Universität Ulm

ulm university universität
uulm

Algorithms for curves of low genus: complex multiplication and Dieudonné theory

Vorgelegt von
Bogdan Adrian Dina

aus Ulm im Jahr 2021

Dissertation zur Erlangung des Doktorgrades Dr. rer. nat. der Fakultät für Mathematik und Wirtschaftswissenschaften der Universität Ulm

Amtierender Dekan:
Prof. Dr. Stefan Funken

Gutacher:
Prof. Dr. Irene Ingeborg Bouw
Dr. Elisa Lorenzo García

Tag der Promotion: 08. November 2021

Parts of this dissertation have already been published:

(i) B. Dina and S. Ionica. Genus 3 hyperelliptic curves with CM via Shimura reciprocity. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), Mathematical Sciences Publishers, Berkeley, 2020 ([17]).

(ii) B. Dina, S. Ionica, and J. Sijsling. cm-calculations, a Magma package for calculating with CM curves. https://github.com/JRSijsling/cm-calculations, 2021 ([18]).

(iii) B. Dina, S. Ionica, and J. Sijsling. Isogenous hyperelliptic and non-hyperelliptic jacobians with maximal complex multiplication. arxiv:2104.04519, 2021 ([19]).

Contents

Introduction **v**
Setting . . . v
Main results . . . vi
The algorithms . . . viii
Outline . . . viii
Acknowledgments . . . x

1 Abelian Varieties **1**
1.1 Definitions . . . 2
1.2 The dual abelian variety and polarizations . . . 2
1.3 Pairings . . . 3

2 Abelian Varieties over $\mathbb{C}$ **5**
2.1 Complex tori . . . 5
2.2 Line bundles on complex tori . . . 6
2.3 The Riemann relations . . . 7
2.4 The dual abelian variety and polarizations . . . 8
2.5 Pairings . . . 10
2.6 Endomorphisms of abelian varieties . . . 10
2.7 The Siegel upper half space . . . 13

3 Jacobian Varieties **15**
3.1 Definitions . . . 15
3.2 The analytic construction of the Jacobian . . . 15
3.3 The Abel-Jacobi map . . . 16
3.4 The genus-3 case . . . 17

4 Smooth Projective Curves **19**
4.1 Definitions . . . 19
4.2 Smooth projective curves of genus 3 . . . 19
4.3 Hyperelliptic curves of genus 3 . . . 19
4.4 Non-hyperelliptic curves . . . 21

5 The Hyperelliptic Locus **23**
5.1 Definitions . . . 23
5.2 Riemann theta functions . . . 23
5.3 Theta functions with half-integer characteristics . . . 23
5.4 η-maps . . . 25
5.5 The genus-3 case . . . 28

6 Abelian Varieties with Complex Multiplication **31**
6.1 Definitions . . . 31
6.2 Ideals and polarizations . . . 32

7 Isogenous Hyperelliptic and Non-Hyperelliptic Jacobians with Maximal Complex Multiplication **35**
7.1 Definitions . . . 35
7.2 The main results . . . 36
7.3 Structure of sextic CM fields . . . 38
7.4 CM types . . . 39
7.5 Reflex CM types . . . 42
7.6 The Shimura class group and the Galois action . . . 45
7.7 Torsor and moduli spaces . . . 46
7.8 Representatives up to Galois conjugacy . . . 49
7.9 The algorithms . . . 52
7.10 Invariants . . . 59
7.11 Explicit defining equations . . . 62
7.12 Around the André–Oort conjecture . . . 66

8 Genus 3 Hyperelliptic Curves with Complex Multiplication via Shimura Reciprocity **69**
8.1 Definitions . . . 70
8.2 Class field theory . . . 71
8.3 The Shimura class group modulus $\mathfrak{m}$ and the Galois action . . . 71
8.4 Shimura's Second Main Theorem of complex multiplication . . . 74
8.5 Computing class polynomials . . . 74

9 Linear Algebra Data of Supersingular Abelian Varieties **85**
9.1 Definitions . . . 85
9.2 Polarized flaq type quotients . . . 87
9.3 The Dieudonné-Cartier-Oda-classification . . . 87
9.4 Polarized flag type quotients of supersingular Dieudonné modules . . . 90
9.5 Linear algebra data of supersingular elliptic curves . . . 93
9.6 The genus-2 case . . . 94
9.7 The genus-3 case . . . 105

Appendices **123**

A Group Schemes **125**

B Affine Group Schemes **127**

Bibliography **131**

Zusammenfassung in deutscher Sprache **137**

»*The theory of complex multiplication ...is not only the most beautiful part of mathematics but also of all science.*«

— David Hilbert

Introduction

In this thesis we study *classification problems* in algebraic geometry. In the context of algebraic geometry these classification problems are called *moduli problems*. In an informal way, a moduli problem is that of classifying of families of algebraic objects with certain extra structure. In our case, the algebraic objects are *abelian varieties* with *complex multiplication (CM)*. In order to solve certain (algorithmic) algebraic problems, we give a detailed description of the *linear-algebraic data* of abelian varieties with CM.

Setting

Given a positive number g, we consider moduli problems for abelian varieties, that is that of parametrizing pairs

$$(A, \eta),$$

where A is an abelian variety of dimension g over some field k, and where $\eta : A \to A^t$ is a principal polarization.

In the first part of this thesis, especially in the Chapters 7 and 8, we restrict to the case where $g = 3$. It is known that in this case (A, η) isomorphic over $\overline{k}$ to the Jacobian of a (possibly reducible) algebraic curve X of genus g. In the case where $k = \mathbb{C}$ and the curve X is a smooth projective curve of genus g, we describe abelian varieties by pairs

$$(\mathbb{C}^g/\Lambda, E),$$

where $\mathbb{C}^g/\Lambda$ is a complex torus of dimension g, and where E is the Riemann form on the lattice Λ inducing a principal polarization on the torus. In this thesis, we consider *complex multiplication (CM)* points in the moduli space of principally polarized abelian varieties of dimension g. An abelian variety has CM if its endomorphism ring is "as large as possible". For abelian varieties A over $\mathbb{C}$ this means that their endomorphism ring $\mathrm{End}(A)$ is an order in a CM field. A CM field is an imaginary quadratic extension of a totally real number field. In this thesis we restrict consideration to CM by the maximal order $\mathcal{O}_K$, where K is a CM field of degree $2g$. After considering CM points in the moduli space, these points can instead be described by pairs

$$(\mathbb{C}^g/\Phi(\mathfrak{a}), \xi),$$

where Φ is a primitive CM type on K, where $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, and where ξ is an element in K with some additional properties, inducing a Riemann form $E = E_\xi$ on the lattice $\Phi(\mathfrak{a})$. Another piece of data attached to abelian varieties with CM are their CM types. If A is an abelian variety of dimension g over $\mathbb{C}$ with CM by K, then a CM type Φ on K is a set of g embeddings of K into $\mathbb{C}$, pairwise not complex conjugate to each other. Given the principally polarized abelian variety A of dimension g over $\mathbb{C}$ with CM by K, then only the *equivalence class* of the CM type Φ is well-defined. An explicit moduli problem in this case is to classify (and to determine algorithmically) points in the CM-by-$\mathcal{O}_K$ locus inside the moduli space of principally polarized abelian varieties of dimension g.

