EXPLICIT CONSTRUCTION OF DECOMPOSABLE JACOBIANS

by
MESUT BUĞDAY

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Master of Science

Sabancı University
June 2024

ABSTRACT

EXPLICIT CONSTRUCTION OF DECOMPOSABLE JACOBIANS

MESUT BUĞDAY

Mathematics, Master Thesis, June 2024

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: Hyperelliptic curves, Jacobians, decomposable abelian varieties, rational points

In this thesis we give explicit constructions of decomposable hyperelliptic Jacobian varieties over fields of characteristic 0. These include Jacobians that are isogenous to a product of two absolutely simple varieties, a square of a hyperelliptic Jacobian, and a product of four hyperelliptic Jacobians three of which are of the same dimension. As an application, we produce families of hyperelliptic curves with infinitely many quadratic twists having at least two rational non-Weierstrass points; and families of quadruples of hyperelliptic curves together with infinitely many square-free d such that the quadratic twists of each of the curves by d possess at least one rational non-Weierstrass point.

ÖZET

AYRIŞTIRILABİLİR JAKOBİYENLERİN AÇIK YAPILARI

MESUT BUĞDAY

Matematik, Yüksek Lisans Tezi, Haziran 2024

Tez Danışmanı: Doç. Dr. Mohammad Sadek

Anahtar Kelimeler: Hipereliptik eğriler, Jakobiyen, ayrıştırılabilir abelyen varyeteler, rasyonel noktalar

Bu tezde 0 karakteristikli cisimler üzerinde ayrıştırılabilir hipereliptik Jakobiyen varyetelerin açık yapılarını veriyoruz. Bahsedilen Jakobiyen varyeteleri tamamen basit iki varyetenin çarpımına, bir hipereliptik Jakobiyenin karesi ve üçü aynı boyutta olan dört hipereliptik Jakobiyenlerin çarpımına izojeni olan Jakobiyenleri içermektedir. Bunun bir uygulaması olarak, sonsuz sayıdaki kuadratik twistlerinin en az iki Weierstrass olmayan rasyonel noktaya sahip hipereliptik eğri ailelerini ve hipereliptik eğri ailelerinin sonsuz sayıdaki kuadratik twistlerinin en az iki Weierstrass olmayan rasyonel noktaya sahip eğri ailelerini ve sonsuz sayıdaki tam kare olmayan d ile kuadratik twistlerinin en az bir Weierstrass olmayan rasyonel noktaya sahip dörtlü hipereliptik eğri ailelerini üretiyoruz.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Dr. Mohammad Sadek for his excellent vision, valuable guidance, enlightening advice, constant and supportive feedback throughout my master's. His influence on both my academic journey and my personality has made a significant impact. There are no words that can express my gratitude and feel honored to have a chance to work with him.

I also would like to thank the jury members, Assoc. Prof. Dr. Kağan Kurşungöz and Asst. Prof. Dr. Özer Öztürk for reviewing my thesis.

I owe heartfelt appreciation to the Mathematics Program at Sabancı University for creating a warm and welcoming environment. It was a memorable experience to be a member of Sabancı University during this study.

A very special thanks goes to my dearest friend Mustafa Umut Kazancıoğlu. I appreciate all of his positive energy, deep understanding, and continuous support by his friendship. Our meaningful discussions on various topics will always hold a special place in my mind.

I am extremely grateful with all my heart to my mother and sister for all their boundless motivation, love, and care.

Finally, I gratefully acknowledge the support provided by TÜBİTAK program 1001, project number 122F312.

To my family
Aileme

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

An elliptic curve E is a non-singular projective curve over a field K defined by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, ..., a_6 \in K$ with the point $\mathcal{O}$. In particular, elliptic curves are abelian varieties of dimension 1. Hence, elliptic curves have an abelian group structure. The set of K-rational points

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

is a finitely generated abelian group thanks to the celebrated Theorem of Mordell-Weil. In particular, $E(K) \cong \mathbb{Z}^r \times \mathcal{T}$ where r is the Mordell-Weil rank of E over K and $\mathcal{T}$ is the torsion part of $E(K)$. In [38, 39], Mazur showed that there are 15 possible groups that can occur as torsion subgroups of $E(K)$ when $K = \mathbb{Q}$.

On the other hand, it is commonly known that a hyperelliptic curve possess only a finite number of points over any number field due to Falting's Theorem, [13]. Thus, rational points on hyperelliptic curves unfortunately do not possess a natural group structure. However, it is still possible to define a variety associated to each curve, namely the Jacobian variety denoted by $\mathrm{Jac}(C)$. The Jacobian of an algebraic curve has the structure of abelian varieties. That is the set of rational points on $\mathrm{Jac}(C)$ over a number field forms an abelian group. Let $J(K)$ denotes the set of K-rational points of Jac(C), then due to the Mordell-Weil Theorem $\mathrm{Jac}(C) \cong \mathbb{Z}^r \times J(K)_{\mathrm{tors}}$ where $r \in \mathbb{Z}^{\geq 0}$ is the rank of $J(K)$ and $J(K)_{\mathrm{tors}}$ is the finite torsion subgroup of $J(K)$.

An abelian variety is said to be *decomposable* over a field K if it is isogenous to a product of abelian varieties of lower dimension. The study of decomposable Jacobian varieties of genus two curves was initiated in [20], see also [29].

A family of hyperelliptic curves of arbitrary genus whose Jacobians decompose into

two abelian varieties was given in [10], namely, for the Jacobian of the hyperelliptic curve defined by the equation

$$y^2 = (x^n - 1)(x^n - t), \quad n = 2k+1, \quad k > 1, \quad t \in \mathbb{C} \setminus \{0, 1\},$$

there are two algebraic curves Y_1 and Y_2 of genus k such that $\mathrm{Jac}(X)$ is isomorphic to $\mathrm{Jac}(Y_1) \times \mathrm{Jac}(Y_2)$. Ekedahl and Serre constructed examples of curves whose Jacobians decompose completely into elliptic curves, [11]. The reader may also see [67] for such examples of curves over number fields. Jacobian varieties of algebraic curves with many automorphisms provide examples of abelian varieties that contain many factors in their decompositions. In [51, 52, 53], such curves whose Jacobians contain many elliptic factors were displayed. In [4], the existence of Jacobians that are isogenous to the product of arbitrary many Jacobians of the same genus, not necessarily equal to one, was established.

In this thesis, we consider the following question. Given a positive integer n together with a partition $n_1 \leq n_2 \leq ... \leq n_k$ of n, does there exist an abelian variety of dimension n that decomposes into a product of k abelian varieties of dimensions $n_1, \cdots, n_k$? When $k = 2$ and n is even, we give explicit examples of families of hyperelliptic Jacobian varieties that decompose into the product of two absolutely simple Jacobian varieties of the same dimension $n/2$; and families of hyperelliptic Jacobian varieties that decompose as the square of a Jacobian variety. When n is odd, we present examples of hyperelliptic Jacobian varieties that decompose into the product of two absolutely simple Jacobian varieties of dimensions $(n-1)/2$ and $(n+1)/2$. We exhibit families of hyperelliptic Jacobians that decompose into the product of three Jacobians of dimensions k, $k+1$, $2k$ when $n = 4k+1$, $k \geq 1$; and $k+1$, $k+1$, $2k+1$ when $n = 4k+3$, $k \geq 0$. Further, we prove the existence of hyperelliptic Jacobian varieties of odd dimension n that decompose as the product of four Jacobian varieties of dimensions k, k, k, $k+1$, when $n = 4k+1$, $k \geq 1$; and k, $k+1$, $k+1$, $k+1$ when $n = 4k+3$, $k \geq 1$. In particular, given any integer M, there is a decomposable abelian variety of dimension $4M \pm 1$ whose decomposition contains three factors each of dimension M.

Let C/K be a hyperelliptic curve described by $C : y^2 = f(x)$. The quadratic twist of C by $d \in K \backslash K^2$ is given by

$$C_d : dy^2 = f(x).$$

Goldfeld Conjecture states that the average rank of elliptic curves over the rational field in families of quadratic twists is $1/2$. In other words, quadratic twists of an elliptic curve over the rational field with rank at least 2 are rare. In [55, 30], quadratic

twists of elliptic curves with ranks at least 2 or 3 were given. A similar problem was posed to find tuples of elliptic curves whose quadratic twists by the same rationals are of positive rank infinitely often, [6, 25]. As for hyperelliptic curves, one may construct families of these curves with infinitely many quadratic twists that possess no rational points, [56, 32]. As a byproduct of our construction of decomposable Jacobian varieties, we produce examples of hyperelliptic curves with infinitely many quadratic twists possessing at least two rational non-Weierstrass points. In particular, we introduce examples of elliptic curves with infinitely many quadratic twists of rank at least 2. In addition, we give examples of families of quadruples of hyperelliptic curves, three of which are of the same genus, such that for infinitely many square-free rationals the quadratic twists of each of these hyperelliptic curves by these rationals possess at least one rational non-Weierstrass point.

2. Algebraic Curves

Throughout this thesis K will be a field and $K[x_1,\ldots,x_n]$ denotes the polynomial ring in n variable over K.

2.1 Projective spaces

Definition 2.1. *The Affine space $\mathbb{A}^n(K)$ over K is the collection of n-tuples given by*

$$\mathbb{A}^n(K) = \{(x_1,\ldots,x_n) : x_i \in K\}.$$

Definition 2.2. *The Projective space $\mathbb{P}^n(K)$ over K is the set of $n+1$ tuples in $\mathbb{A}^{n+1}(K)\setminus\{(0,\cdots,0)\}$ under the equivalence relation $\sim$ defined by $(x_0,\ldots,x_n)\sim(x_0^{'},\ldots,x_n^{'})$ if $(x_0,\ldots,x_n)=(\lambda x_0^{'},\ldots,\lambda x_n^{'})$ for some $\lambda\in K^*$.*

In other words, $\mathbb{P}^n(K) = \mathbb{A}^{n+1}(K)\setminus\{(0,\ldots,0)\}/\sim$. The relation $\sim$ holds for two points if they lie on the same line through the origin. We will denote a point in $\mathbb{P}^n$ by $(x_0:\cdots:x_n)$. When $n=1$, $\mathbb{P}^1(K)$ is called the projective line over K, whereas $\mathbb{P}^2(K)$ is called the projective plane over K. When we write $\mathbb{A}^n$, we mean $\mathbb{A}^n(\overline{K})$ where $\overline{K}$ is an algebraic closure of K; similarly $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$.

In $\mathbb{R}^2$, every line through the origin, $y=mx$ where $m\in\mathbb{R}^*$, intersects the line $y=1$ in one point, namely $(1/m,1)$. In other words, every line $y=mx$ corresponds to the point $(1/m:1)$ in $\mathbb{P}^1(\mathbb{R})$. In addition, the y-axis corresponds to the point $(0:1)$ in $\mathbb{P}^1(\mathbb{R})$. The x-axis does not intersect the line $y=1$, and it corresponds to the point $(1:0)$ in $\mathbb{P}^1(\mathbb{R})$.

Following the argument above, one can see that $\mathbb{P}^1(K) = \{(x:1) : x\in K\}\cup\{(1:0)\}$. Therefore, the projective line $\mathbb{P}^1(K)$ can be considered as an extension of the affine space $\mathbb{A}^1(K)$ by an extra point $(1:0)$; called the point at infinity. The latter

description can be justified using the map $\Theta^1 : \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ defined by $x \mapsto (x : 1)$. In general, we can embed $\mathbb{A}^n$ in $\mathbb{P}^n$ via the map $\Theta^n : (x_1, \ldots, x_n) \to (x_1 : \cdots : x_n : 1)$.

2.2 Projective Curves

Definition 2.3. *A point $P = (a_1, ..., a_n) \in \mathbb{A}^n$ is called a zero of the polynomial $f \in K[X_1, ..., X_n]$ if $f(P) = 0$.*

Definition 2.4. *Let $S \subseteq K[X_1, ..., X_n]$. The vanishing set of S is defined by*

$$V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\} \subseteq \mathbb{A}^n$$

Definition 2.5. *A subset $\mathcal{X} \subseteq \mathbb{A}^n$ is called an algebraic set if there exists $S \subseteq K[X_1, ..., X_n]$ such that $V(S) = \mathcal{X}$.*

In other words, an affine algebraic set is exactly the zero set of polynomials. Moreover, $\mathcal{X}$ is irreducible if $\mathcal{X}$ cannot be written as the union of two of its proper subsets.

Example 2.6. *Consider $F(x, y) = y^2 - x(x^2 - 1)$ over $\mathbb{R}$. Then the vanishing set is*

$$V(F) = \{(x, y) : y^2 = x(x^2 - 1)\} \subseteq \mathbb{R}^2$$

Definition 2.7. *A polynomial $f \in K[X_1, \ldots, X_n]$ is called homogeneous of degree n if*

$$f = (\lambda x_0, ..., \lambda x_n) = \lambda^n f(x_0, ..., x_n) \quad \text{for all } \lambda \in K.$$

Definition 2.8. *A projective curve C of degree d is the zero set of non-constant homogeneous polynomial $f \in K[X_1, \ldots, X_{n+1}]$ of degree d. Namely,*

$$C = \{P = (x_1 : \cdots : x_{n+1}) \in \mathbb{P}^n \mid f(P) = 0\}.$$

When $d = 1$, the projective curve corresponds to lines. More explicitly, the homogeneous polynomial f expressed as $f(x, y, z) = c_0x + c_1y + c_2z$ where c_i's are in K represents a line in $\mathbb{P}^2(K)$. Furthermore, a line L passing through two different points $P = (x_0 : ... : x_n)$ and $P' = (x'_0 : ... : x'_n)$ in $\mathbb{P}^n$ can be represented by

$[cx_0 + dx'_0 : \cdots : cx_n + dx'_n]$ for some $c, d \in K$; or simply $[Cx_0 + x'_0 : \cdots : Cx_n + x'_n]$, $C \in K^*$.

On the other hand, the projective algebraic plane curves given by the equation $F(x, y, z) = c_0x^2 + c_1y^2 + c_3z^2 + c_4xy + c_5xz + c_6yz$ where c_i's are in K are called conics.

Definition 2.9. *Let $F \in K[X_1, X_2, X_3]$ be a homogeneous polynomial with $V := V(F)$. A function field of V is defined as*

$$\overline{K}(V) = \left\{ \frac{f_1}{f_2} : f_1 \text{ and } f_2 \text{ are polynomials of the same degree in } K[X_1, X_2, X_3] \right\}$$

such that the following conditions hold:

i) f_2 does not vanish identically on V.

ii) $\frac{f_1}{f_2} \sim \frac{g_1}{g_2}$ if $f_1g_2 - f_2g_1$ vanishes identically in V.

Definition 2.10. *Let $V_1 = V(F_1)$, $V_2 = V(F_2) \subseteq \mathbb{P}^2$. A rational map $\Phi = (f_1, f_2, f_3) : V_1 \to V_2$ is a map such that $\Phi(P) = (f_1(P), f_2(P), f_3(P)) \in V_2$; $P \in V_1$ where $f_1, f_2, f_3 \in \overline{K}(V_1)$.*

Remark 2.11. *We say that Φ is defined over K if there exists $\lambda \in \overline{K}^*$ such that λf_1, λf_2, $\lambda f_3 \in K(V_1)$.*

Definition 2.12. *Φ is regular at $P \in V_1$ if there is $g \in \overline{K}(V_1)$ so that $gf_1(P)$, $gf_2(P)$, $gf_3(P)$ are all defined and not all zero at P.*

Definition 2.13. *A rational map is a morphism if Φ is regular at every point in V_1.*

We have the following result that can be found in [66].

