$

Proof. The first equality follows immediately from Lemma 2.4.20. That it is an endomorphism follows from the fact it is a sum of endomorphisms. □

By applying the above lemma twice we obtain

Corollary 3.5.4. *Let $\widetilde{C} \xrightarrow{\alpha} C' \xrightarrow{\beta} C$ be ramified double covers with $Gal(\widetilde{C}/C) = \langle\sigma,\tau\rangle \cong C_2 \times C_2$. Then*

$$(\mathbb{1}+\sigma)(\mathbb{1}+\tau) = \alpha^*\beta^* \circ \beta_*\alpha_* \in \operatorname{End}(J(\widetilde{C})).$$

Proposition 3.5.5. *Let*

$$\pi\colon A \to C_F$$
$$\alpha\colon \Omega \to A$$
$$\gamma\colon \Omega \to C_f$$

be the covering maps as in Lemma 3.4.6 with corresponding maps on the Jacobians $\pi^*, \pi_*, \alpha^*, \ldots, \gamma_*$. *Then the following diagram commutes.*

$$\begin{array}{ccc} J(C_f) \times J(C_F) & & \\ \downarrow [2] & \searrow^{\alpha_* \circ \gamma^* + \pi^*} & \\ & & J(A) \\ & \swarrow_{(\gamma_* \circ \alpha^*, \pi_*)} & \\ J(C_f) \times J(C_F) & & \end{array}$$

Proof. By composing we get a map

$$J(C_f) \times J(C_F) \xrightarrow{(\gamma_* \alpha^* (\alpha_* \gamma^* + \pi^*), \pi_* (\alpha_* \gamma^* + \pi^*))} J(C_f) \times J(C_F) \ .$$

Since for isogenies ϕ, ψ, ρ we have $\phi(\psi + \rho) = \phi\psi + \phi\rho$ it suffices to check that

$$\begin{aligned} (i) \qquad & \pi_* \pi^* = [2] \\ (ii) \qquad & \pi_* \alpha_* \gamma^* = 0 \\ (iii) \qquad & \gamma_* \alpha^* \pi^* = 0 \\ (iv) \qquad & \gamma_* \alpha^* \alpha_* \gamma^* = [2]. \end{aligned}$$

(i) Given by Lemma 2.4.20.

(ii) Let $[D] \in \gamma^* J(C_f) = \mathrm{Im}(\mathbb{1} + \iota)$. Then we may find a class $[D'] \in J(\Omega)$ such that $[D] = (\mathbb{1} + \iota)[D']$. Now by Corollary 3.5.4

$$\begin{aligned} \alpha^* \pi^* \circ (\pi_* \alpha_*)((\mathbb{1} + \iota)[D']) &= (\mathbb{1} + \rho)(\mathbb{1} + \tau)(\mathbb{1} + \iota)[D'] \\ &= (\mathbb{1} + \rho + \tau + \iota + \rho\tau + \rho\iota + \tau\iota + \rho\tau\iota)[D']. \end{aligned}$$

We recognize this as the pull back of a $\mathbb{P}^1_x$ divisor class and so it must be trivial. Since $\alpha^* \pi^*$ is an embedding we have $(\pi_* \alpha_*)[D] = 0$.

(iii) Let $[D] \in \alpha^* \pi^* (J(C_F)) = \mathrm{Im}((\mathbb{1} + \rho)(\mathbb{1} + \tau))$. As before write $[D] = (\mathbb{1} + \rho)(\mathbb{1} + \tau)[D']$. Now as before

$$\gamma^* \gamma_* ((\mathbb{1} + \rho)(\mathbb{1} + \tau)[D']) = (\mathbb{1} + \iota)(\mathbb{1} + \rho)(\mathbb{1} + \tau)[D'] = 0.$$

Since γ^* is an embedding we have $\gamma_*([D]) = 0$.