In our research we often aim to explicitly find an algebraic equation of curves X with additional properties. It is known that in the genus-3 case there are two types of algebraic

curves, namely *hyperelliptic* and *non-hyperelliptic* curves. These types can be distinguished by the form of their algebraic equations. Given a principally polarized abelian variety (A, η) of dimension $g = 2, 3$ over $\mathbb{C}$ described by pairs $(\mathbb{C}^g/\Phi(\mathfrak{a}), \xi)$, we want to describe the corresponding curve by an *explicit equation*. Moreover, we would like to find an equation over the smallest possible number field, and *not merely* over $\mathbb{C}$. The key step here is to find so-called *invariants* of the curve. In the hyperelliptic case we consider the *Rosenhain* and *Shioda* invariants. In the non-hyperelliptic case, we use instead the *Dixmier-Ohno* invariants.

In order to introduce moduli problems related to the last part of this thesis, see Chapter 9, we change the scene. Let k be an algebraically closed field of $\mathrm{char}(k) = p > 0$. Let E be a *supersingular elliptic curve* over a finite field $k \supset \mathbb{F}_p$. An abelian variety A in positive characteristic is called *supersingular* if it is isogenous to a product of supersingular elliptic curves. It is known that this is equivalent to the condition that A is isogenous to E^g for a fixed supersingular elliptic curve. The *supersingular locus* inside the moduli space of principally polarized abelian varieties of dimension g forms a (reducible) locus of $\dim = [g^2/4]$, see [46]. Li and Oort described in [46] the points of this locus in terms of linear-algebraic data. In Chapter 9 we provide more details on their results for genus $g = 2, 3$, making the linear-algebraic data completely explicit.
We notice that in Chapters 7 and 8, the construction of the Jacobian played a key role in the *explicit* construction of the algebraic equation of the curve. We expect that the linear-algebraic data from Li-Oort plays a similar role for explicit constructions of curves of genus g. We now describe the linear algebra of Li-Oort in somewhat more detail. We refer to Section 9.2 for a precise definition. We consider *polarized flag type quotients (pftq's)* over k with respect to a polarization η_{g-1}, given by

$$\left(\left(Y_{g-1} = E^g, \eta_{g-1}\right) \xrightarrow{\rho_{g-1}} \left(Y_{g-2}, \eta_{g-2}\right) \xrightarrow{\rho_{g-2}} \ldots \longrightarrow (Y_1, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0)\right)$$

where (Y_i, η_i) are polarized abelian varieties of dimension g over k, where η_0 is an isomorphism, where $\ker(\eta_i) \subset Y_i[F^i]$ for $0 \leq i \leq g-1$, where F is the relative Frobenius, together with isogenies ρ_i such that $\ker(\rho_i)$ is an α-group of rank i for $1 \leq i \leq g-1$. Given a pair

$$(g, p),$$

where $g \geq 2$ is a positive integer, $p \geq 2$ a prime number and E a supersingular elliptic curve over a finite field $k \supset \mathbb{F}_p$, our goal is to classify the pairs (A, η) such that

$$(A, \eta) \cong (Y_0, \eta_0),$$

for some pftq's with respect to (E^g, η_{g-1}).

Main results

The main results in this thesis discussed in the Chapters 7 and 8 are about principally polarized abelian varieties of dimension 3 with CM. We will call a curve X of genus g over an algebraically closed field a *CM* curve, if the endomorphism ring of its Jacobian $\mathrm{Jac}(X)$ is an order in a number field of degree $2g$. If a curve X has CM by a number field K, then there exists an embedding

$$\iota : K \hookrightarrow \mathrm{End}^0(A).$$

Such a field K is called a *CM field*. Let $\mathcal{O}_K$ be the ring of integers of K. We say X has *CM by* $\mathcal{O}_K$ if $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}_K$.

The main results in Chapter 7 are given by the following three theorems. Before stating these, a motivating question for the paper [19] = Chapter 7 was: *Do there exist sextic CM fields for which there are both hyperelliptic and non-hyperelliptic Jacobians of dimension* 3 *with CM by the maximal order of this field*? One such CM field has been already well known.

Theorem 0.0.1 (Theorem 7.2.1)**.** *Heuristically, there are at least* 14 *sextic CM fields* K *for which there exist both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order* $\mathcal{O}_K$ *of* K*. All these fields have Galois group*

$$\mathrm{Gal}(K|\mathbb{Q}) \simeq C_2^3 \rtimes S_3.$$

The "L-functions and Modular Forms Database" (LMFDB) is a catalog of mathematical objects together with connections between them. In order to get our Main Results in Theorems 0.0.1 and 0.0.2, we used all of the 547,156 sextic CM fields included in the LMFDB ([73]) for our computations.
Let K be a CM field of degree 6. The possibilities for the Galois group $\mathrm{Gal}(K|\mathbb{Q})$ are known; there are 4 possibilities (see [20]). The following theorem is an alternative version of the Theorem 0.0.1.

Theorem 0.0.2 (Theorem 7.2.3)**.** *Heuristically, including the fields mentioned in Theorem 0.0.1, there are* 3,422 *CM fields* K *for which there exists a hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order* $\mathcal{O}_K$ *of* K*. Of these fields,* 348 *(resp.* 3,057*, resp.* 17*) have Galois group isomorphic to* C_6 *(resp.* D_6*, resp.* $C_2^3 \rtimes S_3$*). We have* $\mathbb{Q}(i) \subset K$ *for all but* 19 *of these fields* K*. Among the exceptional cases,* 2 *(resp.* 17*) have Galois group isomorphic to* C_6 *(resp.* $C_2^3 \rtimes S_3$*).*

Besides determining the fields involved, we can also find corresponding invariants. Our final theorem in this chapter even gives a defining equation for the field in the Main Theorem 0.0.1 with the smallest discriminant.

Theorem 0.0.3 (Theorem 7.2.6)**.** *Let* K *be a CM field with smallest absolute absolute discriminant among the fields from Theorem 0.0.1, defined by the polynomial* $t^6 + 10t^4 + 21t^2 + 4$*. Equations* (7.2.1) *and* (7.2.2) *give a hyperelliptic curve* X *and a non-hyperelliptic curve* Y *such that heuristically* $\mathrm{Jac}(X)$ *and* $\mathrm{Jac}(Y)$ *both have CM by* $\mathcal{O}_K$*. Moreover, heuristically there exists an isogeny of degree* 2 *between* $\mathrm{Jac}(X)$ *and* $\mathrm{Jac}(Y)$*.*

In Chapter 8, we consider the computation of the *Shioda* and *Rosenhain class polynomials* of hyperelliptic curves of genus 3 by using Shimura's reciprocity law. The main result in this Chapter is given by the following theorem.

Theorem 0.0.4 (Theorem 8.5.9)**.** *Given the Jacobian* $\mathrm{Jac}(X)$ *of a marked hyperelliptic curve* X *of genus* 3 *over* $\mathbb{C}$ *with CM by the maximal order* $\mathcal{O}_K$ *of a CM field* K*, we can use Shimura's reciprocity law to explicitly compute (approximations of) the Galois conjugate Rosenhain invariants of the Galois conjugate hyperelliptic curve of* X *over the reflex field* K^r *of* K*.*

The descriptions in Chapter 9 serve as an introduction, and a preparation in the theory of *supersingular* polarized abelian varieties of dimension g over fields of positive characteristic. In

this chapter we introduce *Li* and *Oort's* construction of *polarized flag type quotients (pftq's)*. In the main part of this chapter we explicitly describe the linear-algebraic data related to the finite commutative group schemes of pftq's of dimension 2 and 3. The explicit description of pftq's using linear-algebraic data enables algorithmic questions to be answered in this area.

The algorithms

Let K be a sextic CM field and Φ a primitive CM type of K. We give in the first main part of the thesis, especially in the Chapters 7 and 8 explicit algorithms for the construction of principally polarized abelian varieties $A(\Phi, \mathfrak{a}, \xi)$ of dimension 3 over $\mathbb{C}$ with CM. We give further algorithms for the computation of the *Rosenhain* and *Shioda class polynomials* by using Shimura's reciprocity law. The construction of the algorithms in this thesis are based in part on the construction of principally polarized abelian surfaces with CM by M. Streng, see [69].