Theorem 2.14. *[66] A morphism between projective curves either constant or surjective.*

Definition 2.15. *A morphism $\Phi : V_1 \to V_2$ is an isomorphism if there exists $\Psi : V_2 \to V_1$ such that $\Phi \circ \Psi = \mathrm{id}_{V_2}$ and $\Psi \circ \Phi = \mathrm{id}_{V_1}$.*

Definition 2.16. *A plane projective curve C over K described by a homogeneous polynomial $f(x, y, z)$ has a singular point P if*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0.$$

If C does not have any singular point, then C is called smooth.

Example 2.17. *Two algebraic curves C_1 and C_2 described by the polynomials*

$$C_1 : f(x,y) = y^2 - x^3 - x = 0, \qquad C_2 : g(x,y) = y^2 - x^3 = 0$$

One can easily see that C_1 is smooth at every point P, however C_2 has only one singular point, $(0,0)$.

Example 2.18. *Consider the projective algebraic plane curve C with the equation of the form $F(x,y,z) = x^3 + y^3 - z^3$. It can be seen that*

$$F_x(x,y,z) = F_y(x,y,z) = F_z(x,y,z) = 0 \iff P = (0,0,0)$$

Obviously, P does not lie in $\mathbb{P}^2$. Hence, C is smooth.

The following result can be found in [62].

Proposition 2.19. *[62, Prop. 2.1] Let V_1 and V_2 be a projective curves in $\mathbb{P}^2$ with a rational map $\Phi : V_1 \to V_2$. If V_1 is smooth at P then Φ is regular at P.*

2.3 Conics

In this section, all materials can be found in [63] and [66].

Definition 2.20. *A plane projective curve C over a field K defined by a homogeneous polynomial equation of the form*

$$Ax^2 + By^2 + Cz^2 + 2Dxy + 2Exz + 2Fyz = 0, \qquad A, B, C, D, E, F \in K$$

is called a conic.

In particular, C is called a rational conic if $K = \mathbb{Q}$. In case of $\mathrm{char}(K) \neq 2$, and after a suitable transformation, each conic C can be described by the following form

$$C_{a,b,c} : ax^2 + by^2 + cz^2 = 0, \text{ with } abc \neq 0.$$

The conic $C_{a,b,c}$ is called a diagonal conic. In other words, if $\mathrm{char}(K) \neq 2$ then each conic C is isomorphic to $C_{a,b,c}$ for some $a, b, c \in K$.

One question to pose is how one can find a point on a given conic $ax^2 + by^2 + cz^2 = 0$ where $a, b, c \in \mathbb{Z}$. Thanks to Legendre, we have the following theorem.

Theorem 2.21. *[66] Let a, b, c be pairwise coprime square-free integers whose signs are not all the same. The equation $ax^2 + by^2 + cz^2$ has a rational solution if and only if the congruence*

$$X^2 \equiv -bc \mod a, \qquad Y^2 \equiv -ca \mod b, \qquad Z^2 \equiv -ab \mod c$$

can be simultaneously satisfied.

Moreover, considering the above, the following question may be asked.

Question 2.22. *Is there any way to parameterize the set of all points on a conic $C_{a,b,c} : ax^2 + by^2 + cz^2 = 0$ if there is a known point on $C_{a,b,c}$?*

The following theorem gives a parametrization of points on conics.

Theorem 2.23. *[66] Let $C_{a,b,c} : ax^2 + by^2 + cz^2 = 0$ be an irreducible diagonal conic with a point $[x_0 : y_0 : z_0]$ and assume without loss of the generality that $z_0 \neq 0$. Then, a point (x, y, z) on $C_{a,b,c}$ can be parametrized as follows*

$$\begin{aligned} x &= Q_1(U, V) = ax_0U^2 + 2by_0UV - bx_0V^2 \\ y &= Q_2(U, V) = -ay_0U^2 + 2ax_0UV + by_0V^2 \\ z &= Q_3(U, V) = -az_0U^2 - bz_0V^2 \end{aligned}$$

where U and V are parameters.

$(Q_1(U,V) : Q_2(U,V) : Q_3(U,V))$ is a polynomial map defined over K that sends each $(U : V)$ in $\mathbb{P}^1$ to a point on the curve C. Moreover, we can recover the point $(U : V)$ via the inverse map from C to $\mathbb{P}^1$ defined by

$$U = x - \frac{x_0}{z_0}z, \; V = y - \frac{y_0}{z_0}z.$$

Therefore, we have an invertible map from C to $\mathbb{P}^1$ that is given by rational (in fact polynomial) functions that are defined at every point.

Theorem 2.24. *[66] Let C be a geometrically irreducible conic with a rational point over a field K of $\mathrm{char}(K) \neq 0$. Then C is isomorphic to the projective line $\mathbb{P}^1$ over K.*

As an application, finding rational solutions of an equation $x^2 + y^2 = z^2$ is equivalent to finding triples (a, b, c) corresponding to a point $(x, y) = (\frac{a}{c}, \frac{b}{c})$ on the circle $C : x^2 + y^2 = 1$.

In particular, a unit circle has a rational point $P = (-1, 0)$, and certainly, P is not the only point with rational coordinates.

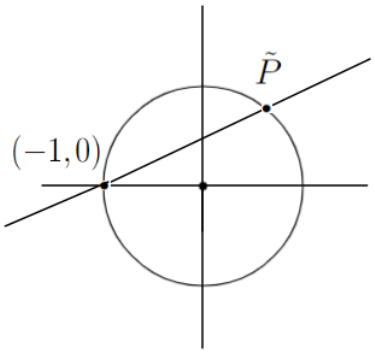

Figure 2.1 Parametrization of the unit circle

Now, draw a line passing through $(-1,0)$ with a rational slope a. That line intersects the circle at another point $\tilde{P}$. Obviously, the equation of that line is $y = ax + a$. By substituting $y = ax + a$ into the equation of a circle, one can express x in terms of a after solving the quadratic equation $(a^2+1)x^2 + 2a^2x + (a^2-1) = 0$. Hence, straightforward calculations provide a parametrization

$$x = \frac{1-a^2}{1+a^2}, \quad y = \frac{2a}{1+a^2}.$$

In other words, one can write x and y in terms of one free parameter a that creates an isomorphism between the unit circle and the projective line.

Therefore, in general, once a point lies on the conic, then this leads to the existence of infinitely many points on it.

2.4 Elliptic Curves

Consider the homogeneous polynomial $F(X,Y,Z)$ given by an equation of the form

$$F(X,Y,Z) = aX^3 + bY^3 + cZ^3 + dX^2Y + eX^2Z + fXY^2 + gXZ^2 + hXYZ + iY^2Z + jYZ^2$$

in $K[X,Y,Z]$. Any such F with $V(F) \neq \emptyset$ can be written as a Weierstrass equation

$$\tilde{F}(X,Y,Z) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

In particular, the point $(0:1:0)$ lies in $\tilde{F}(X,Y,Z)$.

Definition 2.25. *An elliptic curve over a field K is defined as $V(F)$ for some $F \in K[X,Y,Z]$ where*

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

with the point $[0:1:0]$, called the point at infinity, and the coefficients belong to K.

After substituting $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ and dehomogenization, one may obtain the polynomial

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

Definition 2.26. *An elliptic curve E/K has a Weierstrass equation of the form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, ..., a_6 \in K$ having the point $\mathcal{O} = (0:1:0)$ with nonzero discriminant $\Delta(E)$

where the discriminant $\Delta(E)$ of an elliptic curve E is defined by

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

We also define the following quantities,

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_3^2 + 36b_2b_4 - 216b_6, \\ j &= c_4^3/\Delta. \end{aligned}$$

In particular, the quantity j is called j-invariant of the elliptic curve E, denoted by $j(E)$.

In the case of $\operatorname{char} K \neq 2, 3$ and after a suitable transformation, an elliptic curve E can always be described by the model which is called the short Weierstrass equation,

$$E_{A,B} : y^2 = x^3 + Ax + B, \qquad A, B \in K.$$

Therefore, one may obtain the following equivalent definition of an elliptic curve.

Definition 2.27. *An elliptic curve E is a smooth projective plane curve over K with* $\mathrm{char}(K) \neq 2,3$ *defined by an equation of a form*

$$E_{A,B} : y^2 = x^3 + Ax + B, \qquad A, B \in K$$

having the point $\mathcal{O} = (0:1:0)$ with associated discriminant $-16(4A^3 + 27B^2)$.

Moreover, it is straightforward from the definition of smoothness that $\Delta(E_{A,B}) \neq 0$ if and only if $x^3 + Ax + B$ does not have a multiple root.

Apparently, Δ depends on the choice of the Weierstrass equation describing the elliptic curve. However, that is not the case for the j-invariant.

Definition 2.28. *Let $(E, \mathcal{O}_{E_1})$ and $(E', \mathcal{O}_{E_2})$ be two elliptic curves over K described by equations of the form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

are isomorphic if and only if there is a transformation ω defined in the following way

$$\omega(x, y) = (u^2x' + r,\ u^3y' + u^2tx' + s); \qquad u, r, s, t \in K,\ u \neq 0$$

In particular, $\omega(\mathcal{O}_{E_1}) \to \mathcal{O}_{E_2}$.

In case of $\mathrm{char}(K) \neq 2,3$, the two elliptic curves defined by equations

$$E : y^2 = x^3 + Ax + B, \qquad E' : y^2 = x^3 + A'x + B', \qquad A, B, A', B' \in K$$

are isomorphic over K if and only if $A' = u^4A$ and $B' = u^6B$ for some $u \in K^*$.

One can have a useful related proposition over an algebraically closed field.

Proposition 2.29. *[62, Proposition 1.4] Two elliptic curves E and E' are isomorphic over $\overline{K}$ if and only if $j(E) = j(E')$.*

Example 2.30. *Consider the three elliptic curves E_1, E_2, E_3 over $\mathbb{F}_2$ defined by*

$$E_1 : y^2 + y = x^3, \qquad E_2 : y^2 + y = x^3 + 1, \qquad E_3 : y^2 + y = x^3 + x$$

Clearly, $j(E_1) = j(E_2) = j(E_3) = 0$ so they are all isomorphic over $\overline{\mathbb{F}_2}$.

Let $E(K)$ be the set of K- rational points of elliptic curve E,

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

It is widely known that elliptic curves have an algebraic group structure with the operation denoted by "+". Hence, the pair $(E,+)$ forms a group. This group law can be explained geometrically through the chord and tangent process for any field of characteristic 0. Before discussing the group operation, we must mention the key ingredient, Bézout's Theorem.

Theorem 2.31. *[19, Bézout's Theorem] Let $f_1, f_2 \in K[x_1,x_2,x_3]$ and $V(f_1), V(f_2) \subseteq \mathbb{P}^2$ be two projective plane curves having no common components in K. Then the number of points of intersection between $V(f_1)$ and $V(f_2)$ is given by $\deg(f_1)\deg(f_2)$.*

Let P_1, P_2 be two distinct points on the elliptic curve E. Let ℓ be the line passing through P_1 and P_2. Theorem 2.31 guarantees that line ℓ intersects the curve at third point, call that point P_3. Let ℓ' be the line passing through P_3 and $\mathcal{O}$. The line ℓ' touches the curve at $P_3, \mathcal{O}$ and a third point which we call $P_1 + P_2$. Hence, $P_1 + P_2$ corresponds to the reflection of P_3 across to x-axis. Also, $P_1 + P_2 = \mathcal{O}$ if and only if $P_2 = -P_1 = (x,-y)$ where $P_1 = (x,y)$.

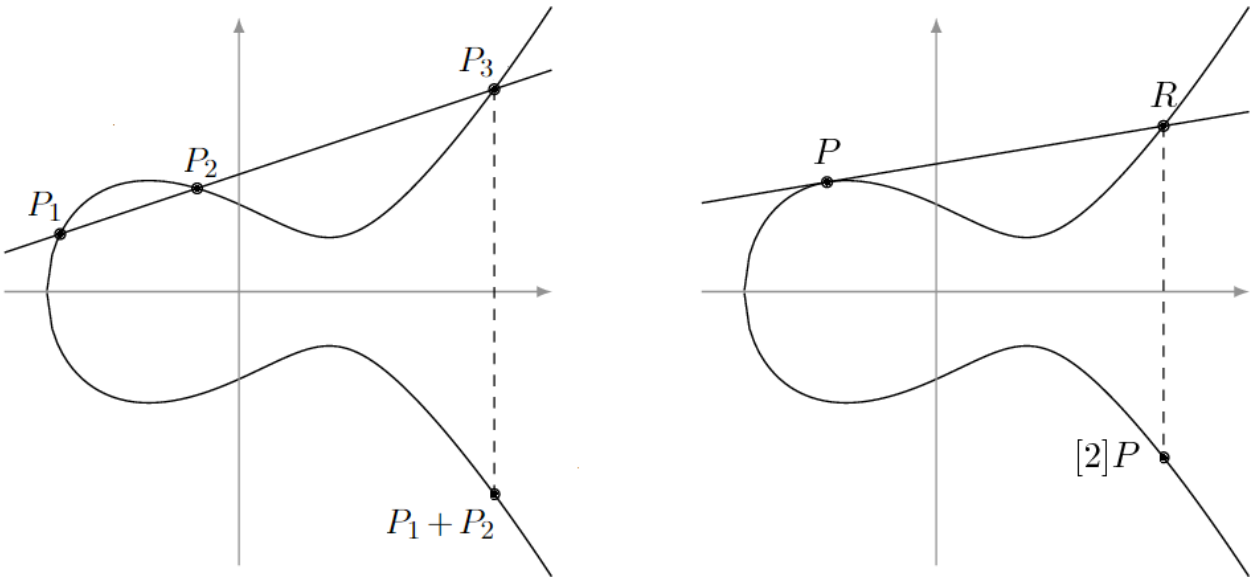

Figure 2.2 Geometric interpretation of group law over K, [14]

If we want to add $P_1 + \mathcal{O}$, the lines ℓ and ℓ' overlap. Draw the vertical line through P_1 then the reflection of P_1 about x-axis will be the common point of ℓ and the curve which is $-P_1$. Thus, $P_1 + \mathcal{O} = P_1$. It holds for any points on elliptic curve so $\mathcal{O}$ is the identity element.

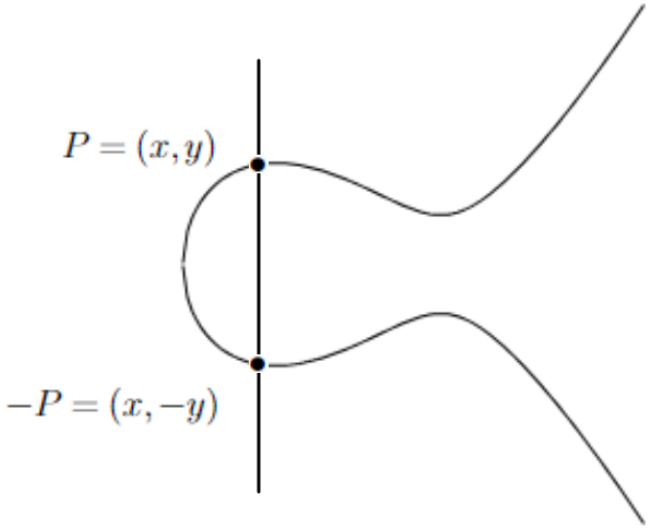

Figure 2.3 Adding a point with its inverse

Remark 2.32. *$E(K)$ is a subgroup of the elliptic curve $(E, +)$. We call $E(K)$ the Mordell-Weil group of E over K.*

It is clear that $E(K)$ is an abelian group by construction. The following result is called the Mordell-Weil Theorem.

Theorem 2.33. *[62, Theorem 6.7] Let K be a number field and E/K be an elliptic curve. Then, the Mordell-Weil group $E(K)$ is finitely generated.*

We have the following result thanks to the Fundamental Theorem of Finitely Generated Abelian group.

Corollary 2.34. *There exists an integer $r \geq 0$ such that*

$$E(K) \cong \mathbb{Z}^r \times \mathcal{T}$$

where r is the rank of E over K and $\mathcal{T}$ is the finite part consisting of elements of finite order of $E(K)$.