(iv) Notice that

$$\begin{aligned}\gamma_*\alpha^*\alpha_*\gamma^* - [2] &= \gamma_*\alpha^*\alpha_*\gamma^* - \gamma_*\gamma^* \\ &= \gamma_*(\alpha^*\alpha_* - \mathbb{1})\gamma^* \\ &= \gamma_*((\mathbb{1}+\rho) - \mathbb{1})\gamma^*.\end{aligned}$$

Let $[D] = (\mathbb{1}+\iota)[D'] \in \gamma^*J(C_f) = \mathrm{Im}(\mathbb{1}+\iota)$. Now

$$\begin{aligned}&\rho\gamma^*\gamma_*(\rho)(\mathbb{1}+\iota)[D'] \\ &= \rho(\mathbb{1}+\iota)(\rho)(\mathbb{1}+\iota)[D'] \\ &= (\mathbb{1}+\rho\tau\iota)(\mathbb{1}+\iota)[D'] \\ &= (\mathbb{1}+\iota+\rho\tau+\rho\tau\iota)[D'].\end{aligned}$$

Again this is the pullback of a $\mathbb{P}^1_t$ class and is trivial. Since $\rho\gamma^*$ is an embedding we conclude

$$\gamma_*\alpha^*\alpha_*\gamma^* - [2] = 0 \Rightarrow \gamma_*\alpha^*\alpha_*\gamma^* = [2].$$

□

Proposition 3.5.6. *Let α, γ, π be as in Proposition 3.5.5. Then the isogeny $\alpha_*\gamma^* + \pi^*$ respects polarizations.*

Proof. By Proposition 2.5.30 we may replace $(\pi^*)^\vee$ by $\lambda_{C_F}\pi_*\lambda_A^{-1}$ and make similar substitutions for α_* and γ_*. It follows that

$$(\alpha_*\gamma^* + \pi^*)^\vee = (\lambda_{C_f} \times \lambda_{C_F}) \circ (\gamma_*\alpha^*, \pi_*) \circ \lambda_A^{-1}.$$

Now by Proposition 3.5.5 we have that

$$\begin{aligned}(\alpha_*\gamma^* + \pi^*)^\vee\lambda_A(\alpha_*\gamma^* + \pi^*) &= (\lambda_{C_f} \times \lambda_{C_F}) \circ (\gamma_*\alpha^*, \pi_*) \circ \lambda_A^{-1} \circ \lambda_A \circ (\alpha_*\gamma^* + \pi^*) \\ &= (\lambda_{C_f} \times \lambda_{C_F}) \circ (\gamma_*\alpha^*, \pi_*) \circ (\alpha_*\gamma^* + \pi^*) \\ &= (\lambda_{C_f} \times \lambda_{C_f})[2].\end{aligned}$$

Thus $\alpha_*\gamma^* + \pi^*$ respects polarizations. □

3.5.2 Kernel data

In order to finish the main result we must identify the kernel of $\alpha_*\gamma^* + \pi^*$. Notice that the kernel must be contained in $J(C_f)[2] \times J(C_F)[2]$ so we restrict our attention there. First we show how to explicitly write down representatives of 2-torsion classes on hyperelliptic curves.

Lemma 3.5.7. *Let $\theta_i \in C_f$ be a Weierstrass point. Then there exists a point $\widetilde{\theta}_i \in C_F$ such that*

$$\pi^{-1}\left(\widetilde{\theta}_i\right) = \alpha(\gamma^{-1}(\theta_i)).$$

Proof. Since θ_i is a Weierstrass point of C_f, both θ_i and $\gamma^{-1}(\theta_i)$, are fixed by $\rho\tau$. Moreover, $\theta_i \in \mathbb{P}^1_t$ is disjoint from the ramification locus of $\mathbb{P}^1_t \to \mathbb{P}^1_x$. Thus since ρ acts trivially on A we can push down to get that $\alpha(\gamma^{-1}(\theta_i))$ is fixed by $\tau \in \mathrm{Aut}(A/C_F)$. But then $\alpha(\gamma^{-1}(\theta_i))$ is a cover of $\pi^{-1}(Y)$ for some $Y \subseteq C_F$. Since $\pi^{-1}(Y)$ cannot contain a ramification point of π we see

$$\left|\gamma^{-1}(\theta_i)\right| = 2 \geq \left|\pi^{-1}(Y)\right| > 1$$

and so the cover is degree 1. Moreover, since $\left|\pi^{-1}(Y)\right| = 2$ and intersects trivially with the ramification divisor we see that

$$Y = \left\{\widetilde{\theta}_i\right\}.$$

□

Corollary 3.5.8. *The map*

$$\begin{aligned}\psi\colon J(C_f)[2] &\to \left(\pi^* J(C_F)\right)[2] \\ [D] &\to (\pi^*)^{-1}\alpha_*\gamma^*([D])\end{aligned}$$

is an isomorphism.