In order to answer the motivating question for the paper [19], we focused our search on the "L-functions and Modular Forms Database" (LMFDB). It contains 547,156 sextic CM fields. To achieve our goal, the third author in [19] and I developed and implemented effective computational methods that, given a CM field K and a primitive CM type Φ, determine a small set of period matrix representatives of the corresponding isomorphism classes of principally polarized abelian threefolds up to Galois conjugation over the reflex field. A calculation with theta-null values (using [38]) then allows us to see which of these representatives correspond to hyperelliptic or non-hyperelliptic curves.

In order to compute Rosenhain and Shioda class polynomials, we computed Galois conjugate Rosenhain and Shioda invariants of CM hyperelliptic curves over the reflex field K^r of K in Theorem 0.0.4. I developed and implemented computational methods that, given a CM field K, determine the set of all primitive CM types of K up to conjugacy. Then determine a (small) set of representatives of elements in the Shimura class group of K, corresponding to isomorphism classes of principally polarized abelian threefolds with CM by $\mathcal{O}_K$ up to Galois conjugation over the reflex field. A calculation with theta-null values (using the method from [2]) then allows us to see which of these representatives correspond to hyperelliptic or non-hyperelliptic curves. Then finally compute Galois conjugate Rosenhain invariants using the representation of these in Theorem (0.0.4).

Outline

This thesis is divided into three main parts.
In the first part, we introduce the (algebraic and analytic) theory of polarized abelian varieties. Since in the genus-3 case, polarized abelian varieties are Jacobian of (possibly reducible) algebraic curves of genus 3, we introduce the analytic construction of the Jacobians, and we discuss the two different types of algebraic curves in genus 3. Then we introduce *Shimura* and *Taniyama's* construction of polarized abelian varieties with CM.

The second part contains the paper [19] and a revised version of the paper [17]. We begin Chapter 7 with the theory on CM fields, their reflex CM types, and their Shimura class groups. More precisely, we give an explicit description of (reflex) CM types of sextic CM fields, followed by the classification of CM types up to Galois conjugation. In order to determine a small set of period matrix representatives of the isomorphism classes of principally polarized abelian

threefolds, up to Galois conjugation over the reflex field, we study the image of the reflex type norm. In particular, we prove general results on the transitivity of the Galois action on CM types and on the image of the reflex type norm. In Section 7.9 we use these results and further speedups to check the 547,156 sextic CM fields in the LMFDB for the existence of a corresponding hyperelliptic curve, which leads to Main Theorems 0.0.1 and 0.0.2. In the Sections 7.10 and 7.11 we discuss techniques for determining explicit defining equations, and includes the proof of the Main Theorem . We conclude the chapter by some discussions around the relevance of the André–Oort conjecture to our considerations in Section 7.12.
We begin Chapter 8 with a brief introduction to class field theory. In the Sections 8.2 and 8.3, we recall the definition of the ray class field of a modulus $\mathfrak{m}$. Then we define the Shimura class group for a modulus $\mathfrak{m}$ of a sextic CM field K, and the reflex type norm map with respect to the modulus $\mathfrak{m}$. In order to compute the Rosenhain and Shioda class polynomials, we recall Shimura's Second Main Theorem of complex multiplication in Section 8.4. We begin Section 8.5 by introducing the Shioda invariants of hyperelliptic curves of genus 3. Then, by using Shimura's Second Main Theorem of complex multiplication, we give an explicit description of the Galois conjugate Shioda and Rosenhain invariants of hyperelliptic curves of genus 3 over the reflex field K^r of K. This section includes the proof of the Theorem 0.0.4. We finish this chapter with an explicit example of the computation of the coefficients of the Shioda and Rosenhain class polynomials.

In the third part of this thesis, in Chapter 9, we discuss the theory in [46]. We begin this chapter with the definition of supersingular abelian varieties of dimension g. In Section 9.2 we introduce polarized flag type quotients (pftq's) with respect to polarizations. In Section 9.3 we recall the Dieudonné-Cartier-Oda-classification and the definition of Dieudonné modules of supersingular elliptic curves. This classification allow us to identify pftq's as linear-algebra objects in terms of Dieudonné modules. In section 9.4 we define polarized flag type quotients of supersingular Dieudonné modules and introduce the concept of quasi-polarization on Dieudonné modules. In Section 9.5 we give an explicit description of the linear-algebraic data of supersingular elliptic curves. This serves as a preparation for the last sections of this thesis. In the Sections 9.6 and 9.7, we give a detailed description of pftq's of Dieudonné modules of genus $g = 2, 3$. We finish these sections by considering the moduli spaces of supersingular principally polarized abelian varieties of dimension 2 and 3.

Acknowledgments

First and foremost I want to thank my supervisor *Prof. Dr. Irene Ingeborg Bouw*. We have know each other since 2013. At that time you were my lecturer in the course Cryptology, and I was studying computer science in my first master's semester. I remember our first conversation and that you encouraged me to study mathematics. And today I can say that, from an academic point of view, it was the best decision I have taken. I thank you for your support and guidance during the course of my studies. I would especially like to thank you for offereding to supervise me without hesitation in a time when I was very unhappy and dissatisfied. Thank you for all of our mathematical and private discussions we had, for the confidence you gave me, for the calm you exude, and for the many comments and questions you asked while working on my thesis.

In addition I would like to thank *Jun. Prof. Dr. Jeroen Sijsling*. First of all for our joint project. Without your foresight and your expertise, this project would not have been possible. I am also grateful for our meetings and discussions almost every weekend. You listened to me at a time when I had a lot of self-doubt and helped me regain my confidence.

I would like to thank *Andreas Pieper* for all of your mathematical questions and explanations that you have been asking and giving me for almost one year. Through you I got to know one of the most beautiful mathematical structures for me. Two sentences from you have accompanied me in our time: "Wrong" and "Very well done", and where I suppose the first happened more often than the second.

In addition I would like to thank *Prof. Dr. Uwe Schöning* for giving me my job and the freedom to do mathematics and develop where I wanted to develop myself.

I would like to thank *Elise Andréa Pollet* for her support in the years 2018 – 2020. Especially for getting to know you and that we made it possible to live together. I had a wonderful time with you in Amiens, and on all parts of the world that we have visited together. I will never forget this time and I will definitely never forget you.

In addition I would like to thank *Prof. Dr. Stefan Wewers* who introduced me as a student to the wonderful theory of algebraic geometry and algebraic number theory.

I would like to thank *Jeroen Hanselman* for our mathematical and private conversations, and for your beautiful drawings.

I would like to thank especially my parents, *Olimpia and Vasile (Bebe)*. Thank you for all the opportunities you have created for me. None of this would have been possible without your love and your self-sacrifice for your children.

In addition I would like to thank *Dr. Sorina Ionica* for our first joint project and the opportunity to do research. Thank you for giving me the topic that I could work on.

1

Abelian Varieties

There are several approaches to introduce the concept of the main objects in this thesis, *abelian varieties*: A purely algebraic concept and an analytic concept.

The first book that I have read about abelian varieties with complex multiplication was the book of Shimura [63]. I remember that at this time, it was during the preparation for my paper in [17], that one of the biggest difficulties I had was to understand the concept of polarizations. It would stay something "miraculous" to me for a while. Studying Shimura and Taniyama's construction of (principally) polarized abelian varieties with complex multiplication (CM), and having in mind elliptic curves as an example of abelian varieties with CM, does not necessarily explain immediately the need for polarization, especially because elliptic curves are always (principally) polarized. Another difficulty for me in connection with polarizations came from the multitude of descriptions for these objects. In order to try to better understand polarizations, especially in its multifaceted description, I began to study the book of Birkenhake and Lange [4]. Here I could get a better understanding for the several descriptions of polarizations, and maybe most of all the need to consider this structure, since *not* every complex torus admits a complex-analytic embedding into some projective space $\mathbb{P}^n_{\mathbb{C}}$.