The torsion structure is completely classified when $K = \mathbb{Q}$, no surprises left. However, the intriguing part is the rank. For example, people believe that all elliptic curves with rank 0 are fifty percent and those with rank 1 are another fifty percent, and elliptic curves of higher rank are quite rare. This is at least what people believe due to the famous Rank Distribution Conjecture [60]. The following results can be found in the corresponding references.

Theorem 2.35. *[2, Bhargava-Shankar] At least $\frac{5}{8}$ of elliptic curves over $\mathbb{Q}$ have rank 0 or 1.*

Theorem 2.36. *[66, Bhargava-Shankar] The average rank of all elliptic curves over* $\mathbb{Q}$ *is less than* 1*.*

On the other hand, there exists elliptic curves of rank 0 with trivial torsion even on the number fields, see the reference for more examples [35, 40].

Theorem 2.37. *[46] An elliptic curve is defined by the following expression*

$$E : y^2 = 4x^n - 1, \qquad n = 3,\ 4$$

has only the point at infinity.

Theorem 2.38. *[40, Mazur-Rubin] For each number field* K*, there are infinitely many* E/K *with* $E(K) = 0$*.*

On the other hand, even though there is no upper bound for the rank, it is also known as Folklore Conjecture [60], the largest rank over $\mathbb{Q}$ that we know up to now is 28 by Elkies.

Mazur managed to classify all possible torsion subgroups of $E(K)$ when $K = \mathbb{Q}$. There are also studies about the classification of the torsion part of elliptic curves over quadratic, cubic and quartic fields. We will not dig deeply in the torsion structure as it is out of the thesis's scope.

Theorem 2.39. *[38, 39, Mazur] Let* $E/\mathbb{Q}$ *be an elliptic curve. The possible rational torsion subgroup* $\mathcal{T}$ *is one of the fifteen groups stated in below:*

$$\begin{cases} C_m & 1 \leq m \leq 12,\ m \neq 11 \\ C_2 \times C_{2m} & 1 \leq m \leq 4 \end{cases}$$

where C_m *is the cyclic group of order* m*.*

One can notice that the order of torsion point cannot exceed 12. In order to decide whether the point belongs to the torsion part of $E(\mathbb{Q})$ or not, it is enough to keep adding point up to 12.

Theorem 2.40. *[62, Nagell-Lutz] Let* $E/\mathbb{Q}$ *be an elliptic curve described by*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

If $P = (x, y)$ *is a nonzero torsion point then,*

i) $x, y \in \mathbb{Z}$*, and*

ii) either $y = 0$ *or* $y^2 \mid 4A^3 + 27B^2$*.*

2.5 Elliptic Surfaces

Definition 2.41. *[61] An elliptic surface $\mathcal{E}(t)$ is defined by the following Weierstrass equation*

$$\mathcal{E}(t) : y^2 = x^3 + P(t)x + Q(t), \qquad P(t), Q(t) \in K[t]$$

with the discriminant $\Delta(t) = -16(4P(t)^3 + 27Q(t)^2) \neq 0$.

Basically, $\mathcal{E}(t)$ is an elliptic curve over $K(t)$. More precisely, the curve obtained by replacing $t_0 \in K$ in the Weierstrass equation is called the specialization or fibre. For all but finitely many specializations by $t_0 \in K$ represents an elliptic curve. Namely, $\mathcal{E}_{t_0}$ be an elliptic curve of the form

$$\mathcal{E}(t_0) : y^2 = x^3 + P(t_0)x + Q(t_0)$$

provided that $P(t_0), Q(t_0) \neq \infty$ and $\Delta(t_0) = -16(4P(t_0)^3 + 27Q(t_0)^2) \neq 0$

Theorem 2.42. *[31, Lang-Neron] Let $\mathcal{E}(t)/K(t)$ be an elliptic surface then $\mathcal{E}(K(t))$ is a finitely generated abelian group.*

We have the following results over $\mathbb{Q}(t)$ that can be found in [60, 62]. On the other hand, Mestre provided examples of elliptic surfaces with the rank $\geq 11, 12$, and an example of the rank ≥ 13 over $\mathbb{Q}(t)$ is given by Nagao. One may see that the elliptic surfaces of rank $\geq 18, 19, 20, 21, 22$ over $\mathbb{Q}(t)$ in the references [60, 15, 44, 45, 16], respectively.

Theorem 2.43. *[62, Silverman Specialization Theorem] Let $\mathcal{E}_t/\mathbb{Q}(t)$ be a non-constant elliptic curve. Then, for all but finitely many $t_0 \in \mathbb{Q}$ the specialization map $E_t(\mathbb{Q}(t)) \to E_{t_0}(\mathbb{Q})$ is injective. Therefore,*

$$\operatorname{rank}(E_{t_0}(\mathbb{Q})) \geq \operatorname{rank}(E_t(\mathbb{Q}(t))).$$

In particular, if the point $(x(t), y(t))$ lies in $\mathcal{E}(\mathbb{Q}(t))$ and there is a specialization $t = t_0 \in \mathbb{Q}$ such that $P_{t_0} : (x(t_0), y(t_0)) \in E_{t_0}(\mathbb{Q})$ is a point of infinite order on E_{t_0} then $(x(t), y(t))$ is a point of infinite order in elliptic surface $\mathcal{E}(\mathbb{Q}(t))$.

In elliptic surfaces, each term is written in terms of polynomials on t and the specialization reduces a surface to a curve over $\mathbb{Q}$. Luckily, we have a criteria to decide whether point is of finite or infinite order over $\mathbb{Q}$ by Theorem 2.40. Hence, it enjoys the torsion property.

As we mentioned above, there is relation between the rank of an elliptic surface $\mathcal{E}(\mathbb{Q}(t))$ and the rank of a specialization $\mathcal{E}(\mathbb{Q}(t_0))$ for some $t_0 \in \mathbb{Q}$. Is it possible to force this inequality to be strict i.e., $\text{rank}(\mathcal{E}_{t_0}(\mathbb{Q})) > \text{rank}(\mathcal{E}_t(\mathbb{Q}(t)))$?

Question 2.44. *Can one find infinitely many $t_0 \in \mathbb{Q}$ such that the rank of the specialization at t_0 is strictly larger than the rank of the elliptic surface?*

$$\text{rank}(\mathcal{E}_{t_0}(\mathbb{Q})) \geq n + \text{rank}(\mathcal{E}_t(\mathbb{Q}(t)))$$

n is called the jump in the rank.

Cassels and Schinzel showed that an elliptic surface defined by the equation

$$\mathcal{E}(t) : y^2 = x(x^2 - (7 + 7t^4)^2)$$

has rank 0 but the rank of $\mathcal{E}(r)$ is odd for any $r \in \mathbb{Q}$, see [5]. This means that there is a jump in the rank by at least 1.

Can one improve the jump for other elliptic surfaces by $+2$ or $+3$? In fact, there is some research on that problem. For example, C. Salgado managed to show that the jump in the rank can be $1, 2$ or 3 for certain elliptic surfaces, see the references [7, 37, 57]. In addition, 3 is the largest jump that the author reached.

On the other hand, we can define the root number of an elliptic curve E denoted by $\mathcal{W}(E)$. The well-known Parity conjecture asserts that the root number of an elliptic curve $E/\mathbb{Q}$ is

$$\mathcal{W}(E) = (-1)^{\text{rank}(E)}.$$

Roughly, $\mathcal{W}(E)$ is always ± 1. In particular, an elliptic curve E with $\mathcal{W}(E) = -1$ must contain infinitely many rational points i.e., E has odd rank.

Example 2.45. *[9] Every elliptic surface given by the equation of the form*

$$\mathcal{E} : y^2 = x^3 + c(3a^2t^6 + b^2)$$

with generic rank 2 has a constant root number on their fibres: $W(\mathcal{E}_t) = +1$ for all $t \in \mathbb{Q}$.

Note that Theorem 2.43 together with the Parity conjecture implies that every single specialization must have even rank ≥ 2. It is a nice example although it does not provide a strict jump, it may lead to new questions. One of them is the following, can we find an elliptic surface $\mathcal{E}_t$ such that $W(\mathcal{E}_t) = -1$ for all $t \in \mathbb{Q}$? Apparently, the possible answer provides a strict inequality.

There may be a relation between the root number and the jump in the rank. Consider an elliptic surface $\mathcal{E}(t)$ of $\text{rank}(\mathcal{E}(t)) = 1$ with $\mathcal{W}(E_{t_0}) = +1$ for all specialization t_0. Then there is a jump by at least 1. The remaining problem is to find an elliptic surface that satisfies these properties.

2.6 Quadratic Twists of Elliptic Curves

Definition 2.46. *Let E/K be an elliptic curve defined by an equation of the form $E : y^2 = f(x)$. The quadratic twist of elliptic curve E by $d \in K \backslash K^2$ is given by*

$$E_d : dy^2 = f(x).$$

Indeed, E and E_d are isomorphic over $K[\sqrt{d}]$ via the map $(x, y) \mapsto (x, y\sqrt{d})$.

Theorem 2.47. *[60, Goldfeld Conjecture] The average rank of quadratic twists of elliptic curves is $1/2$ over $\mathbb{Q}$.*

In other words, $\text{rank}(E_d) = 0$ or 1. Moreover, Goldfeld conjecture states that $\text{rank}(E_d) \geq 2$ have zero density. On the other hand, there are also papers about quadratic twists of elliptic curves with the rank ≥ 2, for those of the rank is 2, see [55].

Example 2.48. *[46] There are infinitely many elliptic curves having only point at infinity defined by*

$$E_D : Dy^2 = 4x^n - 1, \qquad n = 3, 4 \text{ and } D \in \mathbb{Z}$$

Hence, the quadratic twists of an elliptic curve $E : y^2 = 4x^n - 1$ where $n = 3, 4$ by infinitely many square-free integers D do not have non-trivial rational points. In particular, $E(K)$ is trivial, see Theorem 2.37.

Besides the base field $\mathbb{Q}$, we have the following results over a number field that can be found in [40].

Theorem 2.49. *[40] Let E/K be an elliptic curve. Then for all but finitely many quadratic twists E' of E, $E'(K)$ has no odd-order torsion.*

Theorem 2.50. *[40] Let K be a number field. There are elliptic curves E/K such that E has many twists E'/K with $E'(K) = 0$.*

Putting all of this together, one may naturally ask the following questions about quadratic twists of elliptic curves.

Question 2.51. *Can we find families of elliptic curves $E/\mathbb{Q}$ with rank 0 such that E_d has a positive rank for any square-free d?*

Question 2.52. *Can we find pairs of elliptic curves E and $\tilde{E}$ over a field K such that their quadratic twists by infinitely many square-free d satisfying one of the followings:*

$$i) \quad \text{rank}(E_d) = 0 \ \textit{and} \ \text{rank}(\tilde{E}_d) = 0$$

$$ii) \quad \text{rank}(E_d) = 0 \ \textit{and} \ \text{rank}(\tilde{E}_d) > 0$$

$$iii) \quad \text{rank}(E_d) > 0 \ \textit{and} \ \text{rank}(\tilde{E}_d) > 0$$

Obviously, Example 2.48 satisfies $i)$ as E_D has only the point at infinity for any $D \in \mathbb{Z} \setminus \{0\}$.

2.7 Isogeny of Elliptic Curves

Definition 2.53. *Let E_1 and E_2 be two elliptic curves defined over a number field K. A non-zero morphism ϕ from E_1 to E_2 such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is called an isogeny. If an isogeny exists between E_1 and E_2, then E_1 and E_2 are called isogenous.*

The fact that ϕ is either the constant map $\phi(E_1) = \{\mathcal{O}_{E_2}\}$ or, $\phi(E_1) = E_2$ is justified by Theorem 2.14. The set of all isogenies between two elliptic curves E_1 and E_2 form a group, denoted by $\text{Hom}(E_1, E_2)$ under the operation $+$ defined by $\phi_1 + \phi_2 : P \mapsto \phi_1(P) + \phi_2(P)$. In case of $E_1 = E_2$, it is also possible to compose isogenies such that $\phi_1 \circ \phi_2 : P \mapsto \phi_1(\phi_2(P))$ for all $\phi_1, \phi_2 \in \text{Hom}(E_1, E_2)$. Therefore, given an elliptic curve E, the set of all isogenies from E to itself, denoted by $\text{End}(E)$, forms a ring structure with two operations $+$ and $\circ$. Note that the composition is not necessarily commutative.

Example 2.54. *Let E_1 and E_2 be two elliptic curves over K. The trivial isogeny or constant isogeny $[0] \in \text{Hom}(\text{E}_1, \text{E}_2)$ is defined by $[0] : P \mapsto \mathcal{O}_{E_2}$ for all $P \in E_1$.*

Example 2.55. *Let E be an elliptic curve over a field K. For each $n \in \mathbb{Z}$, one can define an isogeny $[n] : E \to E \in \mathrm{End}(E)$ defined by*

$$[n](P) := \begin{cases} nP = P + \cdots + P & , \text{if } n > 0 \\ (-n)(-P) = (-P) + \cdots + (-P) & , \text{if } n < 0 \\ \mathcal{O} & , \text{if } n = 0 \end{cases}$$

If there exists $P \in E(K)$ such that P is not an n-torsion point, i.e., $nP \neq \mathcal{O}$. Then $[n]$ must be a surjective ring homomorphism of E by construction and Theorem 2.14. Thereof, the only constant isogeny of elliptic curves is the trivial isogeny. Altogether, there are two options for isogenies either all E map to $\mathcal{O}$ or it is surjective. One may see that $\mathbb{Z} \hookrightarrow \mathrm{End}(C)$ by the map $\varphi : n \mapsto [n]$. In the case of $\mathrm{char}(K) \neq 0$, mostly φ is not only an injective but also a surjective ring homomorphism. Hence, $\mathrm{End}(C) \cong \mathbb{Z}$. That is the curve C has no non-trivial automorphisms except the ones coming from only $\mathbb{Z}$ which means it is trivial.

Example 2.56. *[62] Consider the pairs of elliptic curves E_1 and E_2 over K of $\mathrm{char}(K) \neq 2$ defined by the following equations*

$$E_1 : y^2 = x(x^2 + Ax + B), \quad E_2 : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$$

There are two isogenies $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$ so that

$$\phi_1 : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(B - x^2)}{x^2} \right), \quad \phi_2 : (x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(R - x^2)}{8x^2} \right), \text{ where } R = A^2 - 4B.$$

Example 2.57. *[62] Let E/K be an elliptic curve described by the following equation*

$$E : y^2 = x^3 - x$$

Then $\mathrm{End}(C)$ includes an extra endomorphism $[i] : (x, y) \mapsto (-x, iy)$ as well as $[n]$ for all $n \in \mathbb{Z}$. It turns out that $\mathrm{End}(C) \cong \mathbb{Z}[i]$ by $a + bi \mapsto [a] + [i] \circ [b]$.

Like any algebraic structure, we can mention the isomorphism between elliptic curves. In case of an elliptic curve, there are some invariants that we can link to an elliptic curve. Two elliptic curves are isomorphic if the following three relations hold.

Proposition 2.58. *[62, p.45] Let E and E' be two elliptic curves defined over K whose algebraic closure is $\overline{K}$ with $\mathrm{char}\, K \neq 2, 3$. The elliptic curves E and E' are*

isomorphic over K, denoted by $E \cong E'$, if there exists $\mu \in K^*$ such that

$$\mu^4 c_4' = c_4, \quad \mu^6 c_6' = c_6, \quad \mu^{12}\Delta' = \Delta$$

where c_4, c_6 and Δ are defined in Definition 2.26.

Basically, an isogeny between elliptic curves is a special type and can be interpreted as a weaker version of isomorphism and not vice versa. Similarly, checking isogeny between two curves is more challenging than finding isomorphism as there are various types of isogeny that can be defined.