Proof. It is immediate from Lemma 3.5.7 that

$$[\alpha_*\gamma^*(\theta_i - \theta_j)] = [\pi^*(\widetilde{\theta}_i - \widetilde{\theta}_j)].$$

Since the $[\widetilde{\theta}_i - \widetilde{\theta}_j]$ generate $J(C_F)[2]$ by Lemma 2.7.7 the map we have written down is a surjection of finite abelian groups and their finite underlying algebraic sets. The algebraic sets are of equal cardinality so it is an isomorphism. □

Proposition 3.5.9. *Let ψ be the isomorphism above and let*

$$\Delta := \{([D], [-1]\psi([D])) \in J(C_f)[2] \times J(C_F)[2] : D \in J(C_f)[2]\}.$$

Then $\Delta = \ker(\alpha_* \circ \gamma^* + \pi^*)$.

Proof. That Δ is contained in the kernel is easy to show. For equality we let $([D'], [D]) \in J(C_f)[2] \times J(C_F)[2]$. Then

$$\begin{aligned}(\alpha_*\gamma^* + \pi^*)([D'], [D]) &= (\alpha_*\gamma^* + \pi^*)([D'] - [D'], [D] + \psi[D']) = (\alpha_*\gamma^* + \pi^*)(0, [D] + \psi[D']) \\ &= \pi^*([D] + \psi[D']).\end{aligned}$$

Since π^* is injective this is $[0]$ if and only if $[D] = [-1]\psi([D'])$. □

This in conjunction with Proposition 3.5.5 gives

Proposition 3.5.10. *$J(C_f) \times J(C_F)/\Delta \cong J(A)$. Which is to say that $J(A)$ is obtained as a gluing of hyperelliptic Jacobian varieties of dimension g along their 2-torsion.*

3.6 Proof of the main result

In this section we give a proof of the main result.

Theorem (Main Result)**.** *Let k be a field of characteristic not equal to 2. Let C_f be a hyperelliptic genus g curve defined over k, and $J(C_f)$ its Jacobian. Then there exists a two parameter family of explicitly determined curves C_F of genus g and A of genus $2g$ such that*

1. *C_F is hyperelliptic and there is an isomorphism of finite algebraic sets $\psi\colon J(C_F)[2] \to J(C_f)[2]$.*
2. *A is a double cover of C_F.*
3. *$J(A) \cong J(C_f) \times J(C_F)/\Delta$ as polarized abelian varieties, where Δ is the (anti)-diagonally embedded 2-torsion of $J(C_f)$.*

Proof. The norm construction (Lemma 3.4.5) gives a two parameter family of (A, C_F) such that C_F is hyperelliptic and A is a double cover of C_F, so (2) has been proven. Corollary 3.5.8 shows that $\psi\colon J(C_F)[2] \to J(C_f)[2]$ is an isomorphism, thus we have proven (1). Proposition 3.5.10 gives

that $J(A) \cong J(C_f) \times J(C_F)/\Delta$ as abelian varieties and Proposition 3.5.6 shows the isomorphism respects polarizations. This completes (3) and finishes the proof. □

3.7 Corollaries

One immediate consequence of this construction is:

Corollary 3.7.1. *Any Jacobian of a hyperelliptic genus g curve arises as an isogeny factor of some Jacobian of a genus $2g$ curve where the isogeny ϕ is defined over k.*

3.7.1 MAGMA script

We provide a MAGMA script to demonstrate how our construction can be used to create non-hyperelliptic genus 4 curves with larger than expected automorphism groups. First we construct a genus 2 curve C_f isogenous to a product of elliptic curves by using a technical lemma. Then with a careful choice of involution μ we apply the norm construction (Lemma 3.4.5) to obtain a genus 2 curve C_F which is also isogenous to a product of two elliptic curves. We apply the main result to see that $J(A)$ is isogenous to a product of four elliptic curves. We verify with MAGMA that the automorphism group of A is larger than $\mathbb{Z}/2\mathbb{Z}$.