Another difficulty I had at the beginning of my complex multiplication (CM) "journey", were the different equivalent ways of looking at the same objects. In my case in this thesis, these objects are simple (principally) polarized abelian varieties of dimension 2 and 3. The different perspectives on these objects are at the one side given by the construction of CM abelian varieties by Shimura and Taniyama in [63], and at the other side by their pure analytic construction of abelian varieties explained in [4, Chapters 1–4]. By a theorem of Ueno and Oort (see [57]), these objects are Jacobians of smooth projective curves of genus 2 and 3.

Another point where I "struggled" during my PhD was to understand the concept of *invariants* of smooth projective curves. The main focus in the paper [17] was to construct (so-called) *class polynomials*. In the case of elliptic curves with CM, this polynomial is the so-called *Hilbert class polynomial*. It is a monic polynomial whose roots are the j-invariants of all elliptic curves with CM by the maximal order $\mathcal{O}_K$ where K is a given CM field of degree 2 over $\mathbb{Q}$. In the case of Chapter 8 in this thesis , in order to compute class polynomials, I needed to understand the construction of the (so-called) *Rosenhain* and *Shioda* invariants of hyperelliptic curves of genus 3. In the non-hyperelliptic case, which we will also consider in Chapter 7 , we use instead the (so-called) *Dixmier-Ohno* invariants.

Based on my difficulties of understanding the concept of (principally) polarized abelian varieties (with CM), as well as the concept of invariants of smooth projective curves, I will try to give in the first 6 chapters of this thesis a brief introduction into this *elegant* and *fascinating theory*. At this moment, I will try as best I can to relate these chapters to each other, and to explain their need for the last 3 chapters of this thesis. I am sure that in a few years I will have a much deeper insight into these structures and that I will be able to describe them better than today.

In this chapter we discuss some basic properties of abelian varieties and their polarizations in a purely algebraic concept. We follow here [76, Chapters 2–7, 11, 14], respectively [49].

1.1 Definitions

For the rest of this chapter we denote by k an arbitrary field that we assume to be algebraically closed.

Definition 1.1.1. An *abelian variety* over k is a complete abelian group variety. We call an abelian variety A over k *simple* if A has no non-zero proper subvarieties. If A is a (simple) abelian variety over k then the set $A(k)$ of *k-rational points* naturally inherits the structure of an abelian group. See [49, Page 8 and Corollary 1.4] or [76, Definition 1.3], respectively.

Before continuing our discussion, we consider the main examples of abelian varieties in this thesis.

Example 1.1.2. (i) Elliptic curves are abelian varieties of dimension one. Over the complex numbers this follows e.g. from [65, Chapter 6, Corollary 5.1.1].

(ii) The Jacobian $\mathrm{Jac}(X)$ of a smooth projective curve X of genus g is an abelian variety of dimension g, see e.g. [57].

(iii) A product of elliptic curves $E_1 \times \ldots \times E_g$ is an abelian variety. For the case where the E_i are supersingular elliptic curves, see [46].

As usual in algebra, where morphisms between algebraic structures are considered, we consider in our case homomorphisms (isogenies, more precisely) between abelian varieties.

Definition 1.1.3. A homomorphism $\rho : A \to A'$ between abelian varieties is called an *isogeny* if ρ is surjective and $\ker(\rho)$ is finite. The *degree* of an isogeny is the degree of the function field extension $k(A)$ over $k(A')$.

Remark 1.1.4. In a more general context, the right notion is for $\ker(\rho)$ to be a finite group scheme. We will consider this in the context of polarized supersingular abelian varieties over algebraically closed fields k in positive characteristic. See Chapter 9.

Remark 1.1.5. In this thesis we consider the following polarized abelian varieties:

(i) In the Chapters 3, 7 and 8: Jacobian of smooth projective curves curves of genus 3.

(ii) In Chapter 9: Polarized flag type quotients (see Definition 9.2.1)

$$\left(\left(Y_{g-1} = E^g, \eta_{g-1}\right) \xrightarrow{\rho_{g-1}} \left(Y_{g-2}, \eta_{g-2}\right) \xrightarrow{\rho_{g-2}} \ldots \longrightarrow (Y_1, \eta_1) \xrightarrow{\rho_1} (Y_0 = Y, \eta_0)\right)$$

where (Y_i, η_i) are polarized abelian varieties of dimension g over algebraically closed fields of positive characteristic $p > 0$, together with isogenies ρ_i such that $\ker(\rho_i)$ is an α-group (see Definition B.1.1) of rank i for $1 \leq i \leq g-1$, and where E is a supersingular elliptic curve over $\mathbb{F}_p$.

1.2 The dual abelian variety and polarizations

In this section we recall the notion of the dual abelian variety of A, and of the polarization on A.

In order to define polarizations on abelian varieties A of arbitrary dimension g over algebraically closed fields k, we recall here the following special case:

Let $(E,\mathcal{O})$ be an elliptic curve over k and let $\mathrm{Pic}^0(E) = \mathrm{Pic}^0_k(E)$ be the group of equivalence classes of degree-0 line bundles on E. Then

$$\begin{aligned} \eta : E(k) &\xrightarrow{\sim} \mathrm{Pic}^0(E) \\ P &\mapsto ([\mathcal{O}] - [P]) \end{aligned}$$

defines an isomorphism between the group of k-rational points $E(k)$ and $\mathrm{Pic}^0(E)$. We call η a principal polarization on E.

Definition 1.2.1. Let A be an abelian variety of dimension g over k and let $\mathrm{Pic}^0(A) = \mathrm{Pic}^0_k(A)$ be the group of equivalence classes of degree-0 line bundles on A. It is an abelian variety over k, we call it the *dual (abelian) variety* of A and denote it by A^t. See [76, Theorem 6.18].

Remark 1.2.2. Any homomorphism $\rho : A \to A'$ of abelian varieties induces an homomorphism $\rho^t : (A')^t \to A^t$ between the dual abelian varieties, see [76, Definition 6.19].

For any line bundle $\mathscr{L}$ on an abelian variety A over k, we define the map

$$\begin{aligned} \varphi_{\mathscr{L}} : A &\to A^t \\ x &\mapsto [t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}], \end{aligned} \tag{1.2.1}$$

where t_x corresponds to the translation by x-map on $A(k)$. If $\mathscr{L}$ is ample then $\varphi_{\mathscr{L}}$ is an isogeny, see [76, Theorem 6.18].

Definition 1.2.3. We define a *polarization* on an abelian variety A over an algebraically closed field k as an isogeny $\eta = \varphi_{\mathscr{L}}$ where $\mathscr{L}$ is a certain class of ample line bundle on A modulo algebraic equivalence, see [76, Chapter 11.1]. If η is an isomorphism then we call it a *principal polarization*.

Definition 1.2.4. A tuple (A,η) where A is an abelian variety over k and η a polarization on A is called a *polarized abelian variety*. If η is a principal polarization on A, then we call (A,η) a *principally polarized abelian variety*.

1.3 Pairings

Notation 1.3.1. We denote by $\mathbb{G}_m = \mathbb{G}_{m,k} = \mathrm{Spec}(k[x,x^{-1}])$ the *multiplicative group scheme* over k, see Example B.0.5.

Notation 1.3.2. If $\rho : A \to A'$ is an isogeny with finite k-group scheme $\ker(\rho)$, then we denote by $\ker(\rho)^D$ the *Cartier dual* of $\ker(\rho)$, see [76, Chapter 3.21].