Recall that a set of all endomorphisms of an elliptic curve possess a ring structure. This indicates that some being units while others do not. The set of all invertible elements of $\mathrm{End}(C)$, $\mathrm{End}(C)^*$ is the automorphism group of C, denoted by $\mathrm{Aut}(C)$. The automorphisms of an elliptic curve are all classified by the j-invariant, no mysteries remain. The following table demonstrates the structure of automorphism, [62, Theorem 10.1].

Theorem 2.59. *Let E be an elliptic curve over K. The automorphism group* $\mathrm{Aut}(E)$ *is given by*

TABLE		
$\mathrm{char}\, K$	$j(E)$	$\lvert\mathrm{Aut}(E)\rvert$
No condition	$j(E) \neq 0, 1728$	2
$\mathrm{char}\, K \neq 2, 3$	$j(E) = 1728$	4
$\mathrm{char}\, K \neq 2, 3$	$j(E) = 0$	6
$\mathrm{char}\, K = 3$	$j(E) = 0 = 1728$	12
$\mathrm{char}\, K = 2$	$j(E) = 0 = 1728$	24

Table 2.1 The automorphism group of an elliptic curve over K

Moreover, it can be concluded that $\mathrm{Aut}(E)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $j(E) \neq 0, 1728$; $\mathbb{Z}/4\mathbb{Z}$ if $j(E) = 1728$, and $\mathbb{Z}/6\mathbb{Z}$ if $j(E) = 0$.

2.8 Hyperelliptic Curves

In this section, we overview facts about hyperelliptic curves based on the papers [41, 65]. Although there is much known about elliptic curves, that is not the case for hyperelliptic curves compared to elliptic curves. Hyperelliptic curves can be seen as a generalization of elliptic curves to higher genus. All genus 2 curves are hyperelliptic, but not all curves of larger genus are hyperelliptic. In case of genus 1, a hyperelliptic curve is an elliptic curve.

The genus of an algebraic curve acts as a tool to measure complexity of curves. There are several ways to define genus however this thesis focuses on the curves of the form $y^2 = f(x)$ where $f(x)$ is a polynomial of degree at least 3 without repeated factors. The genus of such curves can be obtained in the following way.

Definition 2.60. *Let $f(x)$ is polynomial with no repeated roots over K and the curve C is described by $C : y^2 = f(x) \in K[x]$. The genus of curve is given by*

$$\lfloor \frac{\deg(f) - 1}{2} \rfloor$$

Definition 2.61. *A hyperelliptic curve C is an algebraic curve of genus $g > 1$ over K described by an equation of the form*

$$C : \quad y^2 + p(x)y = q(x), \quad p(x), q(x) \in K[x]$$

such that $\deg(p) < g + 2$ and $q(x)$ is polynomial of degree $2g + 1$ or $2g + 2$ without multiple root over K.

Remark 2.62. *If C is a hyperelliptic curve as above with $\mathrm{char}(K) \neq 2$ then C can be described by an equation of the form*

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

We consider the two cases, when the degree of the polynomial f is odd or even. If the degree is odd then the projective form of the equation becomes

$$F(x, y, z) : \quad \mathcal{Y}^2 = (yz^k)^2 = y^2 z^{2k} = Ax^{2k+1} z + \cdots + Bz^{2k+2}$$

with assuming the existence of a constant term B. Hence, the curve always has a

rational point which is the point at infinity $\infty = (1:1:0)$. In case of even degree,

$$F(x,y,z): \quad \mathcal{Y}^2 = (yz^{k-1})^2 = y^2z^{2k-2} = Ax^{2k} + \cdots + Bz^{2k}$$

there are two points at infinity however these are most probably not rational. In particular, set $z = 0$ and $x = 1$ then there are two K-rational points if and only if the leading coefficient A is a square in K.

Although a lot of research has been done on the rank of elliptic curves and many techniques have been found to find it, there are still many unsolved questions on the rank. Unfortunately, this is not the case for the hyperelliptic curves. For a given hyperelliptic curve, it is well-known that a hyperelliptic curve possess only a finite number of points over any number field by Falting's Theorem.

Theorem 2.63. *[13, Faltings's Theorem] If C is a smooth projective curve over a number field K of genus $g \geq 2$, then there are only finitely many rational points on C.*

Mordell proposed this conjecture around 1910 and it was proved by Faltings in 1983.

One may also define quadratic twists of hyperelliptic curves in a similar way to elliptic curves and ask whether there is a rational point or not in the quadratic twists of a hyperelliptic curve.

Definition 2.64. *Let C/K be a hyperelliptic curve described by $C : y^2 = f(x)$. The quadratic twist of C by $d \in K\backslash K^2$ is given by*

$$C_d : dy^2 = f(x).$$

One may construct families of hyperelliptic curves with infinitely many quadratic twists that possess no rational points different from the points at infinity, see [56, 32, 46].

Example 2.65. *[46] There are infinitely many hyperelliptic curves C defined by*

$$C : Dy^2 = 4x^n - 1, \qquad \text{where } n \text{ is divisible by } 5, 7, 11 \text{ and } D \in \mathbb{Z}$$

have no rational point different from the points at infinity.

Note that a point $P = (x, y)$ on a hyperelliptic curve is called a Weierstrass point if P is invariant under the hyperelliptic involution i.e., x is a root of the defining polynomial of a hyperelliptic curve. As we will see in the following chapter, we produce examples of hyperelliptic curves with infinitely many quadratic twists possessing at

least two rational non-Weierstrass points. In addition, we give examples of families of quadruples of hyperelliptic curves, three of which are of the same genus, such that for infinitely many square-free rationals the quadratic twists of each of these hyperelliptic curves by these rationals possess at least one rational non-Weierstrass point.

The following questions may be asked about quadratic twists as well as elliptic curves. By a trivial point on a hyperelliptic curve, we mean a rational point that is different from the point at infinity and not a Weierstrass point.

Question 2.66. *Can we find a hyperelliptic curve C over $\mathbb{Q}$ with no rational points so that its quadratic twists C_d have a rational point for any square-free integer d?*

Question 2.67. *Is there a recipe for twisting simultaneously two different hyperelliptic curves infinitely many times so that they both have non-trivial rational points; or exactly one of the curves has non-trivial rational points; or neither of them has non-trivial rational points?*

Clearly, Example 2.65 fits in the third possibility of the Question 2.67 as they both do not have any rational point. On the other hand, hyperelliptic curves are chosen without restrictions, so one may add more conditions, such as whether one of them has a rational point or not.

The next proposition identifies when two hyperelliptic curves of the same genus are isomorphic.

Proposition 2.68. *[34] Let K be a field of char $K \neq 2$ and algebraic closure $\overline{K}$. Two hyperelliptic curves of genus $g \geq 2$ described by the following equations*

$$y^2 = f(x) \in K[x] \ \text{ and } \ y^2 = f'(x) \in K[x]$$

are isomorphic if and only if

$$x = \frac{ax+b}{cx+d}, \quad y = \frac{ey}{(cx+d)^{g+1}}, \ \text{ for some } \ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K) \text{ and } e \in K^*$$

In case of hyperelliptic curves of genus 2, one can attach a certain type of invariants, namely, Igusa invariants denoted by $I_2, I_4, I_6, I_8, I_{10}$. We refer the reader to see [24] and [33] for more details.

Let C be hyperelliptic curve of genus 2 defined by an equation $C : y^2 = f(x)$ where $f(x)$ is a sextic polynomial. Assume, moreover, that $f(x) = (x-\alpha_1)\dots(x-\alpha_6)$ in its splitting field of f, and $\alpha_1, \dots, \alpha_6$ are roots of f. Define the following sequence

of Igusa-Clebsch invariants:

$$
\begin{aligned}
I_2 &= c^2 \sum (\alpha_1-\alpha_2)^2 (\alpha_3-\alpha_4)^2 (\alpha_5-\alpha_6)^2 \\
I_4 &= c^4 \sum (\alpha_1-\alpha_2)^2 (\alpha_2-\alpha_3)^2 (\alpha_3-\alpha_1)^2 (\alpha_4-\alpha_5)^2 (\alpha_5-\alpha_6)^2 (\alpha_6-\alpha_4)^2 \\
I_6 &= c^6 \sum (\alpha_1-\alpha_2)^2 (\alpha_2-\alpha_3)^2 (\alpha_3-\alpha_1)^2 (\alpha_4-\alpha_5)^2 (\alpha_5-\alpha_6)^2 (\alpha_6-\alpha_4)^2 \\
&\qquad (\alpha_1-\alpha_4)^2 (\alpha_2-\alpha_5)^2 (\alpha_3-\alpha_6)^2 \\
I_{10} &= \Delta_f, \text{ where } \Delta_f \text{ denotes the discriminant of polynomial } f.
\end{aligned}
$$

Now, define the following sequence of Igusa invariants J_{2m}, $m = 1, 2, 3, 4, 5$.

$$
\begin{aligned}
J_2 &= I_2/8, \\
J_4 &= (4J_2^2 - I_4)/96, \\
J_6 &= (8J_2^3 - 160 J_2 J_4 - I_6)/576, \\
J_8 &= (J_2 J_6 - J_4^2)/4, \\
J_{10} &= I_{10}/4096.
\end{aligned}
$$

One may notice that even though a hyperelliptic curve of genus 2 might not be expressed by a sextic polynomial, f can be converted into a sextic by Proposition 2.68.

There is an alternative way to check isomorphism between hyperelliptic curves of genus 2 over $\overline{K}$ by comparing their Igusa invariants.

Proposition 2.69. *The genus 2 hyperelliptic curves C and C' over K are isomorphic over $\overline{K}$ if and only if there exists $\mu \in \overline{K}^*$ such that $J_{2m}(C) = \mu^{2m} J_{2m}(C')$.*

One can also mention the automorphism group of hyperelliptic curves. $\mathrm{Aut}(C)$ denotes the set of all isomorphisms between hyperelliptic curve C to itself and likewise it has a group structure similar to the case of elliptic curves. Basically, points map to points. In fact, this is not limited to just these two algebraic structures. In general, let C_g denotes the curve of genus g over K whose algebraic closure is $\overline{K}$. The set $\mathrm{Aut}(C_g)$ represents the set of all automorphisms of C_g. Moreover, in case of $\mathrm{char}(K) = 0$, $\mathrm{Aut}(C_g)$ is bounded by Riemann-Hurwitz formula. Indeed, it is well-known that $|\mathrm{Aut}(C_g)|$, $g \geq 2$ is finite in each characteristic, see [19].

Theorem 2.70. *[23, Riemann-Hurwitz] Let C_g be an algebraic curve of genus $g \geq 2$ over a field of characteristic 0. Then,*

$$|\mathrm{Aut}(C_g)| \leq 84(g-1)$$

Example 2.71. *Consider the curve hyperelliptic curve $C : y^2 = x^6 + x^3 + 1$ with its*

isomorphisms.

$$\tau_1 : (x, y) \mapsto (1/x, y/x^3), \quad \tau_2 : (x, y) \mapsto (\zeta_3 x, y)$$

where ζ_3 is cube root of unity. Basically, $(1/x, y/x^3)$ and $(\zeta_3 x, y)$ are points on C.

Example 2.72. *Let C be curve defined by $C : y^2 = x(x^4 + Ax^3 + Ax^2 + 1)$ then,*

$$\alpha : (x, y) \mapsto (1/x, y/x^3) \quad \beta : (x, y) \mapsto \left(-\frac{1}{x}, \frac{iy}{x^3}\right)$$

One can see that $\alpha\beta(x, y) \neq \beta\alpha(x, y)$. Later we will see $\mathrm{Jac}(C)$ decomposes into a square of an elliptic curve over $\mathbb{Q}(i)$ by Lemma 4.5.

Example 2.73. *Let C be a hyperelliptic curve defined by $C : y^2 = x^8 + Ax^4 + 1$. Then the automorphism group contains*

$$\alpha : (x, y) \mapsto (ix, y) \quad \beta : (x, y) \mapsto \left(-\frac{i}{x}, \frac{y}{x^4}\right)$$

Similarly, $\alpha\beta(x, y) = \left(\frac{i}{x}, \frac{y}{x^4}\right) \neq \beta\alpha(x, y) = \left(-\frac{i}{x}, \frac{y}{x^4}\right)$.

One may observe that a hyperelliptic curve C over K always admits a nontrivial automorphism called the hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$. This indicates that the automorphism group of a curve cannot be trivial. On the other hand, the involution $\sigma : (x, y) \mapsto (-x, y)$ is an automorphism on hyperelliptic curves defined by polynomials $p(x) \in K[x^2]$. Clearly, the automorphisms σ and ι are of order 2.

Points on hyperelliptic curves do not possess a natural group structure so the rank notion is inapplicable. However, it is still possible to define a variety associated to each curve with a natural group structure by the operation inherited from the divisor group of the curve, called the Jacobian variety.

Finally, we remark that the trivial endomorphism ring leads to a trivial automorphism ring and determining completely the automorphism group of any curve can be quite a demanding problem, however especially for genus 2 and 3, it may be more worthy to show that certain groups lie inside the automorphism group of a curve. We shall soon see that the decomposition behavior of Jacobian can be obtained by means of the automorphism groups of curves.

3. Abelian Varieties

Definition 3.1. *An algebraic variety V over K is defined in the following way*

$$V = \{P = (a_1, ..., a_n) : f_1(P) = \cdots = f_m(P) = 0\},$$

where $f_1, \ldots, f_m \in K[x_1, ..., x_n]$.

In other words, an algebraic variety is the zero set of a system of polynomials.

Definition 3.2. *An algebraic variety A over K with the specific point $\mathcal{O}$ in $A(K)$ having a binary operation φ and an inversion i*

$$\varphi : A \times A \to A, \quad i : A \to A$$

satisfying the following properties:

(1) $\varphi(S, \mathcal{O}) = \varphi(\mathcal{O}, S) = S$; *for all* $S \in A$,

(2) $\varphi(S, i(S)) = \mathcal{O}$; *for all* $S \in A$,

(3) $\varphi(\varphi(S,T), R) = \varphi(S, \varphi(T,R))$; *for all* $S, R, T \in A$.

$(A, \mathcal{O}, \varphi, i)$ is called an abelian variety.

In other words, A satisfies the axioms of a group and the group law is commutative, see [42]. In case of dimension 1, A is a non-singular projective curve, [61]. Hence, an abelian variety of dimension 1 is an elliptic curve. On the other hand, the set of all points of an abelian variety $A(K)$ forms a group, indeed a finitely generated abelian group.

Theorem 3.3. *[31, Mordell-Weil] Let A be an abelian variety over a number field K, the group $A(K)$ of K-rational points of A is a finitely generated abelian group over a number field.*

Mordell proved this theorem over $\mathbb{Q}$ and after that Weil extended it to number fields even for abelian varieties.

Definition 3.4. *A map ϕ between two abelian varieties $(A, \mathcal{O}_A, \varphi_A, i_A)$ and $(B, \mathcal{O}_B, \varphi_B, i_B)$ is called a morphism if the following condition holds for all $P, Q \in A$.*

$$\phi(P \varphi_A Q) = \phi(P) \varphi_B \phi(Q)$$

with $\phi(\mathcal{O}_A) = \mathcal{O}_B$.

Definition 3.5. *Let A and B be two abelian varieties over a field K. An isogeny $\phi : A \to B$ is a surjective morphism with a finite kernel.*

In case of $A = B$, the set of all isogenies of an abelian variety A forms a ring similar to the situation of elliptic curves, denoted by $\mathrm{End}(A) = \{\phi^{\mathrm{isogeny}} : A \to A\}$.

An abelian variety A defined over K is called simple if there are no lower dimensional abelian varieties B and C over K such that A is isogenous to the product $B \times C$, otherwise it is called decomposable or split. If A is simple over $\overline{K}$, then it is called absolutely simple. As we will see, the endomorphism ring of an abelian variety will assist to examine decomposition of the Jacobian of hyperelliptic curves together with useful propositions.