First we shall require two technical lemmas that ensure the correctness of the program. One lemma allows us to generate genus 2 curves isogenous to a product of elliptic curves and the other gives a family of μ such that the curve produced by the norm construction also has this property.

Lemma 3.7.2. *Let $a, b, c \in k^*$ be distinct elements. Let C be the hyperelliptic genus 2 curve defined by the affine model*

$$C : y^2 - (x^2 - a)(x^2 - b)(x^2 - c).$$

We claim that $J(C)$ is isogenous to a product of elliptic curves.

Proof. The quotient of C by the map $\eta((x, y)) = (-x, y)$ gives the elliptic curve

$$E_1 := y^2 - (x - a)(x - b)(x - c).$$

Thus we obtain the idempotent relation in $\mathrm{End}(J(C)) \otimes_{\mathbb{Z}} \mathbb{Q}$

$$\mathbb{1} = \left(\frac{\mathbb{1} + \eta}{2}\right) + \left(\frac{\mathbb{1} - \eta}{2}\right).$$

By Theorem 2.6.10 we see $J(C) \sim E_1 \times A$. Comparing dimensions we see $\dim A = 1$ so A must be an elliptic curve. □

Lemma 3.7.3. *Let C and η be as above. Let μ be an involution of $\mathbb{P}^1_t$ and let $\pi\colon \mathbb{P}^1_t \to \mathbb{P}^1_x$ be the quotient by μ. Assume that $\mu\eta = \eta\mu$ and $\pi_*(f)$ is a square-free polynomial of degree 6. Then the genus 2 curve C_F defined by the affine model*

$$V(y^2 - \pi_*(f))$$

is isogenous to a product of elliptic curves.

Proof. We need only show that η pushes down to an involution on C_F, i.e, that it is an involution on the roots of $\pi_*(f)$. Write

$$\pi_*(f) = f \cdot f^\mu = d^2 \prod_{i=1}^{6} (t - a_i)(t - \mu a_i).$$

Since μ and η commute

$$\begin{aligned}\pi_*(f)^\eta &= d^2 \prod_{i=1}^{6} (t - \eta^{-1} a_i)(t - \eta^{-1}\mu a_i) \\ &= d^2 \prod_{i=1}^{6} (t - \eta^{-1} a_i)(t - \mu(\eta^{-1} a_i))\end{aligned}$$

so η acts on the roots of $\pi_*(f) \in k[x]$ as well. Thus $(x, y) \to (\eta x, y)$ is an automorphism of

$$C_F := V(y^2 - \pi_*(f)(x)).$$

□

Corollary 3.7.4. *Let C_f and μ be as above. We apply the main result to obtain the isogeny relation*

$$J(A) \cong J(C_f) \times J(C_F)/\Delta \sim E_1 \times E_2 \times E_1' \times E_2'.$$

We now explain some of procedural details of the script. Given C_f and μ the script creates C_F and A based on the explicit formulae given by the norm construction (Lemma 3.4.5). We see that A must have an extra involution since C_F has an extra involution.

Example

Our example computation was done over the finite field $k := \mathbb{F}_{101}$. We chose $f := (t^2-1)(t^2-4)(t^2-9)$ and μ to be the involution $\mu(t) := \frac{14}{t}$. Our computation gives

$$\begin{aligned} C_f &= V(w^2 - f) \\ C_F &= V(y^2 - (65x^6 + 2x^4 + 11x^2 + 78)) \\ g(x) &= 51x^6 + 52x^4 + 36x^2 + 52 \\ A &= V(y^2 + 36x^6 + 99x^4 + 90x^2 + 23, 50x^6 + 49x^4 + 65x^2 + 49 + 100y + z^2) \subseteq \mathbb{A}^3_k. \end{aligned}$$

We assert $g(C_F) = 2$ in the program. The MAGMA command "AutomorphismGroup" assures us that $\mathrm{Aut}(A) = V_4$.