Notation 1.3.3. If $\rho : A \to A'$ is an isogeny then we denote by $\rho^t : (A')^t \to A^t$ the *dual isogeny*. It is induced by ρ and it is given by pullback of line bundles. See [76, Chapter 7.2].

Definition 1.3.4. Let $\rho : A \to A'$ be an isogeny of abelian varieties over k. Then there is an isomorphism of finite k-group schemes $\beta : \ker(\rho^t) \xrightarrow{\sim} \ker(\rho)^D$, and we define a non-degenerate, skew-symmetric perfect pairing to ρ, which is on points given by

$$\begin{aligned} \langle , \rangle_\rho : \ker(\rho) \times \ker(\rho^t) &\to \mathbb{G}_m \\ (x,y) &\mapsto \langle x,y\rangle_\rho := \beta(y)(x). \end{aligned}$$

If n is a positive integer and if $\ker(\rho)$ is killed by n, then $\langle , \rangle_\rho$ has values in the affine group scheme of the n-roots of unity, $\mu_{n,k} \subset \mathbb{G}_{m,k}$.

If $A' = A$ and $\rho = n : A \to A$, then the assigned pairing to the multiplication by n-map

$$\langle , \rangle_n : A[n] \times A^t[n] \to \mu_n$$

is called the *Weil pairing*. It is a perfect pairing.

If $A' = A^t$ and $\rho = \eta : A \to A^t$ is a polarization, then we obtain (with this additional structure) a pairing

$$\begin{aligned} \langle , \rangle_n^\eta : A[n] \times A[n] &\to \mu_n \\ (x, y) &\mapsto \langle x, y \rangle_n^\eta := \langle x, \eta(y) \rangle_n. \end{aligned}$$

If n is relatively prime to $\deg(\eta)$ then it is a perfect pairing. See [76, Definition 11.11].

Proposition 1.3.5. *If $\eta : A \to A^t$ is a polarization and if $\rho : A \to A'$ is an isogeny, then there is a unique polarization $\eta' : A' \to (A')^t$ that makes the following diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{\rho} & A' \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta'} \\ A^t & \xleftarrow[\rho^t]{} & (A')^t \end{array}$$

if and only if $\ker(\rho) \subset \ker(\eta)$ *is totally isotropic with respect to the pairing $\langle , \rangle_\eta$ in Definition 1.3.4.*

Proof. See [76, Prop. 11.25]. □

2 Abelian Varieties over $\mathbb{C}$

In the next chapter we discuss the analytic perspective on abelian varieties and their polarizations. We follow [4, Chapter 1–4, 11].

2.1 Complex tori

In this chapter we fix our ground field to be the field of complex numbers $\mathbb{C}$.[1] A g-dimensional *complex torus* is a quotient of a complex vector space V of dimension g by a *lattice* $\Lambda \subset V$. This means that Λ is a discrete subgroup of V such that

$$\Lambda \cong \mathbb{Z}^{2g}, \quad \text{and} \quad \Lambda\mathbb{R} = V.$$

Remark 2.1.1. The analytic perspective on abelian varieties includes some restrictions which we will elucidate in the follows, since not every complex torus admits a complex-analytic embedding into some projective space $\mathbb{P}^n_{\mathbb{C}}$, see i.e. [29, Example A.5.0.3.b]. The complex tori admitting such an embedding possess an extra structure.

Definition 2.1.2. Let $A = V/\Lambda$ be a complex torus, where V is a complex vector space of dimension g and Λ a lattice in V. Choose a basis $e_1, \dots, e_g$ for V, and a basis $\lambda_1, \dots, \lambda_{2g}$ for Λ. We write $\lambda_i = \sum_{j=1}^{g} \lambda_{j,i} e_j$. Consider the matrix

$$\Pi = \begin{bmatrix} \lambda_{1,1} & \dots & \dots & \lambda_{1,2g} \\ \vdots & & & \vdots \\ \lambda_{g,1} & \dots & \dots & \lambda_{g,2g} \end{bmatrix} \tag{2.1.1}$$

in $\mathrm{Mat}_{g,2g}(\mathbb{C})$. We call Π a *big period matrix* for the complex torus A. The former fully determines the latter, but given A, the matrix Π depends on the choice of the bases for V and Λ, see [4, page 9].

In the previous chapter we discussed some properties of morphisms (especially isogenies) of abelian varieties in the "algebraic language". We discuss here the analogue in the "analytic language" by using holomorphic maps between complex tori.

Definition 2.1.3. Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be complex tori over $\mathbb{C}$ of dimensions g and g'. A *homomorphism* of A to A' is a holomorphic map $\rho : A \to A'$, compatible with the additive group structure of A and A'. The *translation by an element* $x \in A$ is defined to be the holomorphic map $t_x : A \to A,\ y \mapsto y + x$. See [4, page 10].

Proposition 2.1.4. *Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be complex tori over $\mathbb{C}$ of dimensions g and g'. Let $\rho : A \to A'$ be a homomorphism. Then there exists a unique $\mathbb{C}$-linear map T_ρ that makes the following diagram commute:*

$$\begin{array}{ccc} V & \xrightarrow{T_\rho} & V' \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_{A'}} \\ A & \xrightarrow{\rho} & A' \end{array} \tag{2.1.2}$$

[1] Also for abelian varieties over number fields, we will often need to consider these over $\mathbb{C}$ in order to apply complex-analytic techniques as in Chapters 7 and 8.

Here $\pi_A, \pi_{A'}$ are the canonical projection maps. Moreover, $T_\rho(\Lambda) \subset \Lambda'$ and the restriction $T_\rho|_\Lambda : \Lambda \to \Lambda'$ is a $\mathbb{Z}$-linear map between Λ and Λ'. See [4, Proposition 1.2.1].

Definition 2.1.5. Let $A = V/\Lambda$ and $A' = V/\Lambda'$ be complex tori of dimensions g over $\mathbb{C}$. A homomorphism $\rho : A \to A'$ is called an *isogeny* if ρ is surjective and $\ker(\rho)$ is finite. The *degree* of an isogeny ρ is the cardinality of the kernel of ρ. See [4, page 12].

Example 2.1.6. Let $[n] : A = V/\Lambda \to A,\ x \mapsto nx$ be the multiplication by $n \in \mathbb{Z}_{\geq 1}$-map. Then $[n]$ is an isogeny of degree n^{2g}, with kernel given by

$$\ker([n]) = \left(\frac{1}{n}\right)\Lambda/\Lambda \cong (\mathbb{Z}/2\mathbb{Z})^{2g}.$$

See [4, Proposition 1.2.5].

Proposition 2.1.7. *Let $\rho : A = V/\Lambda \to A' = V/\Lambda'$ be an isogeny between complex tori. If $\deg(\rho) = d$, then there exists a unique isogeny $\psi : A' \to A$, such that the multiplication by d-map factors as*

$$[d]_A = (A \xrightarrow{\rho} A' \xrightarrow{\psi} A)$$
$$[d]_{A'} = (A' \xrightarrow{\psi} A \xrightarrow{\rho} A').$$

We call ψ the dual isogeny *and denote it by $\psi := \rho^t$.*

Proof. See [4, Proposition 1.2.6]. □

2.2 Line bundles on complex tori

As mentioned in the introduction of this chapter, not every complex torus gives rise to an abelian variety over $\mathbb{C}$. An abelian variety A over $\mathbb{C}$ is a complex torus V/Λ admitting an ample line bundle. Then A comes equipped with an algebraic embedding $\iota : A \hookrightarrow \mathbb{P}^n_{\mathbb{C}}$. The embedding ι is associated to an ample line bundle $\mathscr{L}$ on V/Λ. In order to understand which complex tori admit an embedding into a projective space we need to describe (ample) line bundles on V/Λ.