3.1 Jacobian Varieties of Hyperelliptic Curves

As previously mentioned, hyperelliptic curves do not possess a natural group structure however we can define the Jacobian variety associated with it. Although there are several equivalent ways to define the Jacobian, we consider the following series of definitions to be most practical. Now, we collect necessary fundamentals of algebraic curves to introduce the Jacobian variety.

Definition 3.1.1. *Let $C = V(F) \subseteq \mathbb{P}^2$ be a smooth curve over a field K. A divisor on C is a formal sum*

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

where $n_P \in \mathbb{Z}$ and n_P's are non-zero for only finitely many $P \in C$.

In other words, divisors on C can be described by formal $\mathbb{Z}$-linear combination of points in $C(K)$. The degree of the divisor D is defined by

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

In general, we denote $\mathrm{Div}^n(C) = \{D^{\text{divisor}} : \deg(D) = n\}$. The divisors of C form a free abelian group generated by points on curves under the addition denoted by $\mathrm{Div}(C)$. Hence, the degree 0 divisors, $\mathrm{Div}^0(C)$ is a subgroup of $\mathrm{Div}(C)$. For example, if P, Q and R are points in C then $P-Q, P+Q-2R, -P+2Q+-R \in \mathrm{Div}^0(C)$.

A partial ordering on $\mathrm{Div}(C)$ can be defined by $D_1 \geq D_2$ if $D_1 - D_2$ has only positive coefficients for $D_1, D_2 \in \mathrm{Div}(C)$.

Let $f \in K(C)$, we say $\mathrm{ord}_P(f) > 0$ if P is a zero of f and $\mathrm{ord}_P(f) < 0$ if P is a pole of f.

Definition 3.6. *A principal divisor of $f \in \overline{K}(C)^*$ is defined by*

$$(f) = \sum \mathrm{ord}_P(f) \cdot P$$

Equivalently, a principal divisor f can be expressed in terms of zeros and poles as follows:

$$(f) = (f)_0 - (f)_\infty \text{ where}$$

$$(f)_0 = \sum_{\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f) \cdot P, \text{ and } (f)_\infty = \sum_{\mathrm{ord}_P(f)<0} -\mathrm{ord}_P(f) \cdot P$$

$(f)_0$ and $(f)_\infty$ are called zero and pole divisor, respectively.

One may define equivalence relation on $\mathrm{Div}(C)$ in the following way:

Definition 3.1.2. *An equivalence relation exists between divisors, defined as*

$$D \sim D' \iff D - D' \text{ is principal.}$$

$$\iff D - D' = (f),\ f \in \overline{K}(C)^*$$

The set of all principal divisors of C is denoted by $\mathrm{Princ}(C)$. It is known that every rational function on a curve has the same number of zeros and poles [64, Theorem 1.4.11]. That means that every principal divisor has degree 0. It turns out that $\mathrm{Princ}(C)$ is the group of divisors that are linearly equivalent to zero. Hence, $\mathrm{Princ}(C) \subset \mathrm{Div}^0(C)$.

Definition 3.1.3. *The Picard group of C denoted by $\mathrm{Pic}(C)$ is defined by the following quotient*

$$\mathrm{Pic}(C) := \mathrm{Div}(C)/\mathrm{Princ}(C)$$

and

$$\mathrm{Jac}(C) := \mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Princ}(C)$$

Basically, an element $[D] \in \mathrm{Pic}(C)$ is of the form $[D] = D + \mathrm{Princ}(C)$ for $D \in \mathrm{Div}(C)$. On the other hand, $\mathrm{Pic}^0(C)$ forms naturally a subgroup of $\mathrm{Pic}(C)$.

In particular, the Jacobian of curve C can be interpreted as the linear equivalence classes of degree zero divisors. Therefore, Jac(C) can also be expressed by

$$\mathrm{Jac}(C) = \mathrm{Div}^0(C)/\sim .$$

It is clear that $\mathrm{Jac}(C)$ does not only have an abelian group structure due to the divisor group but also has the structure of a variety, see [19]. Moreover, if C is a curve of genus g over a field K then its Jacobian is also defined over the field K with dimension g, see [42, Prop 2.1, p. 91]. In case of an elliptic curve, as we mentioned, its Jacobian and an elliptic curve itself are the same up to isomorphism. Explanation is provided below and we refer the reader to [8] for more details about abelian varieties.

Definition 3.7. *Let C/K be a non-singular genus one curve defined by a quartic polynomial*

$$C : y^2 = f(x) = ax^4 + bx^3 + cx^2 + dx + e, \qquad a, b, c, d, e \in K.$$

Then the Jacobian of C is described by

$$\mathrm{Jac}(C) = E_{I,J} : y^2 = \tilde{F}(X) = X^3 - 27IX - 27J,$$

where I and J are given as follows:

$$I = 12ae - 3bd + c^2 \ \text{ and } \ J = 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3.$$

Moreover, the point $(X, Y) = \left(\dfrac{9b^2 - 24ac}{4a}, \dfrac{27(b^3 + a^2d - 4abc)}{(4a)^{3/2}} \right)$ *lies in* $\mathrm{Jac}(C)$.

In particular, if C is a non-singular genus 1 curve with a point, then C is an elliptic curve, see [62]. Therefore, C has a Weierstrass equation by Definition 2.26. Note that $\mathrm{Jac}(C)$ enjoys the same argument thanks to the following two propositions. In particular, the first proposition states when a curve defined by a quartic polynomial has a rational point and the second proposition indicates that C is isomorphic to $E_{I,J}$.

Proposition 3.8. *[8] The curve C has a K-rational point if and only if there is a quartic polynomial $g(x)$ with the square leading coefficient equivalent to $f(x)$.*

Proposition 3.9. *[8] Let C/K be genus 1 curve defined by a quartic polynomial*

with a point then there is a birational map ξ of degree 4 described by

$$\xi : C \to E_{I,J} \text{ such that } \xi : [x : y : z] \to [6yzg_4(x,y) : 26g_6(x,z) : (2yz)^3] \text{ where}$$

$$\begin{aligned} g_4(X,Y) &= (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3Y + 2(2c^2 - 24ae - 3bd)X^2Y^2 + 4(cd - 6be)XY^3 \\ &\quad + (3d^2 - 8ce)Y^4, \\ g_6(X,Y) &= (b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y + 5(8abe + b^2d - 4acd)X^4Y^2 \\ &\quad + 20(b^2e - ad^2)X^3Y^3 - 5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 \\ &\quad - (d^3 + 8be^2 - 4cde)Y^6. \end{aligned}$$

Let $J(K)$ represents the set of K-rational points of Jac(C). As an immediate consequence of Theorem 2.3, one can obtain that $J(K)$ is a finitely generated abelian group. Moreover, we can state the following corollary by the Fundamental Theorem of Finitely Generated Abelian groups as in the case of abelian varieties.

Corollary 3.10. *[65] Let C be a curve defined over a number field K. $J(K)$ can be expressed as*

$$\mathbb{Z}^r \times J(K)_{tors}$$

where $r \in \mathbb{Z}^{\geq 0}$ is the rank of $J(K)$ and $J(K)_{tors}$ is the finite torsion subgroup of $J(K)$.

It is natural to expect that Jacobian varieties may decompose into the product of varieties of smaller dimensions. A huge advantage of an automorphism group is that it enables us to practically examine the Jacobian's behavior, simply the Jacobian decomposes or not even if you could not determine full automorphism group of a curve. Jacobian varieties of algebraic curves with many automorphisms provide examples of abelian varieties that contain many factors in their decompositions. In order to see such curves whose Jacobian decompose into a product of many elliptic factors, see [51, 52, 53].

4. Families of Decomposable Abelian Varieties

Given that the automorphism group of a smooth algebraic curve C is non-trivial, we may obtain new curves from C by taking the quotient of C by a non-trivial subgroup of its automorphism group. The existence of such a curve is guaranteed by the following theorem. Therefore, we may discuss the genus of such curves.

Theorem 4.1. *[43] Let C be an algebraic curve with finite non-trivial subgroup of its automorphism group G then C/G is an algebraic curve.*

We write genus(C) for the genus of C.

Theorem 4.2. *[58, 62, Riemann-Hurwitz Formula] Let C be an algebraic curve of genus g having a finite automorphism group G with $\Omega : C \to C/G$. Then,*

$$2g-2 = \deg(\Omega)(2\,\text{genus}(C/G)-2) + \sum_{P\in C} e_P - 1 \ ,$$

where e_P is the ramification index.

It follows directly that $g \geq g'$ where g' is genus(C/G).

Consider the group generated by an automorphism σ having only two elements, σ and the identity. Basically, the quotient $C/\langle\sigma\rangle$ refers to the fact that any elements that have the same image under σ will be identified. That is, $C/\langle\sigma\rangle$ is a curve fixed by σ.

Lemma 4.3. *[3] Let C be a hyperelliptic curve of genus 2 with non-trivial subgroup $\mathcal{W}$ of* Aut(C)*. Then, the genus of the quotient is 1 if $\mathcal{W}$ is order 2, otherwise it is 0.*

In other words, a quotient curve of C becomes a genus 1 curve if C is a genus 2 hyperelliptic curve with $\mathcal{W}$ a subgroup of Aut(C) of order 2.

An abelian variety A defined over K is called *simple* if there are no lower dimensional abelian varieties B and C over K such that A is isogenous to the product $B \times C$, otherwise it is called *decomposable*. If A is simple over $\overline{K}$, then it is called *absolutely*

simple.

The study of decomposable Jacobian varieties of genus two curves was initiated in [20], see also [29].

The following theorem assists to decompose Jacobian varieties if possible.

Theorem 4.4. *[26, 59] Let C be a curve of genus g with the automorphism group* $\mathrm{Aut}(C)$*. Let $H \leq \mathrm{Aut}(C)$ such that*

$$H = \bigcup_{i=1}^{r} H_i \text{ so that } H_i \cap H_j = \{1\} \text{ for all } i \neq j \text{ and each } H_i \leq H.$$

Then, the following relation holds

$$\mathrm{Jac}^{\,r-1}(C) \times \mathrm{Jac}^{\,|H|}(C/H) \cong \mathrm{Jac}^{\,|H_1|}(C/H_1) \times \cdots \times \mathrm{Jac}^{\,|H_r|}(C/H_r).$$

In other words, a succinct way of describing a decomposition of the Jacobian variety of a hyperelliptic curve is observing its automorphism group.

In particular, the Jacobian of a genus 2 hyperelliptic curve having non-trivial automorphisms decompose into either a product of two distinct elliptic curves; or a square of an elliptic curve, otherwise it is simple. Moreover, the Jacobian of a genus 3 hyperelliptic curves having non-trivial automorphisms decompose into either a cube of an elliptic curve; or a product of a square of an elliptic curve E and an elliptic curve that is not isogenous to E; or the product of three non-isogenous elliptic curves; or a product of an elliptic curve and an abelian variety of dimension 2, otherwise it is simple.

Furthermore, we have the following result over $\overline{\mathbb{Q}}$.

Lemma 4.5. *[3] Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus 2 with a non-commutative* $\mathrm{Aut}(C)$*. Then,* $\mathrm{Jac}(C) \simeq E^2$ *over* $\overline{\mathbb{Q}}$*.*

From here on, all facts are referenced with modified notations. A family of hyperelliptic curves of arbitrary genus whose Jacobians decompose into two abelian varieties was given in [10]. Namely,

Example 4.6. *[10] Consider the Jacobian* $\mathrm{Jac}(X)$ *of the hyperelliptic curve defined by an equation*

$$X : y^2 = (x^n - 1)(x^n - t), \quad n = 2k+1, \quad k > 1, \quad t \in \mathbb{C} \setminus \{0, 1\}.$$

There are two algebraic curves Y_1 and Y_2 of genus k such that $\mathrm{Jac}(X)$ *is isomorphic*

to $\mathrm{Jac}(Y_1) \times \mathrm{Jac}(Y_2)$.

Ekedahl and Serre constructed examples of curves whose Jacobians decompose completely into elliptic curves, see [11]. The reader may also see [47] for examples of three non-hyperelliptic curves whose the Jacobian variety is isogenous to a product of elliptic curves.

A family of genus 3 and 5 hyperelliptic curves over a number field K whose Jacobians decompose into a product of elliptic curves was given in [67]. Explicitly,

Example 4.7. *The genus* 3 *hyperelliptic curve* C *given by the equation*

$$C : y^2 = (x^4 + ax^2 + 1)(x^4 + bx^2 + 1)$$

decomposes into a product of an elliptic curve Γ_1 *and the Jacobian of a genus two curve,* Γ_2*. Namely,*

$$\begin{aligned} \Gamma_1 : y^2 &= (x^2 - 2 + a_1)(x^2 - 2 + a_2), \\ \Gamma_2 : y^2 &= (x^2 - 4)(x^2 - 2 + a_1)(x^2 - 2 + a_2) \end{aligned}$$

where $C \to \Gamma_1$ *is defined by* $(x, y) \mapsto \left(x + \frac{1}{x}, \frac{y}{x^2}\right)$ *and* $C \to \Gamma_2$ *is defined by* $(x, y) \mapsto \left(x + \frac{1}{x}, \left(x - \frac{1}{x}\right)\frac{y}{x^2}\right)$*. Therefore,* $\mathrm{Jac}(C) \simeq \mathrm{Jac}(\Gamma_1) \times \mathrm{Jac}(\Gamma_2)$.

In addition, Γ_2 *admits a non-hyperelliptic involution* $\sigma : (x, y) \mapsto (-x, y)$*. It turns out that, the quotient curve* $\Gamma_2/\langle\sigma\rangle$ *corresponds to an elliptic curve. Hence,* $\mathrm{Jac}(C) \simeq E_1 \times E_2 \times E_3$ *where* E_i*'s are not necessarily isogenous elliptic curves.*

On the other hand, there exists an elliptic curve C_1 covered by C defined by an equation

$$C_1 : y^2 = (x^2 + ax + 1)(x^2 + bx + 1), \qquad (x, y) \mapsto (x^2, y).$$

In particular, C has two automorphisms σ and $\zeta : \left(\frac{1}{x}, \frac{y}{x^4}\right)$. One may easily see that $C/\langle\iota\rangle \cong \Gamma_1$, $C/\langle\zeta\rangle \cong C_1$ and $\Gamma_1 \ncong C_1$ while they can be isogenous. On the other hand, it is given that the automorphism group of the curve C is $D_4 \times C_2$, see [18, 54]. This implies that the elliptic curves are not isogenous over $\overline{K}$.

Example 4.8. *The genus* 5 *hyperelliptic curve* $\tilde{C}$ *defined by an equation*

$$\tilde{C} : y^2 = (x^4 + ax^2 + 1)(x^4 + bx^2 + 1)(x^4 + cx^2 + 1)$$

has decomposable Jacobian. Namely, $\mathrm{Jac}(\tilde{C}) \simeq \mathrm{Jac}(\tilde{\Gamma_1}) \times \mathrm{Jac}(\tilde{\Gamma_2})$ *where* $\tilde{\Gamma_1}$ *and* $\tilde{\Gamma_2}$

are two curves covered by $\tilde{C}$ given by

$$\tilde{\Gamma_1} : y^2 = (x^2-2+a)(x^2-2+b)(x^2-2+c), \qquad (x,y) \mapsto \left(x+\frac{1}{x}, \frac{y}{x^3}\right),$$
$$\tilde{\Gamma_2} : y^2 = (x^2-4)(x^2-2+a_1)(x^2-2+a_2)(x^2-2+a_3), \qquad (x,y) \mapsto \left(x+\frac{1}{x}, \left(x-\frac{1}{x}\right)\frac{y}{x^3}\right).$$

One can see that $\tilde{\Gamma_i}$'s admit automorphisms $(\pm x, \pm y)$. As a consequence, the Jacobian of $\tilde{C}$ decomposes into a product of elliptic curves.