Chapter 4

Future directions

We discuss some of the future directions of research we can pursue from this point. Specifically we focus on the converse to the main theorem. We conjecture that the construction of the main theorem is the only way the Jacobian of a non-hyperelliptic genus 4 curve A decomposes like

$$\Delta \to J(C_F) \times J(C_f) \to J(A)$$

where Δ is the graph of the 2-torsion subgroup of $J(C_f)$. We provide a rough outline of the argument.

4.1 Converse to the main theorem

Suppose A is a genus 4 curve which is a double cover of a genus 2 curve C. Notice since C is hyperelliptic it is a double cover of a $\mathbb{P}^1$. If $A/\mathbb{P}^1$ is Galois then it is hyperelliptic. Otherwise, the Galois closure of $A/\mathbb{P}^1$ is dihedral and so A can be constructed from the norm construction. If we can show that $J(A)$ decomposing according to our restrictions implies that A is the double cover of a genus 2 curve then the converse to the main result will follow. The ideal tool to investigate this conjecture is the Torelli theorem. Throughout let

1. B_1, B_2 be principally polarized abelian varieties of dimension 2 such that there is an isomorphism $\psi\colon B_1[2] \to B_2[2]$.
2. $\Delta := \{(D, -\psi(D)) \subseteq B_1[2] \times B_2[2] : D \in B_1[2]\}$

Proposition 4.1.1. *Let $\phi\colon B_1 \times B_2 \to J(A)$ be the morphism of principally polarized abelian varieties as in the main result and let*

$$\tau' := \mathbb{1}_{B_1} \oplus [-1]_{B_2}\colon B_1 \times B_2 \to B_1 \times B_2.$$

Then there is a non-trivial involution on $J(A)$ respecting the polarization.

Proof. By Proposition 2.5.27 we see τ' respects polarizations. Moreover τ' fixes the kernel of ϕ. Since $\mathrm{char}(k) \neq 2$ and $\deg \phi$ is a power of 2 (See [14, Theorem I.7.2]) we see that $k(B_1 \times B_2)/\phi^* k(J(A))$ is a separable extension of degree $\#\Delta$. Let K/k be a finite extension such that each $P \in \Delta$ is a K-rational point and let $L := K(B_1 \times B_2)$. Then the map $t_P\colon B_1 \times B_2 \to B_1 \times B_2$ given by

$$t_P(x) := x + P$$

is an automorphism (as varieties) of $B_1 \times B_2/J(A)$ defined over K. Thus each t_P^* is an automorphism of $L/\phi^* K(J(A))$, so the extension is Galois. Notice for any $f \in \tau'^* \phi^* K(J(A))$ we have that f is fixed by each t_P^*, so $f \in \phi^* K(J(A))$. Hence $(\phi \circ \tau')^* K(J(A)) = \phi^* K(J(A))$, so

$$(\phi \circ \tau')^* k(J(A)) = \phi^* k(J(A)).$$

By Proposition 2.5.28 there is a unique τ respecting polarizations such that

$$\begin{array}{ccc} B_1 \times B_2 & \xrightarrow{\phi} & J(A) \\ & \searrow^{\phi\circ\tau'} & \downarrow \tau \\ & & J(A) \end{array}$$

commutes. Finally we see that since τ' is non-trivial so τ is also non-trivial. □

We see by combining Corollary 4.1.1 with Torelli's theorem that A must double cover a curve C.

Lemma 4.1.2. *Let $\phi\colon B_1 \times B_2 \to J(A)$ be as before and let $\tau\colon J(A) \to J(A)$ be the induced involution. Then there is a non-trivial isomorphism $\alpha\colon A \to A$ such that $\alpha_* = \tau$ or $\alpha_* = -\tau$.*