Lemma 2.2.1. *Let V be a complex vector space. There is a bijection between the set of hermitian forms H on V and the set of real valued alternating forms E on V with $E(iv, iw) = E(v, w)$, given by*

$$E(v, w) = \operatorname{Im} H(v, w)$$
$$H(v, w) = E(iv, w) + iE(v, w),$$

where $\operatorname{Im} H$ is the imaginary part of the hermitian form H.

Proof. See [4, Lemma 2.1.7]. □

Definition 2.2.2. Let $A = V/\Lambda$ be a complex torus and let H be a hermitian form on V with real alternating form $E = \operatorname{Im} H$ with $E(\Lambda, \Lambda) \subset \mathbb{Z}$. Let $\chi : \Lambda \to \mathbb{C}_1 = \{z \in \mathbb{C} : |z| = 1\}$ be a map satisfying

$$\chi(\lambda + \mu) = \chi(\lambda)\chi(\mu) \cdot e^{(\pi i E(\lambda, \mu))}$$

for all $\lambda, \mu \in \Lambda$. There is a well-defined action of Λ on $V \times \mathbb{C}$ given by

$$a_\lambda(v, t) = (v + \lambda, t \cdot \chi(\lambda) \cdot e^{(\pi H(v,\lambda) + \frac{\pi}{2} H(\lambda,\lambda))}). \tag{2.2.1}$$

for $\lambda \in \Lambda$ and $(v, t) \in V \times \mathbb{C}$. We define by $\mathscr{L}(H, \chi)$ to be the line bundle given by the quotient $(V \times \mathbb{C})/\Lambda$ for the action in Equation (2.2.1). See [4, Chapter 2.2] or [53, page 20–21], respectively.

Theorem 2.2.3 (Appell-Humbert)**.** *Let $A = V/\Lambda$ be a complex torus. Any line bundle $\mathscr{L}$ on A is isomorphic to an $\mathscr{L}(H,\chi)$ for a unique tuple (H,χ) as in Definition 2.2.2. Furthermore the class of $\mathscr{L}(H,\chi)$ modulo algebraic equivalence only depends on the choice of the hermitian form H.*

Proof. See [4, Theorem 2.2.3]. □

2.3 The Riemann relations

By the Appell-Humbert Theorem we have identified line bundles on complex tori $A = V/\Lambda$ by equivalence classes of line bundles $\mathscr{L}(H,\chi)$, which are uniquely determined by hermitian forms H on V with $\operatorname{Im} H(\Lambda,\Lambda) \subseteq \mathbb{Z}$. We relate the ampleness condition on line bundles on A to properties of the hermitian forms H on V. In this subsection we follow the discussion in [4, Chapters 3.1 and 4.2] or [53, Chapter 1], respectively.

Definition 2.3.1. An *abelian variety* $A = V/\Lambda$ of dimension g over $\mathbb{C}$, is a g-dimensional complex torus V/Λ admitting an ample line bundle.

Theorem 2.3.2. *Let $A = V/\Lambda$ be a g-dimensional complex torus and let $\Pi \in \mathrm{Mat}_{g,2g}(\mathbb{C})$ be the big period matrix for some bases of V respectively of Λ (see Definition 2.1.2). Then A is an abelian variety if and only if there is a non-degenerate alternating matrix $M \in \mathrm{Mat}_{2g}(\mathbb{Z})$ such that*

(i) $\Pi M^{-1}\Pi^t = 0$,

(ii) $i\Pi M^{-1}\overline{\Pi}^t > 0$,

where $\overline{\Pi}$ corresponds to the complex conjugate matrix.

Proof. See [4, Theorem 4.2.1]. □

It turns out that the matrix $M \in \mathrm{Mat}_{2g}(\mathbb{Z})$ in Theorem 2.3.2 is the matrix of the alternating form defining the polarization.

Lemma 2.3.3. *Let $A = V/\Lambda$ be g-dimensional complex torus. Let $\Pi \in \mathrm{Mat}_{g,2g}(\mathbb{C})$ be a big big period matrix for some bases $e_1,\dots,e_g$ of V and $\lambda_1,\dots,\lambda_{2g}$ of Λ. Let E be a non-degenerate alternating form on Λ and let M_E be the matrix representation of E with respect to the basis $\lambda_1,\dots,\lambda_{2g}$. Extend E to a map $H : V \times V \to \mathbb{C}$ by*

$$H(v,w) = E(iv,w) + iE(v,w).$$

Then:

(i) H is a hermitian form on V if and only if $\Pi M_E^{-1}\Pi^t = 0$,

(ii) H is positive definite if and only if $i\Pi M^{-1}\overline{\Pi}^t > 0$.

Proof. See [4, Lemmas 4.2.2 and 4.2.3]. □

Theorem 2.3.4 (Lefschetz)**.** *Let $A = V/\Lambda$ be a g-dimensional complex torus, H an hermitian form on V such that $E = \operatorname{Im} H$ and $E(\Lambda,\Lambda) \subset \mathbb{Z}$. Let a_λ be the function in Definition 2.2.2 and let $\mathscr{L}(H,\chi)$ the associated line bundle on A. Then $\mathscr{L}(H,\chi)$ is ample if and only if H is positive definite.*

Proof. Follows from [53, page 29]. □

Lemma 2.3.5 (Frobenius). *Let $A = V/\Lambda$ be a g-dimensional complex torus, H an hermitian form on V such that $E = \operatorname{Im} H$ and $E(\Lambda, \Lambda) \subset \mathbb{Z}$. There exists a basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ of Λ and positive integers $d_1, \ldots, d_g$ satisfying $d_i \mid d_{i+1}$ and such that if we set $D = \operatorname{diag}(d_1, \ldots, d_g)$ then the matrix representation of E with respect to this basis is given by the matrix*

$$\begin{bmatrix} 0 & D \\ -D & 0 \end{bmatrix}. \tag{2.3.1}$$

Proof. See [29, Lemma A.5.3.1]. □

Definition 2.3.6. Let $A = V/\Lambda$ be a g-dimensional complex torus, H an hermitian form on V such that $E = \operatorname{Im} H$ and $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$. Let $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ be a basis of Λ and let $d_1, \ldots, d_g$ be positive integers satisfying $d_i | d_{i+1}$. We call the basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ with these properties a *symplectic basis* of Λ for H (for E, respectively). We call the coefficients d_i *elementary divisors*, and we call $D = \operatorname{diag}(d_1, \ldots, d_g)$ the *type* of the line bundle $\mathscr{L}$ on A associated to H. See [4, Chapter 3.1].

2.4 The dual abelian variety and polarizations

In order to define polarizations on complex abelian varieties, we begin this section by discussing properties of the dual abelian variety A^t of an abelian variety $A = V/\Lambda$ over $\mathbb{C}$. We follow [4, Chapter 2.4] or [53, Chapter 2.9], respectively.

Definition 2.4.1. If V is a complex vector space, then a function $f : V \to V$ is called $\mathbb{C}$-*antilinear* if

$$f(\alpha u + \beta v) = \overline{\alpha} f(u) + \overline{\beta} f(v)$$

for all $u, v \in V$ and $\alpha, \beta \in \mathbb{C}$ where $\overline{(*)}$ denotes complex conjugation.