In particular, a genus 2 curve given by the following equation

$$\tilde{F} : y^2 = x(x-1)\left(x-\frac{2-a}{4}\right)\left(x-\frac{2-b}{4}\right)\left(x-\frac{2-c}{4}\right)$$

is covered by $\tilde{\Gamma}_2$ i.e., the Jacobian of $\tilde{\Gamma}_2$ decomposes into an elliptic curve and $\tilde{F}$. Note that, moreover, $\tilde{F}$ is decomposable.

Families of genus 2 hyperelliptic curves whose Jacobian decompose into a square of elliptic curves over an extension of perfect field K with $\mathrm{char}(K) \neq 2,3$ are studied in [17]. In the next two examples, consider K to be a perfect field with $\mathrm{char}(K) \neq 2,3$.

Example 4.9. *[17] The genus 2 hyperelliptic curve over the field K described by the equation*

$$C : y^2 = x^5 + ax^3 + bx$$

has decomposable Jacobian such that $\mathrm{Jac}(C)$ is isogenous to the square of an elliptic curve E over $K(b^{1/8}, i)$ where E is an elliptic curve defined over $K(b^{1/2})$ by

$$E : y^2 = (c+2)x^3 - (3c-10)x^2 + (3c-10)x - (c+2)$$

where $c = a/\sqrt{b}$ and $i \in \overline{K}$ is a primitive fourth root of unity.

In particular, in case of $K = \mathbb{Q}$, the isogeny exists over the number field $\mathbb{Q}(i)$ if b is chosen to be a power of eight.

Example 4.10. *[17] The genus 2 hyperelliptic curve over the field K defined by the equation*

$$C' : y^2 = x^6 + ax^3 + b$$

has decomposable Jacobian such that $\mathrm{Jac}(C')$ is isogenous to the square of an elliptic curve E' over $K(b^{1/6}, \zeta_3)$ where E is an elliptic curve defined over $K(b^{1/2})$ by

$$E' : y^2 = (c+2)x^3 - (3c-30)x^2 + (3c+30)x - (c-2)$$

where $c = a/\sqrt{b} \in \overline{K}$ and $\zeta_3 \in \overline{K}$ be a primitive third root of unity. In particular, if

$K = \mathbb{Q}$ then the isogeny exists over $\mathbb{Q}(\zeta_3)$ if b is sixth power.

On the other hand, in case of a field of $\mathrm{char}(K) > 2$, the following is established in [22].

Theorem 4.11. *[22] Let K be field of $\mathrm{char}(K) > 2$ and E/K be an elliptic curve having $j(E) \neq 0, 1728$. Then there exists a genus 2 curve C such that $\mathrm{Jac}(C) \simeq E^2$ over K.*

Algebraic curves with many automorphisms allow their Jacobian varieties to be decomposed into abelian varieties containing many factors in their decompositions. Such curves whose Jacobians contain many elliptic factors were shown in [51, 52, 53]. On the other hand, the existence of Jacobians that are isogenous to the product of not necessarily isogenous arbitrary many Jacobians of the same genus are studied in [4].

Altogether, the following series of questions may be proposed.

Question 4.12. *Can we find a family of hyperelliptic curve of genus g whose jacobian decomposes for all $g \geq 2$?*

Question 4.13. *How far can we go to construct families of curves of higher genus whose Jacobian decomposes into a product of only elliptic curves?*

We answered positively Question 4.12 over a number field in the following chapter and J. Paulhos posed related questions as follows.

Question 4.14. *For which genus g, is it possible to construct a curve C whose $\mathrm{Jac}(C) \simeq E^g$ where E is an elliptic curve?*

Question 4.15. *What is the maximum number t so that the Jacobian decomposition of a curve C contains t-many elliptic curves for fixed genus g? That is,*

$$\mathrm{Jac}(C) \simeq E^t \times A_{g-t}$$

where A_{g-t} is an abelian variety of dimension $g-t$.

Paulhos was the first who provided the following example for Question 4.14 over a number field when $g = 5$, see [52] for more details.

Example 4.16. *[52] C be a hyperelliptic curve given by the equation*

$$C : y^2 = x(x^{10} + 11x^5 - 1).$$

has decomposable Jacobian such that $\mathrm{Jac}(C) \simeq E^5$ over a number field where E is

an elliptic curve given by

$$E : y^2 = x(x^2 + 11x - 1).$$

In [51], Paulhos classified the splitting behavior of some genus 2 and 3 curves by examining its automorphism group. We write C_n, D_n, S_n, U_n, V_n and H_n for the cyclic group with n elements, the dihedral group with n elements, symmetric group of order $n!$ and the rest is defined by the following relations

$$U_n = \langle a, b \mid a^2, b^{2n}, abab^{n+1} \rangle, \quad V_n = \langle a, b \mid a^4, b^n, (ab)^2, (a^{-1}b)^2 \rangle, \quad H_n = \langle a, b \mid a^2, b^2a^2, (ab)^n \rangle.$$

Proposition 4.17. *[51] If C is a curve of genus 3 or 4 over an algebraically closed field K with $\operatorname{char} K = 0$ having an automorphism group containing one of the groups given below, then the corresponding Jacobian decomposition is given in the following table where E_i's are elliptic curves, whereas A_i's are abelian varieties of dimension 2.*

Genus 3

$\mathrm{Aut}(C)$	$\mathrm{Jac}(C)$
$C_2 \times C_2$	$E \times A_2$
$D_4 \times C_2$	$E_1 \times E_2 \times E_3$
H_2	$E_1 \times E_2^2$
U_2	$E_1 \times E_2$
D_{12}	$E_1^2 \times E_2$
$D_8 \times C_2$	$E_1^2 \times E_2$
U_6	$E_1^2 \times E_2$
V_8	$E_1^2 \times E_2$
$S_4 \times C_2$	E^3

Genus 4

$\mathrm{Aut}(C)$	$\mathrm{Jac}(C)$
$C_2 \times C_2$	$A_1 \times A_2$
$V_2 \cong D_8$	A_2^2
D_8	A_2^2
D_{16}	A_2^2
$D_{10} \times C_2$	$E_1^2 \times E_2$
U_8	A_2^2
V_{10}	A_2^2

Table 4.1 Splitting behavior of genus 3 and 4 hyperelliptic curves.

We do not have data for larger genus as we had for genus 3 and 4. Moreover, afterwards, the genus 3 hyperelliptic curve and smooth planar quartic curves were examined by Shaska in [59].

Theorem 4.18. *[59] Let C be a genus 3 curve then the following statements holds:*

i) If $\mathrm{Aut}(C)$ is isomorphic to V_4 or $C_2 \times C_4$ then $\mathrm{Jac}(C) \simeq E \times A_2$

ii) If $\mathrm{Aut}(C)$ is isomorphic to $C_2 \times C_2 \times C_2$ then $\mathrm{Jac}(C) \simeq E_1 \times E_2 \times E_3$.

iii) If $\mathrm{Aut}(C)$ is isomorphic to D_{12}, $C_2 \times S_4$ or group of order 24, 32 then $\mathrm{Jac}(C) \simeq E_1^2 \times E_2$.

The author attempted the following problem up to genus 4. However, there are still many gaps in our data. We collect the list of hyperelliptic curves even when we were not able to find a family for some cases. In fact, it is extremely difficult to find a decomposition over a base field K, since all known classifications are over $\overline{K}$.

Question 4.19. *Can we construct a list of hyperelliptic curves for a fixed genus g having each possible splitting type in the Jacobian decomposition?*

We need the following remark in order to produce families of hyperelliptic curves whose Jacobian cannot be decomposed further together with Theorem 5.3.

Remark 4.20. *Let K be a number field and $f_t(X) = a_n(t)X^n + a_{n-1}(t)X^{n-1} + \cdots + a_0(t) \in K(T)$. If $\mathrm{Gal}(f_{t_0}(X)) = S_n$ for some $t = t_0 \in K$, then there are infinitely many such t_0 for which $\mathrm{Gal}(f_{t_0}(X)) = S_n$ by Hilbert irreducibility theorem.*

We derive the list which one can add much more examples over $\overline{K}$. We refer the reader to see [1, 36, 49, 52, 59] for more details and examples. The table for the case of $g = 2$ and 3 are given below.

GENUS 2	
Curve C	$\mathrm{Jac}(C)$
$y^2 = ax^6 + bx^4 + bx^2 + a$	E^2
$y^2 = ax^6 + bx^4 + cx^2 + d$	$E_1 \times E_2$
$y^2 = x^4 + ax^3 + bx^2 + cx + d$	A_2

Table 4.2 Possible list of examples having different decomposition types for genus 2

GENUS 3	
Curve C	$\mathrm{Jac}(C)$
$y^2 = x^8 + 14x^4 + 1$	E^3
$y^2 = x^8 + ax^4 + 1$	$E_1^2 \times E_2$
$y^2 = x^8 + ax^6 + bx^4 + ax^2 + 1$	$E_1 \times E_2 \times E_3$
$y^2 = x^8 + ax^6 + bx^4 + cx^2 + 1$	$E \times A_2$
$y^2 = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$	A_3

Table 4.3 Possible list of examples having different decomposition types for genus 3

On the other hand, obtaining elliptic curves in the decomposition of the Jacobian is getting more complicated when the genus becomes larger. For example, we do not have even one single example of a hyperelliptic curve C with a decomposition $\mathrm{Jac}(C) \simeq E^4$. Theoretically, however, if one finds a curve with the automorphism group $(C_3 \times C_3) \rtimes D_8$ then the result is concluded, see [54]. Hence, the list of examples of possible different decompositions for the genus 4 is given in the following table.

GENUS 4	
Curve C	$\mathrm{Jac}(C)$
$y^2 = x(x^4-1)(x^4+2\sqrt{-3}x^2+1)$	$E_1^2 \times E_2^2$
$y^2 = x^{10}+a_1x^8+a_2x^6+a_3x^4+a_4x^2+1$	$A_1 \times A_2$
$y^2 = x^9+1$	$E \times A_3$
$y^2 = x(x^8+ax^4+1)$	A_2^2
$y^2 = x(x^8+ax^7+bx^6+cx^5+dx^4+ex^3+fx^2+gx+1)$	A_4

Table 4.4 Possible list of examples having different decomposition types for genus 4

5. Hyperelliptic Curves With Non-trivial Automorphisms

This chapter contains new materials that were obtained during the thesis.

Throughout this section K is a field with $\operatorname{char} K = 0$ whose algebraic closure is $\overline{K}$.

In this thesis, one of the families we are concerned about is $y^2 = f(x)$ where $f(x)$ is a palindromic polynomial with no multiple roots in $K[x]$.

Definition 5.1. *A polynomial $f(x) \in K[x]$ is said to be* palindromic *if*

$$f(x) = x^d f(1/x)$$

where $d = \deg f$, i.e., if $f(x) = \sum_{i=0}^{d} a_i x^i$, then $a_i = a_{d-i}$ for $0 \leq i \leq d$.

We write C_2, V_4, and D_4 for the cyclic group with 2 elements, the Klein-4 group, and the dihedral group with 8 elements, respectively.

Proposition 5.2. *Let $f(x) \in K[x]$ be an even palindromic polynomial of degree $2g+2$ with no multiple roots.*

i) If $C : y^2 = f(x)$, then $D_4 \hookrightarrow \operatorname{Aut}(C)$, when g is even.

ii) If $C : y^2 = f(x)$, then $C_2 \times C_2 \times C_2 \hookrightarrow \operatorname{Aut}(C)$, when g is odd.

iii) If $C' : y^2 = xf(x)$, then $V_4 \hookrightarrow \operatorname{Aut}(C')$.

Proof. We write $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0$, where $a_{2i} = a_{2g+2-2i}$, $0 \leq i \leq g+1$. For i) and ii) apart from the hyperelliptic involution, the curve C has the following automorphisms of order 2

$$\sigma : (x, y) \mapsto (-x, y) \qquad \text{and} \qquad \tau : (x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right).$$

We note that $\sigma^2 = \tau^2$. Moreover, $(\sigma \circ \tau)^2 = \iota$ when g is even. It follows that the group generated by σ and τ is isomorphic to the dihedral group D_4. Specifically, if we fix a representation $D_4 := \langle a, b \mid a^2 = b^2 = (ab)^4 = 1 \rangle$, then we have the following

inclusion

$$D_4 \hookrightarrow \mathrm{Aut}(C); \qquad a \mapsto \sigma, \quad b \mapsto \tau.$$

ii) follows in a similar fashion by observing that

$$(\sigma \circ \tau)^2(x,y) = (\sigma \circ \tau)\left(-\frac{1}{x}, \frac{y}{x^{g+1}}\right) = \left(-\frac{1}{-1/x}, \frac{y/x^{g+1}}{(-1/x)^{g+1}}\right) = (x,y)$$

Furthermore, automorphisms σ, τ, ι and their composition form a group and are all of order 2 when g is odd. Note that the compositions are commutative.

For *iii*) one my check that the map

$$\sigma : C' \to C' : \qquad (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+2}}\right)$$

is an automorphism of C', see Proposition 2.68, of order 2. The automorhisms ι, σ, $\sigma \circ \iota$, 1 form a subgroup of $\mathrm{Aut}(C')$ isomorphic to the Klein 4-group, V_4. □

Given a hyperelliptic curve, one would like to know whether its Jacobian is simple or not. The following results of Zarhin introduce simplicity criteria for certain hyperelliptic Jacobian varieties based on the Galois group of the defining polynomial.

Theorem 5.3. *Let C be a hyperelliptic curve defined by the equation $y^2 = f(x)$, where $\deg(f) = n$ and $f(x)$ is polynomial without multiple roots in $K[x]$.*

i) Assume $n \geq 5$. If $\mathrm{Gal}(f)$ is either the full symmetric group S_n or the alternating group A_n, then $\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}$. In particular, $\mathrm{Jac}(C)$ is an absolutely simple abelian variety, see [68].

ii) Assume $n \geq 6$ is even. If $f(x) = (x-t)h(x)$ with $t \in K$ and $h(x) \in K[x]$, is such that $\mathrm{Gal}(h)$ is either S_{n-1} or A_{n-1}, then $\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}$. In particular, $\mathrm{Jac}(C)$ is an absolutely simple abelian variety, see [69].

iii) Assume $n \geq 9$ is odd. If $f(x) = (x-t)h(x)$ with $t \in K$ and $h(x) \in K[x]$, is such that $\mathrm{Gal}(h)$ is either S_{n-1} or A_{n-1}, then $\mathrm{Jac}(C)$ is an absolutely simple abelian variety, see [69].

In other words, $\mathrm{Jac}(C)$ with a trivial endomorphism ring cannot be decomposed further. Therefore, as an immediate consequence of Theorem 5.3, in order to generate an absolutely simple Jacobian variety for any genus g, one simply needs to pick a polynomial $f(x)$ of degree n whose the Galois group is S_n or A_n where $n = 2g+1$.

The following result, [12, Theorem 8] introduces a method to construct absolutely simple varieties over number fields.

Proposition 5.4. *Let K be a number field. Let $g \geq 1$ be an integer, and let $f \in K[x]$ be a polynomial of degree $2g$ with no multiple roots. Consider the hyperelliptic curve of genus g over $K(T)$ defined by $C_T : y^2 = f(x)(x-T)$. Then there are only finitely many $t \in K$ such that the Jacobian of C_t is not absolutely simple.*

Proposition 5.5. *Let $f(x) \in K[x]$ be of degree n such that $\mathrm{Gal}_K(f) = S_n$ or A_n. Let C_f, E_f and H_f be as in Proposition 5.10.*

If $n = 2g+1 \geq 5$, then $\mathrm{Jac}(C_f) \simeq \mathrm{Jac}(E_f) \times \mathrm{Jac}(H_f)$, where both $\mathrm{Jac}(E_f)$ and $\mathrm{Jac}(H_f)$ are absolutely simple of dimension g.