Proof. Let $P_0 \in A(\bar{k})$ be a point and let $j\colon A \to J(A)$ be the morphism

$$j(P) = [P - P_0]$$

as in Proposition 2.5.31. Note that j is not necessarily defined over k. By the Torelli theorem (Theorem 2.5.32) there is a $c \in J(A)$ and $\alpha\colon A \to A$ such that

$$j\alpha = \pm\tau j + c.$$

Without loss of generality we may assume the sign is positive. We see by evaluating both sides at P_0 that $c = j\alpha(P_0)$. Let $D \in j(A)$ and write $D = [P - P_0] = j(P)$. Then

$$\begin{aligned}\tau D &= \tau jP \\ &= j\alpha(P) - j\alpha(P_0) \\ &= [\alpha(P) - P_0] - [\alpha(P_0) - P_0] \\ &= \alpha_* D.\end{aligned}$$

So $\tau = \alpha_*$ when restricted to $j(A)$ and since elements of $j(A)$ generate (as a group) $J(A)(\bar{k})$ (See [10, Theorem A.8.1.1]) we have $\tau = \alpha_*$. Finally, since τ is nontrivial α is also nontrivial. □

The only thing left to verify is that $g(C) = 2$.

Lemma 4.1.3. *Let $\phi\colon B_1 \times B_2 \to J(A)$ and τ be as before. Let $\alpha\colon A \to A$ be the induced involution and let $C := A/\alpha$ be the double covered curve. Then $g(C) = 2$.*

Proof. Without loss of generality assume that $\tau = \alpha_*$ (so by abuse of notation we write $\tau = \alpha$). Let $\pi\colon A \to C$ be the quotient map. Then as usual there is the induced morphisms of Jacobians $\pi^*\colon J(C) \to J(A)$. Since $\pi_*\pi^* = [2]$ we see π^* has finite kernel. Since $\langle\tau\rangle = \mathrm{Aut}(A/C)$ we have by Lemma 3.5.2 that $\pi^*J(C) = \mathrm{Im}(\mathbb{1} + \tau)$. We also observe that

$$\begin{array}{ccc} B_1 \times B_2 & \xrightarrow{\phi} & J(A) \\ {\scriptstyle \mathbb{1}+\tau'}\downarrow & & \downarrow{\scriptstyle \mathbb{1}+\tau} \\ [2]B_1 & \xrightarrow{\phi} & \mathrm{Im}(\mathbb{1}+\tau) \end{array}$$

commutes. But $\phi \circ [2]$ has finite kernel. Hence since $\pi^*\colon J(C) \to \mathrm{Im}(\mathbb{1} + \tau)$ and $\phi \circ [2]\colon B_1 \to \mathrm{Im}(\mathbb{1} + \tau)$ are isogenies onto $\mathrm{Im}(\mathbb{1} + \tau)$ we see

$$\dim J(C) = \dim(B_1) = 2.$$

So $g(C) = \dim(B_1) = 2$. □

4.2 Other future directions

Let $\mathcal{J}_{2,2}$ be the set of genus 4 curves whose Jacobians are decomposable according to our restrictions. Since every genus 2 curve is hyperelliptic we can vary the admissible choices of C_f for the norm construction (Proposition 3.4.5) across the whole family of genus 2 curves $\mathcal{M}_2$. We can also vary μ across the set of all choices of involutions, which we shall call $\mathrm{Conf}_2 \mathbb{P}^1_k$. The norm construction gives a map of sets given by polynomial equations

$$\varphi \colon U \to \mathcal{J}_{2,2}$$

where $U \subseteq \mathcal{M}_2 \times \mathrm{Conf}_2 \mathbb{P}^1_k$ is the subset of pairs satisfying the technical conditions of the norm construction. We can ask how well ϕ classifies the objects in $\mathcal{J}_{2,2}$. We conjecture that

Conjecture 4.2.1. *For each $J \in \mathrm{Im}(\varphi)$ the set $\varphi^{-1}(J)$ is finite.*

Bibliography

[1] Oskar Bolza. Ueber die reduction hyperelliptischer integrale erster ordnung und erster gattung auf elliptische durch eine transformation vierten grades. *Mathematische Annalen*, 28(3):447–456, 1887.

[2] N. Bruin and E. V. Flynn. Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory*, 118(2):266–291, 2006.

[3] Nils Bruin. Visualising Sha[2] in abelian surfaces. *Math. Comp.*, 73(247):1459–1476 (electronic), 2004.