Let $A = V/\Lambda$ be an abelian variety of dimension g over $\mathbb{C}$. By following [4, page 34] we consider the *dual vector space* $V^t = \operatorname{Hom}_{\mathbb{C}\text{–antilinear}}(V, \mathbb{C})$ of V, together with a canonical non-degenerate $\mathbb{R}$-bilinear form

$$\begin{aligned} \langle , \rangle : V^t \times V &\to \mathbb{R} \\ (l, v) &\mapsto \langle l, v \rangle := \operatorname{Im} l(v). \end{aligned}$$

Then the *dual lattice* Λ^t of Λ is given by

$$\Lambda^t = \{ l \in V^t : \langle l, v \rangle \subseteq \mathbb{Z} \}.$$

We define the *dual torus* as the quotient

$$A^t = V^t / \Lambda^t. \tag{2.4.1}$$

It is a complex torus of dimension g over $\mathbb{C}$. We identify A^t with $\operatorname{Pic}^0(A)$ (see Definition 1.2.1) via the isomorphism

$$\ell \mapsto \mathscr{L}\left(0, v \mapsto e^{2\pi i \langle \ell, v \rangle}\right),$$

see [4, Proposition 2.4.1].

In Chapter 1, we have defined (see Equation (1.2.1)) for any line bundle $\mathscr{L}$ on an abelian variety A over an arbitrary field $k = \overline{k}$, the map

$$\begin{aligned} \varphi_{\mathscr{L}} : A &\to A^t \\ x &\mapsto [t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}], \end{aligned}$$

where t_x corresponds to the translation by x-map on $A(k)$, and where $\varphi_{\mathscr{L}}$ is an isogeny if $\mathscr{L}$ is ample. We defined a polarization on A over k (see Definition 1.2.3) as an isogeny $\eta = \varphi_{\mathscr{L}}$ where $\mathscr{L}$ is a certain class of ample line bundle on A modulo algebraic equivalence.

We briefly explain the analytic correspondence of the map $\varphi_{\mathscr{L}}$ and refer here to [4, Chapter 2].

Lemma 2.4.2. *Let $A = V/\Lambda$ be an abelian variety over $\mathbb{C}$ and let $\mathscr{L} = \mathscr{L}(H, \chi)$ be a line bundle on A, where H is a hermitian form on V such that $E = \operatorname{Im} H$ and where $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$. The map*

$$\begin{aligned} \varphi_H : V &\to V^t \\ x &\mapsto \varphi_H(x) = H(x, \cdot) \end{aligned}$$

is the analytic representation of $\varphi_{\mathscr{L}}$, and for $\overline{x} \in A(\mathbb{C})$ with representative $x \in V$ we get

$$t_{\overline{x}}^*\mathscr{L} \otimes \mathscr{L} = \mathscr{L}\left(0, v \mapsto e^{2\pi i E(x,v)}\right) = \mathscr{L}\left(0, v \mapsto e^{2\pi i \langle \varphi_H(x), v\rangle}\right).$$

Further $\varphi_{\mathscr{L}}$ is an isogeny if the hermitian form H (or equivalently E) is positive definite.

Proof. See [4, Lemma 2.4.5]. □

Definition 2.4.3. We define a *polarization* on an abelian variety $A = V/\Lambda$ over $\mathbb{C}$ as an isogeny $\eta = \varphi_{\mathscr{L}}$, where $\mathscr{L} = \mathscr{L}(H, \chi)$ is a certain ample line bundle on A modulo analytic equivalence, see [4, page 39]. The *degree* of a polarization η is the determinant $\det(E)$ of the positive definite form $E = \operatorname{Im} H$ with $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$. In this case we call E a *Riemann form* to Λ. If η is an isomorphism, then we call it a *principal polarization*.

Definition 2.4.4. If η is a principal polarization on an abelian variety $A = V/\Lambda$ over $\mathbb{C}$, then by Lemma 2.3.5 there is a symplectic basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ for Λ such that the representation matrix of the Riemann form E with respect to this basis is given by the matrix

$$J_g = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix}, \tag{2.4.2}$$

where I_g is the identity matrix. A basis of Λ with this properties is called a *standard symplectic basis*.

Definition 2.4.5. A tuple (A, η) where $A = V/\Lambda$ is an abelian variety over $\mathbb{C}$ and η a polarization on A is called a *polarized abelian variety* over $\mathbb{C}$. If η is a principal polarization on A, then we call (A, η) a *principally polarized abelian variety* over $\mathbb{C}$.

Remark 2.4.6. In the further course of this thesis, depending on the context, we describe polarized abelian varieties over $\mathbb{C}$ by tuples

$$(A, E) \tag{2.4.3}$$

instead, where $A = V/\Lambda$ is a complex torus for some complex vector spaces V of dimension g and some full lattices Λ in V, and where $E = \operatorname{Im} H$ for some ample line bundle $\mathscr{L} = \mathscr{L}(H, \chi)$. By the above, E determines a polarization η on A.

2.5 Pairings

To connect the theory in this Chapter to the one in Chapter 1, we give an explicit description of bilinear forms attached to isogenous abelian varieties over $\mathbb{C}$.

Notation 2.5.1. If $\rho : A \to A'$ is an isogeny of complex tori then we denote by $\rho^t : (A')^t \to A^t$ the *dual isogeny* of ρ, see [4, Chapter 2.4]. We denote by $\ker(\rho)^D$ the *Cartier dual* of $\ker(\rho)$, see Notation 1.3.2.

Proposition 2.5.2. *Let $\rho : A = V/\Lambda \to A' = V/\Lambda'$ be an isogeny and let $\rho^t : (A')^t \to A^t$ be its dual. If $\beta : \ker(\rho^t) \xrightarrow{\sim} \ker(\rho)^D$ is the $\mathbb{C}$-group schemes isomorphism in Definition 1.3.4, then the analytic representation of β is given by*

$$\left(0, e^{2\pi i \omega}\right) \mapsto \left(\lambda \mapsto e^{2\pi i \cdot \omega \circ \rho(\lambda)}\right),$$

where $\omega : V' \to \mathbb{C}$ is an anti-linear map with $\omega(\Lambda', \Lambda') \subseteq \mathbb{Z}$.

Proof. See [28, Proposition 3.1.18]. □

Let $(A = V/\Lambda, \eta)$ be a polarized abelian variety of dimension g over $\mathbb{C}$. The analytic description of the pairing $\langle , \rangle_n^\eta$ in Definition 1.3.4 is given by

$$\left\langle \frac{1}{n}\lambda_1, \frac{1}{n}\lambda_2 \right\rangle_n^\eta = e^{2\pi i \frac{1}{n} E(\lambda_1, \lambda_2)}$$

for $\lambda_i \in \Lambda$, see [28, Proposition 3.1.20].

2.6 Endomorphisms of abelian varieties

In this section, we follow [4, Chapters 1 and 5] and discuss some basic properties of homomorphisms between complex abelian varieties. Then, we restrict to the structure of the algebra $\mathrm{End}^0(A)$ respectively to the ring $\mathrm{End}(A)$ of abelian varieties A of dimension g over $\mathbb{C}$.

Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be abelian varieties over $\mathbb{C}$ of dimensions g and g'. Let

$$\rho : A \to A'$$

be an element in $\mathrm{Hom}(A, A')$, where the latter is the set of all homomorphisms from A to A' equipped with the operation given by the addition. Then by Proposition 2.1.4, ρ uniquely determines a $\mathbb{C}$-linear map

$$T_\rho : V \to V'$$

that makes the Diagram 2.1.2 commute. We obtain an injective homomorphism of abelian groups

$$\begin{aligned} \iota_a : \mathrm{Hom}(A, A') &\to \mathrm{Hom}_{\mathbb{C}}(V, V') \\ \rho &\mapsto T_\rho \end{aligned} \tag{2.6.1}$$

called the *analytic representation* of $\mathrm{Hom}(A, A')$. Moreover, since $T_\rho(\Lambda) \subset \Lambda'$ and the restriction $T_\rho|_\Lambda : \Lambda \to \Lambda'$ is a $\mathbb{Z}$-linear map between Λ and Λ', there is an injective homomorphism

$$\begin{aligned} \iota_r : \mathrm{Hom}(A, A') &\to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda') \\ \rho &\mapsto T_\rho|_\Lambda \end{aligned} \tag{2.6.2}$$

called the *rational representation* of $\mathrm{Hom}(A, A')$, and where the latter is (as abelian group) free of rank $m \leq 4gg'$, see [4, Proposition 1.2.2].