If $n = 2g+2 \geq 8$, then $\mathrm{Jac}(C_f) \simeq \mathrm{Jac}(E_f) \times \mathrm{Jac}(H_f)$, where both $\mathrm{Jac}(E_f)$ and $\mathrm{Jac}(H_f)$ are absolutely simple of dimension g and $g+1$ respectively.

Proof. The statement follows from the combination of Proposition 5.10 with Theorem 5.3. □

In particular, one can simply construct an absolutely simple Jacobian variety or the triples as in Proposition 5.5 by the following lemma and series of examples.

Lemma 5.6. *[50, Osada] Let $f(x)$ be a monic and irreducible polynomial of degree n with square-free discriminant then, $\mathrm{Gal}_{\mathbb{Q}} f(x) = S_n$.*

Example 5.7. *[50, Osada] The polynomial $f(x) = x^n - x - 1 \in \mathbb{Q}[x]$ has Galois group S_n for all $n \geq 2$.*

Example 5.8. *[48, 50, Nart-Vila, Osada] If the polynomial $f(x) = x^n + x + a$ is irreducible with $(n-1, a) = 1$, then the $\mathrm{Gal}_{\mathbb{Q}} f(x) = S_n$.*

On the other hand, for any integer $n \geq 7$, there exists infinitely many polynomials $f(x)$ with the property that $\mathrm{Gal}_{\mathbb{Q}} f(x) = A_n$, see [21].

We particularly pay attention to a decomposition into two abelian subvarieties.

Remark 5.9. *Let C be a hyperelliptic curve over K with hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$ giving rise to the morphism $C \to C/\langle \iota \rangle \cong \mathbb{P}^1$. We assume that C possesses an automorphism σ of order 2 such that $\sigma \neq \iota$. We set $\tau = \sigma \circ \iota$. Writing C_σ and C_τ for $C/\langle \sigma \rangle$ and $C/\langle \tau \rangle$ respectively, we obtain the quotient morphisms $\phi_\sigma : C \to C_\sigma$ and $\phi_\tau : C \to C_\tau$ respectively. This yields a morphism $\phi = (\phi_\sigma, \phi_\tau) :$*

$C \to C_\sigma \times C_\tau$, hence a morphism

$$\mathrm{Jac}(C) \to \mathrm{Jac}(C_\sigma) \times \mathrm{Jac}(C_\tau).$$

This morphism is an isogeny, in fact, it is a decomposed Richelot isogeny, see [28, Theorem 1]. We refer the reader for more details to [26] and [27].

In this work, we give special attention to the hyperelliptic curve defined by $y^2 = f(x^2)$ where $f(x) \in K[x]$ has no multiple roots.

Proposition 5.10. *Let $f(x) \in K[x] \setminus xK[x]$ have no multiple roots. Define the following hyperelliptic curves over K*

$$E_f : y^2 = f(x), \qquad C_f : y^2 = f(x^2), \qquad H_f : y^2 = xf(x).$$

Then $\mathrm{Jac}(C_f) \simeq \mathrm{Jac}(E_f) \times \mathrm{Jac}(H_f)$.

Proof. We write σ for the automorphism $(x, y) \mapsto (-x, y)$ on C_f. The automorphism σ is of order 2. The map $\phi_\sigma : C_f \to E_f$ defined by $\phi_\sigma : (x, y) \mapsto (x^2, y)$ is the quotient map $C_f \to C_f/\langle\sigma\rangle \cong E_f$. Similarly, if we set $\tau = \sigma \circ \iota : (x, y) \mapsto (-x, -y)$, then $\phi_\tau : C_f \to H_f$ defined by $\phi_\tau : (x, y) \mapsto (x^2, xy)$ is the quotient map such that

$$C_f \to C_f/\langle\tau\rangle \cong H_f.$$

□

One may ask whether it is always possible to find an explicit equation of the quotient curve. The answer is that finding such an explicit equation is not always feasible. We are certainly sure of its existence by Theorem 4.1 nonetheless finding its explicit equation is not always an easy task at all. Finding these equations mostly involves using action of automorphisms on coordinates x and y. In the previous proof, we identify two independent variables, namely x^2 and xy fixed by σ and $\sigma \circ \iota$, respectively. Hence, the equation describing the curve is obtained by finding the equation satisfied by these two parameters.

Theorem 5.11. *Let K be a number field. Given any integer $n \geq 2$, there exists an abelian variety that splits over K into two absolutely simple varieties of dimensions $n/2$ and $n/2$ if n is even; and $(n-1)/2$ and $(n+1)/2$ if n is odd.*

Proof. The statement holds in view of Proposition 5.5 for any integer n except possibly $2, 3$ and 5. A hyperelliptic curve with genus two whose Jacobian splits can

be constructed easily using Proposition 5.10. For example, one may consider the curve $y^2 = f(x^2)$ where $f(x) \in K[x] \setminus xK[x]$ is a polynomial of degree 3 with no multiple roots.

Let $f(x)$ be a polynomial of degree $d = 4$; or of degree $d = 6$ with Galois group either A_6 or S_6. The Jacobian of the curve $y^2 = f(x)$ is absolutely simple. This is justified by the fact that the Jacobian is an elliptic curve when $d = 4$; or it is an absolutely simple Jacobian of a genus two curve when $d = 6$, see Theorem 5.3. Now, for all but finitely many $t \in K$, the Jacobian of the curve $y^2 = (x-t)f(x)$ is absolutely simple, see Proposition 5.4. For each such value of t such that t is not a root of f, one may consider the following curves

$$E_f : y^2 = g_t(x) = f(x+t), \qquad C_f : y^2 = g_t(x^2) = f(x^2+t), \qquad H_f : y^2 = xg_t(x).$$

The latter curves are of genus 1 and 2 respectively when $d = 4$; or of genus 2 and 3 when $d = 6$, with absolutely simple Jacobians. Note that H_f is a shifting of the curve $y^2 = (x-t)f(x)$ by the transformation $x \mapsto (x+t)$, being absolutely simple is preserved since translation is an isomorphism. In addition, the Jacobian of the curve $y^2 = g_t(x^2) = f(x^2+t)$ is of dimension 3 when $d = 4$; or of dimension 5 when $d = 6$, for any such K-rational value t; and it enjoys the required splitting property, see Proposition 5.10. □

In other words, Theorem 5.11 asserts that for any given genus g, there exists a hyperelliptic curve whose jacobian decomposes into a product of two absolutely simple abelian varieties of either same or consecutive dimensions over a number field.

The following proposition indicates that given a polynomial in $K[x]$ of degree n with no multiple roots, one may construct an infinite sequence of hyperelliptic curves of any genus $\geq n-1$ whose Jacobian varieties decompose into two hyperelliptic Jacobian varieties whose dimensions differ by at most 1.

Proposition 5.12. *Let $f(x) \in K[x] \setminus xK[x]$ be a polynomial with no multiple roots. Define the following sequence of polynomials*

$$\begin{aligned} f_0(x) &= f(x), \\ g_i(x) &= xf_i(x), i \geq 0, \\ f_i(x) &= g_{i-1}(x + a_{i-1}), \qquad a_{i-1} \text{ is not a root of } g_{i-1}(x), i \geq 1. \end{aligned}$$

Setting $H_{-1}: y^2 = f(x)$, $H_i: y^2 = g_i(x)$ *and* $C_i: y^2 = f_i(x^2)$, *one has the following*

$$\mathrm{Jac}(C_i) \simeq \mathrm{Jac}(H_{i-1}) \times \mathrm{Jac}(H_i), \quad i \geq 0$$

If $\deg f = 2g+1$, *then* H_{i-1}, H_i *and* C_i *are of genus* $g+i/2$, $g+i/2$ *and* $2g+i$, *respectively, when* i *is even; and of genus* $g+r$, $g+r+1$, $2g+i$, *respectively, when* $i = 2r+1$ *is odd.*

If $\deg f = 2g+2$, *then* H_{i-1}, H_i *and* C_i *are of genus* $g+i/2$, $g+i/2+1$, $2g+i+1$, *respectively, when* i *is even; and of genus* $g+r+1$, $g+r+1$, $2g+i+1$, *respectively, when* $i = 2r+1$ *is odd.*

Proof. Observing that $E_i: y^2 = f_i(x)$ and H_{i-1}, $i \geq 1$, are isomorphic hyperelliptic curves, the proof follows directly from Proposition 5.10. □

In a similar fashion, we note that the construction of the genus 3 and 5 curves using Proposition 5.4 in the proof of Theorem 5.11 can be used to provide an alternative way of constructing families of hyperelliptic curves of genus $2n+1 \geq 5$ whose Jacobians decompose into the product of two absolutely simple abelian varieties of dimensions n and $n+1$. In addition, the defining polynomials of these curves are essentially multiples of a fixed polynomial of even degree with no multiple roots.

Given a polynomial $f \in K[x]$ of even degree with no multiple roots, we set

$$S(f) = \{t \in K : \text{the Jacobian of } y^2 = (x-t)f(x) \text{ is not absolutely simple; or } t \text{ is a root of } f(x)\}.$$

By Proposition 5.4, $S(f)$ is finite.

Corollary 5.13. *Let* K *be a number field. Let* $f(x) \in K[x] \setminus xK[x]$ *be a polynomial of degree* $2g$, $g \geq 1$, *with no multiple roots. Define the following sequence of polynomials*

$$\begin{aligned}
f_0(x) &:= f(x), \\
f_{i,t_{i-1}}(x) &:= (x + r'_{i,t_{i-1}})^{2g+2} g_{i-1,t_{i-1}}\left(\frac{x + r_{i,t_{i-1}}}{x + r'_{i,t_{i-1}}}\right), r_{i,t_{i-1}} \neq r'_{i,t_{i-1}} \\
g_{0,t_0}(x) &:= x f_0(x + t_0), \\
g_{i,t_i}(x) &:= x f_{i,t_{i-1}}(x + t_i), t_i \notin S(f_{i,t_{i-1}}), i \geq 1,
\end{aligned}$$

where $r_{i,t_{i-1}}$ *and* $r'_{i,t_{i-1}}$ *are chosen so that* $f_{i,t_{i-1}}(x) \in K[x] \setminus xK[x]$.

Setting $H_{i,t_i}: y^2 = g_{i,t_i}(x)$, *and* $C_{i,t_{i-1}}: y^2 = f_{i,t_{i-1}}(x^2)$, *then one has the following*

$$\mathrm{Jac}(C_{i,t_{i-1}}) \simeq \mathrm{Jac}(H_{i-1,t_{i-1}}) \times \mathrm{Jac}(H_{i,t_i})$$

where $\mathrm{Jac}(H_{i-1,t_{i-1}})$ *is absolutely simple for* $i \geq 1$. *The genus of the curves* H_{i,t_i} *and* $C_{i,t_{i-1}}$ *are* $g+i$ *and* $2g+2i-1$, *respectively.*

Proof. We remark that the polynomial $f_{i,t_{i-1}}$ is of even degree. The statement holds in view of Proposition 5.4 and Proposition 5.10 as the curves $H_{i-1,t_{i-1}}$ and $E_{i,t_{i-1}} : y^2 = f_{i,t_{i-1}}(x)$ are isomorphic hyperelliptic curves. □

If $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0 \in K[x]$ is an even palindromic polynomial with no multiple roots, we write $f_h(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0$. We notice that $f_h(x)$ is a palindromic polynomial itself. We, moreover, set $F_h(x,y) = a_{2g+2}x^{g+1} + a_{2g}x^g y + \cdots + a_2xy^g + a_0y^{g+1}$.

Theorem 5.14. *Let* $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0 \in K[x]$ *be an even palindromic polynomial with no multiple roots. Let* f_h *is defined to be*

$$f_h(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0.$$

Assume, moreover, that $C : y^2 = f(x)$ *and* $E : y^2 = f_h(x)$.

i) If $g \geq 2$ *is even, then* $\mathrm{Jac}(C) \simeq (\mathrm{Jac}(E))^2$.

ii) If $g \geq 3$ *is odd, then* $\mathrm{Jac}(C) \simeq \mathrm{Jac}(E) \times \mathrm{Jac}(G_1) \times \mathrm{Jac}(G_2)$ *where* $G_1 : y^2 = p(x)$ *and* $G_2 : y^2 = xp(x)$, *and* $p(x) \in K[x]$ *is just that*

$$p(x^2) = (x^2-1)F_h(x+1, x-1)$$

Proof. One observes that $\mathrm{Jac}(C) \simeq \mathrm{Jac}(E) \times \mathrm{Jac}(H)$, where H is defined by $y^2 = xf_h(x)$, see Proposition 5.10.

If $g = 2k$, then E and H are isomorphic hyperelliptic curves via the transformation

$$H \longrightarrow E, \quad (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{k+1}}\right),$$

see Proposition 2.68, hence the result.

If $g = 2k+1$, then we consider the map

$$H \longrightarrow G, \qquad (x,y) \mapsto \left(\frac{x+1}{x-1}, \frac{y}{(x-1)^{k+2}}\right)$$

where $G : y^2 = \ell(x)$. One obtains that

$$\ell(x) = (x^2-1)\left(a_{2g+2}(x+1)^{2k+2} + a_{2g}(x+1)^{2k+1}(x-1) + \cdots + a_2(x+1)(x-1)^{2k+1} + a_0(x-1)^{2k+2}\right),$$

hence $\ell(-x) = \ell(x)$, and ℓ is an even polynomial of degree $2k+4$. It follows that $\ell(x) = p(x^2)$ for some $p(x) \in K[x]$. In view of Proposition one has the following 5.10,

$$\mathrm{Jac}(G) \simeq \mathrm{Jac}(G_1) \times \mathrm{Jac}(G_2)$$

where $G_1 : y^2 = p(x)$ and $G_2 : y^2 = xp(x)$. □

Remark 5.15. *In Proposition 5.2, The curve $C' : y^2 = xf(x)$ possesses the automorphisms σ and $\sigma \circ \iota$ described by $(x,y) \mapsto \left(\frac{1}{x}, \frac{\pm y}{x^{g+2}}\right)$. In Theorem 5.14, the curve C' is described using a different equation, namely, $y^2 = p(x^2)$ where the two aforementioned automorphisms are now $(x,y) \mapsto (-x, \pm y)$. Therefore, $C'/\langle\sigma\rangle$ and $C'/\langle\sigma \circ \iota\rangle$ are isomorphic to the hyperelliptic curves defined by $y^2 = p(x)$ and $y^2 = xp(x)$.*

Corollary 5.16. *i) For any integer $n \geq 1$, there exist abelian varieties of dimension $2n$ that decompose over K as the square of an abelian variety of dimension n.*

ii) For any integer $n \geq 1$, there exist abelian varieties of dimension $2n+1$ that decompose over K as the product of three abelian varieties of dimensions n, $(n+1)/2$, and $(n+1)/2$ if n is odd; and n, $1+n/2$, and $n/2$ if n is even.

Remark 5.17. *We remark that Proposition 5.10 may be used to construct abelian varieties of dimension $2n+1$ that decompose into three abelian varieties of lower dimensions, namely, $n+1$, $(n+1)/2$, $(n-1)/2$ if n is odd; and $n+1$, $n/2$, $n/2$ if n is even; which differs from the partitions of the dimension given in Corollary 5.16. In addition, Proposition 5.10 does not provide a decomposable Jacobian whose dimension is 3.*

Example 5.18. *If we consider the curve*

$$C : y^2 = ax^6 + bx^4 + bx^2 + a \in K[x],$$

then $\mathrm{Jac}(C) \simeq E^2$ where E is the elliptic curve $y^2 = ax^3 + bx^2 + bx + a$.