[4] Ron Donagi. The fibers of the Prym map. In *Curves, Jacobians, and abelian varieties (Amherst, MA, 1990)*, volume 136 of *Contemp. Math.*, pages 55–125. Amer. Math. Soc., Providence, RI, 1992.

[5] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[6] Torsten Ekedahl and J-P Serre. Exemples de courbes algébriques à jacobienne complètement décomposable. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 317(5):509–513, 1993.

[7] A. Fröhlich. Local fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 1–41. Thompson, Washington, D.C., 1967.

[8] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[9] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[10] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[11] Everett W. Howe. New bounds on the maximum number of points on genus-4 curves over small finite fields. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 69–86. Amer. Math. Soc., Providence, RI, 2012.

[12] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[13] Serge Lang. *Abelian varieties*. Springer-Verlag, New York-Berlin, 1983. Reprint of the 1959 original.

[14] J. S. Milne. Abelian varieties. Course notes http://www.jmilne.org/math/CourseNotes/index.html (version 2.00), last accessed 2013-10-05, 2008.

[15] David Mumford. Prym varieties. I. In *Contributions to analysis (a collection of papers dedicated to Lipman Bers)*, pages 325–350. Academic Press, New York, 1974.

[16] Jennifer R. Paulhus. *Elliptic factors in Jacobians of low genus curves*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–University of Illinois at Urbana-Champaign.

[17] H. Poincaré. Sur la réduction des intégrales abéliennes. *Bull. Soc. Math. France*, 12:124–143, 1884.

[18] Sevin Recillas. Jacobians of curves with g^1_4's are the Prym's of trigonal curves. *Bol. Soc. Mat. Mexicana (2)*, 19(1):9–13, 1974.

[19] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[20] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[21] André Weil. Zum beweis des Torellischen satzes. In *Œuvres scientifiques. Collected papers. Volume II (1951–1964)*. Springer-Verlag, Berlin, 2009. Reprint of the 1979 original.

Appendix A

MAGMA script

A.1 "Elliptic_Decomposition.m"

```
//This code builds a pair of genus 2 curves that both cover two elliptic
//curves.

d := 14;
k := FiniteField(101);
_<t>:=PolynomialRing(k);



//This is our starting x-line on the bottom.
KPX<X>:=FunctionField(k);
_<TP1>:=PolynomialRing(KPX);

//This is our t-line constructed as an extension of KPX.
KPT<T> := ext<KPX|TP1^2 - X*TP1 + d>;
_<TP2>:=PolynomialRing(KPT);

//and this is our involution by design
muT := d/T;
```

```
//We verify that we have done things correctly so far.
assert Genus(KPT) eq 0;
assert X eq (T + muT);

//We give an f used to construct C_f.
f := ((t)^2-1)*((t)^2-4)*((t)^2-9);
fT := Evaluate(f,T);
KCf := ext<KPT| TP2^2 - fT>;
assert Genus(KCf) eq 2;

//We identify our invariant and orbiting bits
finv := 1/2*(Evaluate(f,t) + Evaluate(f,muT));
forb := 1/2*(Evaluate(f,T) - Evaluate(f,muT));

//Construct F, r(x) = finv
F := Norm(fT);
r := (1/2)*Trace(fT);


//We construct a hyperelliptic genus 2 curve from F
KCF<Y>:=ext<KPX|TP1^2-F>;
_<TCF>:=PolynomialRing(KCF);
assert Genus(KCF) eq 2;

//This is the genus 4 curve.
KD1<Z>:=ext<KCF|TCF^2-(r-Y)>;
assert Genus(KD1) eq 4;


//Here we build a model of the curve.

P3<x,w,y,z> := ProjectiveSpace(k,[1,1,3,3]);
D := Curve(P3, [ Numerator(y^2 - w^6*Evaluate(F,x/w)),
```

```
                Numerator(z^2 - (w^6*Evaluate(g, x/w)) - w^3*y)]);


//Now we check the automorphism groups.
AutomorphismGroup(KCF);
AutomorphismGroup(KCf);
AutomorphismGroup(KD1);

//These all seem to be unusually large as expected.

assert IsHyperelliptic(D) eq false;
```