Example 5.19. *In Theorem 5.14, if one considers the curve*

$$C : y^2 = ax^8 + bx^6 + cx^4 + bx^2 + a \in K[x]$$

of genus 3, then $\mathrm{Jac}(C)$ is isogenous to the product of three elliptic curves that are

the Jacobians of the following genus 1 *curves*

$$\begin{aligned}
E_1 : y^2 &= ax^4+bx^3+cx^2+bx+a,\\
E_2 : y^2 &= (2a+2b+c)x^3+(10a-2b-3c)x^2+(-10a-2b+3c)x+(-2a+2b-c),\\
E_3 : y^2 &= x\Big((2a+2b+c)x^3+(10a-2b-3c)x^2+(-10a-2b+3c)x+(-2a+2b-c)\Big).
\end{aligned}$$

Proposition 5.20. *Let* $f(x) \in K[x]$ *be a palindromic polynomial of degree at least* 3. *Consider the hyperelliptic curve* $C : y^2 = f(x^4)$. *Then,*

$$\mathrm{Jac}(C) \simeq \mathrm{Jac}(E_1) \times \mathrm{Jac}(E_2) \times \mathrm{Jac}(G_1) \times \mathrm{Jac}(G_2)$$

where $E_1 : y^2 = f(x)$, $E_2 : y^2 = xf(x)$, *and* G_1 *and* G_2 *are as in Theorem 5.14.*

Proof. In view of Theorem 5.14, one has $\mathrm{Jac}(C) \simeq \mathrm{Jac}(E) \times \mathrm{Jac}(G_1) \times \mathrm{Jac}(G_2)$ where $E : y^2 = f(x^2)$. Now due to Proposition 5.10, one obtains that

$$\mathrm{Jac}(E) \simeq \mathrm{Jac}(E_1) \times \mathrm{Jac}(E_2).$$

□

Corollary 5.21. *Given any integer* $n \geq 2$. *There exists abelian varieties of dimension* $2n+1$ *that decompose over* K *as the product of four abelian varieties of dimensions* $(n-1)/2$, $(n+1)/2$, $(n+1)/2$, *and* $(n+1)/2$ *if* n *is odd; and* $n/2$, $n/2$, $n/2$, *and* $1+n/2$ *if* n *is even.*

Example 5.22. *The Jacobian of the hyperelliptic curve* $y^2 = ax^{12}+bx^8+bx^4+a$ *is isogenous to the product of the elliptic curves that are the Jacobians of the genus one curves* E_1, E_2, G_1; *and the Jacobian of the genus* 2 *curve* G_2

$$\begin{aligned}
E_1 : y^2 &= ax^3+bx^2+bx+a,\\
E_2 : y^2 &= x(ax^3+bx^2+bx+a),\\
G_1 : y^2 &= 2(a+b)x^4+2(14a-2b)x^3+2(-14a+2b)x+2(-a-b),\\
G_2 : y^2 &= x\Big(2(a+b)x^4+2(14a-2b)x^3+2(-14a+2b)x+2(-a-b)\Big).
\end{aligned}$$

5.1 Rational Points on Quadratic Twists

In this section, given any integer $g \geq 1$, we construct a hyperelliptic curve of genus g with infinitely many quadratic twists containing at least two K-rational non-Weierstrass points.

Proposition 5.23. *Let $f(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0 \in K[x]$ be a palindromic polynomial with no multiple roots. Consider the curve $C : y^2 = f(x)$. If g is even, then there exists infinitely many quadratic twists of C with at least two K-rational non-Weierstrass points.*

Proof. Consider the curve $C_{f(t^2)}$ defined over $K(t)$ by

$$f(t^2)y^2 = f(x).$$

The set of rational points of $C_{f(t^2)}$ contains the $K(t)$-rational points $\left(t^2, 1\right)$ and $\left(\frac{1}{t^2}, \frac{1}{t^{2k+1}}\right)$ where $g = 2k$. We remark that these points are obtained by considering the quotient maps in 5.14 i). □

In the previous proposition, if $g = 2$, then C is a genus 1 curve. This implies the existence of infinitely many quadratic twists of C that are elliptic curves with Mordell-Weil rank at least 2. That the points are of infinite order follow from Theorem 2.43 together with Theorem 2.40, whereas the independence of the points follows from the fact that the quotient maps in Theorem 5.14 are independent maps by construction.

In what follows, we concern ourselves with the construction of tuples of hyperelliptic curves $C_1, \cdots, C_n$ and infinitely many square-free K-rational d such that the quadratic twists of these curves by each d contain K-rational non-Weierstrass points.

Proposition 5.24. *Let $f(x) \in K[x]$ be a palindromic polynomial of degree at least 3 with no multiple roots. Consider the following curves*

$$E_1 : y^2 = f(x), \quad E_2 : y^2 = xf(x), \quad G_1 : y^2 = p(x), \quad G_2 : y^2 = xp(x)$$

where $p(x)$ is defined as in Theorem 5.14. There exists infinitely many nonzero $d \in K \setminus K^2$ such that the quadratic twists of E_1, E_2, G_1 and G_2 by d contain K-rational non-Weierstrass points.

Proof. We set $n := \deg f$. We will list down the quadratic twists together with the

K-rational points on them

$$\begin{aligned}
f(t^4)y^2 &= f(x), && (t^4, 1), \\
f(t^4)y^2 &= xf(x), && \left(\frac{1}{t^4}, \frac{1}{t^{2n+2}}\right), \\
f(t^4)y^2 &= p(x), && \left(\frac{(t^2+1)^2}{(t^2-1)^2}, \frac{2^{n+1}t}{(t^2-1)^{n+1}}\right), \\
f(t^4)y^2 &= xp(x), && \left(\frac{(t^2+1)^2}{(t^2-1)^2}, \frac{2^{n+1}t(t^2+1)}{(t^2-1)^{n+2}}\right).
\end{aligned}$$

These K-rational points are obtained using the quotient maps in Proposition 5.20. □

In Proposition 5.24, if f is chosen to be of degree 3, then the proposition presents an example of three elliptic curves together with a genus 2 curve such that there are infinitely many d for which the quadratic twists of these curves by such a d has at least one K-rational point. Moreover, we can check these independent rational points have non-constant coordinates by specialization. It follows that the points are of infinite order on the quadratic twists of the elliptic curves by Theorem 2.43 with Theorem 2.40, and it is a K-rational non-Weierstrass point on the genus two curve.

BIBLIOGRAPHY

[1] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski. Chabauty–coleman experiments for genus 3 hyperelliptic curves. In *Research Directions in Number Theory: Women in Numbers IV*, pages 67–90. Springer, 2019.

[2] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[3] G. Cardona, J. González, J.-C. Lario, and A. Rio. On curves of genus 2 with jacobian of gl 2-type. *manuscripta mathematica*, 98:37–54, 1999.

[4] A. Carocca, H. Lange, and R. E. Rodríguez. Decomposable jacobians. *arXiv preprint arXiv:1906.07747*, 2019.

[5] J. W. Cassels and A. Schinzel. Selmer's conjecture and families of elliptic curves. *Bulletin of the London Mathematical Society*, 14(4):345–348, 1982.

[6] G. Coogan and J. Jimenez-Urroz. Mordell–weil ranks of quadratic twists of pairs of elliptic curves. *Journal of Number Theory*, 96(2):388–399, 2002.

[7] R. D. Costa and C. Salgado. Large rank jumps on elliptic surfaces and the hilbert property. *arXiv preprint arXiv:2205.07801*, 2022.

[8] J. Cremona. Classical invariants and 2-descent on elliptic curves. *Journal of Symbolic Computation*, 31(1-2):71–87, 2001.

[9] J. Desjardins and B. Naskrkecki. Geometry of the del pezzo surface $y^2 = x^3 + am^6 + bn^6$. *arXiv: Number Theory*, 2019. URL https://api.semanticscholar.org/CorpusID:207847641.

[10] C. J. Earle. Some jacobian varieties which split. In *Complex Analysis Joensuu 1978: Proceedings of the Colloquium on Complex Analysis, Joensuu, Finland, August 24–27, 1978*, pages 101–107. Springer, 2006.

[11] T. 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.

[12] J. S. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski. Non-simple abelian varieties in a family: geometric and analytic approaches. *Journal of the London Mathematical Society*, 80(1):135–154, 2009.

[13] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73:349–366, 1983.

[14] L. D. Feo. Mathematics of isogeny based cryptography. *ArXiv*, abs/1711.04062, 2017. URL https://api.semanticscholar.org/CorpusID:9252863.

[15] S. Fermigier. Un exemple de courbe elliptique définie sur q de rang ≥ 19. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 315(6): 719–722, 1992.

[16] S. Fermigier. Une courbe elliptique définie sur q de rang ≥ 22. *Acta Arithmetica*, 82(4):359–363, 1997.

[17] D. M. Freeman and T. Satoh. Constructing pairing-friendly hyperelliptic curves using weil restriction. *Journal of Number Theory*, 131(5):959–983, 2011.

[18] J. Gutierrez, D. Sevilla, and T. Shaska. Hyperelliptic curves of genus 3 with prescribed automorphism group. *arXiv: Algebraic Geometry*, 2005. URL https://api.semanticscholar.org/CorpusID:119175131.

[19] R. Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[20] T. Hayashida and M. Nishi. Existence of curves of genus two on a product of two elliptic curves. *Journal of the Mathematical Society of Japan*, 17(1):1–16, 1965.

[21] A. Hermez and A. Salinier. Rational trinomials with the alternating group as galois group. *Journal of Number Theory*, 90(1):113–129, 2001.

[22] E. W. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split jacobians of curves of genus two or three. *Forum Mathematicum*, 12, 1998. URL https://api.semanticscholar.org/CorpusID:5526276.

[23] A. Hurwitz. Über algebraische gebilde mit eindeutigen transformationen in sich. *Mathematische Annalen*, 41(3):403–442, 1892.

[24] J.-i. Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, pages 612–649, 1960.

[25] B.-H. Im. Positive rank quadratic twists of four elliptic curves. *Journal of Number Theory*, 133(2):492–500, 2013.

[26] E. Kani and M. Rosen. Idempotent relations and factors of jacobians. *Mathematische Annalen*, 284(2):307–327, 1989.

[27] T. Katsura. Decomposed richelot isogenies of jacobian varieties of curves of genus 3. *Journal of Algebra*, 588:129–147, 2021.

[28] T. Katsura and K. Takashima. Decomposed richelot isogenies of acobian varieties of hyperelliptic curves and generalized howe curves. *arXiv preprint arXiv:2108.06936*, 2021.

[29] R. M. Kuhn. Curves of genus 2 with split jacobian. *Transactions of the American Mathematical Society*, 307(1):41–49, 1988.

[30] M. Kuwata. Quadratic twists of an elliptic curve and maps from a hyperelliptic curve. *Mathematical Journal of Okayama University*, 47(1):85–98, 2005.

[31] S. Lang. *Fundamentals of Diophantine Geometry*. Springer, 1983.

[32] F. Legrand. Twists of superelliptic curves without rational points. *International Mathematics Research Notices*, 2018(4):1153–1176, 2018.

[33] Q. Liu. Modèles minimaux des courbes de genre deux. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1994:137 – 164, 1994. URL https://api.semanticscholar.org/CorpusID:122754552.

[34] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6. Oxford Graduate Texts in Mathe, 2002.

[35] LMFDB Collaboration. Elliptic curve, 2024. URL https://www.lmfdb.org/EllipticCurve/Q/?rank=0&torsion=%5B%5D.

[36] D. Lombardo, E. L. García, C. Ritzenthaler, and J. Sijsling. Decomposing jacobians via galois covers. *Experimental Mathematics*, 32(1):218–240, 2023.

[37] D. Loughran and C. Salgado. Rank jumps on elliptic surfaces and the hilbert property. In *Annales de l'Institut Fourier*, volume 72, pages 617–638, 2022.

[38] B. Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[39] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.

[40] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and hilbert's tenth problem. *Inventiones mathematicae*, 181(3):541–575, 2010.

[41] A. Menezes, R. Zuccherato, and Y.-H. Wu. *An elementary introduction to hyperelliptic curves*. Faculty of Mathematics, University of Waterloo, 1996.

[42] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[43] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5. American Mathematical Soc., 1995.

[44] K.-i. Nagao. An example of elliptic curve over q with rank ≥ 20. *Proc. Japan Acad. Ser. A Math. Sci*, 69(8):291–293, 1993.

[45] K.-i. Nagao and T. Kouya. An example of elliptic curve over q with rank >21. 1994.

[46] J. Nakagawa and K. Horie. Elliptic curves with no rational points. *Proceedings of the American Mathematical Society*, 104(1):20–24, 1988.

[47] R. Nakajima. On splitting of certain jacobian varieties. *Journal of Mathematics of Kyoto University*, 47(2):391–415, 2007.

[48] E. Nart and N. Vila. Equations of the type $x^n + ax + b$ with absolute galois group S_n. *Revista de la universidad*, 2:821–825, 1979.

[49] R. Ohashi and M. Kudo. Computing superspecial hyperelliptic curves of genus 4 with automorphism group properly containing the klein 4-group. *arXiv preprint arXiv:2312.16858*, 2023.

[50] H. Osada. The galois groups of the polynomials $x^n + ax + b$. *Journal of number theory*, 25(2):230–238, 1987.

[51] J. Paulhus. Decomposing jacobians of curves with extra automorphisms. *Acta Arith*, 132(3):231–244, 2008.

[52] J. Paulhus. Elliptic factors in jacobians of hyperelliptic curves with certain automorphism groups. *The Open Book Series*, 1(1):487–505, 2013.

[53] J. Paulhus and A. M. Rojas. Completely decomposable jacobian varieties in new genera. *Experimental Mathematics*, 26(4):430–445, 2017.

[54] J. R. Paulhus. *Elliptic factors in Jacobians of low genus curves*. PhD thesis, University of Illinois at Urbana-Champaign, 2007.

[55] K. Rubin and A. Silverberg. Rank frequencies for quadratic twists of elliptic curves. *Experimental Mathematics*, 10(4):559–569, 2001.

[56] M. Sadek. On quadratic twists of hyperelliptic curves. *Rocky Mountain Journal of Mathematics*, 44:1015–1026, 2010. URL https://api.semanticscholar.org/CorpusID:119323150.

[57] C. Salgado. On the rank of the fibers of rational elliptic surfaces. *Algebra & Number Theory*, 6(7):1289–1314, 2012.

[58] F.-O. Schreyer. Lecture notes of sheaf cohomology vector bundle of week 11, 2018. URL https://www.math.uni-sb.de/ag/schreyer/images/PDFs/teaching/ws1819_sheaves/LectureNotes/Week11.pdf.

[59] T. Shaska. Genus 3 hyperelliptic curves with (2, 4, 4)-split jacobians. *ACM Commun. Comput. Algebra*, 49:55, 2013. URL https://api.semanticscholar.org/CorpusID:19257838.

[60] A. Silverberg. Ranks "cheat sheet". *Women in*, (2):101–110.

[61] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[62] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[63] J. H. Silverman and J. T. Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[64] H. Stichtenoth. *Algebraic function fields and codes*. Springer Science & Business Media, 2009.

[65] M. Stoll. Arithmetic of hyperelliptic curves. *Screen Version of August*, 1(2014): 1, 2014.

[66] A. Sutherland. 18.783 elliptic curves. Spring 2017.

[67] T. Yamauchi. On curves with split jacobians. *Communications in Algebra®*, 36(4):1419–1425, 2008.

[68] Y. G. Zarhin. Hyperelliptic jacobians without complex multiplication. *Mathematical Research Letters*, 7:123–132, 1999. URL https://api.semanticscholar.org/CorpusID:2409848.

[69] Y. G. Zarhin. Families of absolutely simple hyperelliptic jacobians. *Proceedings of the London Mathematical Society*, 100, 2008. URL https://api.semanticscholar.org/CorpusID:11930411.