Let Π and Π' be big period matrices of $A = V/\Lambda$ and $A' = V'/\Lambda'$ with respect to some bases of V, Λ and V', Λ' respectively. Let $\rho : A \to A'$ be a homomorphism. Then the linear transformation $\iota_a(\rho)$ in Equation (2.6.1) is given by a matrix $M_a \in \mathrm{Mat}_{g',g}(\mathbb{C})$ with respect to the chosen bases. Similarly the representation of $\iota_r(\rho)$ is given by a matrix $M_r \in \mathrm{Mat}_{2g',2g}(\mathbb{Z})$. In terms of matrices the condition $\iota_a(\rho)(\Lambda) \subset \Lambda'$ corresponds to

$$M_a \Pi = \Pi' M_r. \tag{2.6.3}$$

Conversely, any two matrices $M_a \in \mathrm{Mat}_{g',g}(\mathbb{C})$ and $M_r \in \mathrm{Mat}_{2g',2g}(\mathbb{Z})$ satisfying the relation in Equation (2.6.3) define a homomorphism $A \to A'$. The matrices M_a and M_r determine one another.

By following the discussion in [4, Chapter 5], we describe the endomorphism algebra of polarized abelian varieties over $\mathbb{C}$. Let A be an abelian variety of dimension g over $\mathbb{C}$. Then ι_a and ι_r (see Equations (2.6.1) and (2.6.2)) are representations of the *endomorphism ring* $\mathrm{End}(A)$. The latter is the set of all isogenies $\rho : A \to A$ (see Definition 2.1.5) with ring structure given by addition and composition. Let

$$\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \tag{2.6.4}$$

be the *endomorphism algebra* of A.

Proposition 2.6.1. *If A and A' are isogenous abelian varieties, then* $\mathrm{End}^0(A) \cong \mathrm{End}^0(A')$.

Proof. See [4, Chapter 5]. □

We recall (see introduction to Chapter 1), that an abelian variety A is called *simple*, if A has no non-zero proper subvarieties. In other words, the only subvarieties of A are A itself, and 0.

Theorem 2.6.2 (Poincaré's Complete Reducibility Theorem)**.** *Given an abelian variety A there is an isogeny*

$$A \to A_1^{n_1} \times \ldots \times A_r^{n_r}$$

where the A_i are simple abelian varieties that are pairwise non-isogenous to each other, and where the n_i are uniquely determined up to permutations, and where the A_i are determined up to isogeny.

Proof. See [4, Theorem 5.3.7]. □

Corollary 2.6.3. $\mathrm{End}^0(A)$ *is a finite dimensional semisimple $\mathbb{Q}$-algebra, i.e. if $A \to A_1^{n_1} \times \ldots \times A_r^{n_r}$ is an isogeny as in Theorem 2.6.2, then*

$$\mathrm{End}^0(A) \cong \mathsf{M}_{n_1}(F_1) \oplus \ldots \oplus \mathsf{M}_{n_r}(F_r),$$

where the M_{n_i} are matrix algebras *over F_i, where the $F_i = \mathrm{End}^0(A_i)$ are skew fields of finite dimension over $\mathbb{Q}$.*

Remark 2.6.4. From the corollary above, the classification of endomorphism algebras of abelian varieties reduces to the classification of simple abelian varieties. We consider in this thesis simple principally polarized abelian varieties $A = \mathrm{Jac}(X)$, where $\mathrm{Jac}(X)$ is the Jacobian (variety) of a smooth projective curve of genus 3 over $\mathbb{C}$ (respectively over number fields), see Chapter 3.

Let $(A = V/\Lambda, E) = (A, \eta)$ be a simple polarized abelian variety of dimension g over $\mathbb{C}$, as in Equation (6.2.5). By Proposition 2.1.7, there is a unique isogeny $\eta^t : A^t \to A$ corresponding to the multiplication by an integer d on A and A^t respectively. Then η has an inverse in $\mathrm{Hom}(A^t, A) \otimes \mathbb{Q}$, namely

$$\eta^{-1} = d^{-1}\eta^t.$$

Every $\widetilde{\rho} \in \mathrm{End}^0(A)$ can be uniquely (up to isomorphism) written as $\widetilde{\rho} = r\rho$ with $r \in \mathbb{Q}$ and $\rho \in \mathrm{End}(A)$. Then the dual of $\widetilde{\rho}$ is defined as $\widetilde{\rho}^t = r\rho^t \in \mathrm{End}^0(A^t)$.

Definition 2.6.5. We define the *Rosati involution* (with respect to $\mathscr{L}$ (or with respect to η)) to be

$$\widetilde{\rho}^\dagger = \eta^{-1} \circ \widetilde{\rho}^t \circ \eta. \tag{2.6.5}$$

It is an anti-involution on $\mathrm{End}^0(A)$, see [4, page 114].

Notation 2.6.6. In the rest of this chapter, $(F, \dagger)$ denotes a pair with $F = \mathrm{End}^0(A)$ is the endomorphism algebra of a simple polarized abelian variety $A = V/\Lambda$ of dimension g over $\mathbb{C}$ with polarization η, and where $\dagger$ is a Rosati involution on F with respect to η.

Notation 2.6.7. Let $(F, \dagger)$ be a pair as in Notation 2.6.6. The anti-involution $\dagger : F \to F$ restricts to an involution on the *center* K of F, whose *fixed field* under the involution we denote by K_0.

Lemma 2.6.8. *K_0 is a totally real number field, i.e. any embedding $K_0 \hookrightarrow \mathbb{C}$ factorizes via $\mathbb{R}$.*

Proof. See [4, Lemma 5.5.2]. □

Definition 2.6.9. We say $(F, \dagger)$ is *of the first kind* if $K = K_0$, and of *the second kind* otherwise.

For the rest of this thesis we restrict to tuples $(F, \dagger)$ of the second kind. The reason here for is based on the following lemma.

Lemma 2.6.10. *Let $(F, \dagger)$ to be of the second kind. Then the center K is totally complex, i.e. there is no embedding $K \hookrightarrow \mathbb{C}$ which factors via $\mathbb{R}$, and the restriction of the involution $\dagger|_K$ is complex conjugation.*

Proof. See [4, Lemma 5.5.4]. □

Example 2.6.11. If (A, E) is a principally polarized abelian variety of dimension g over $\mathbb{C}$ (respectively over some number fields) with *complex multiplication* by a number field K, then there is an embedding

$$\iota : K \hookrightarrow F = \mathrm{End}^0(A)$$

and $\iota(K) \subset F$ is the center of F in Lemma 2.6.10. By the same lemma, the restriction of the Rosati involution $\dagger|_K$ is complex conjugation on K.

2.7 The Siegel upper half space

In this section we recall the identification of principally polarized abelian varieties of dimension g over $\mathbb{C}$ by points in the Siegel upper half space $\mathcal{H}_g$. Further we define the (analytic) moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g over $\mathbb{C}$.

Let $(A = V/\Lambda, E)$ be a principally polarized abelian variety of dimension g over $\mathbb{C}$. Let Π be a big period matrix of A (see Definition 2.1.2) with respect to a standard symplectic basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ of Λ, such that the representation matrix of E with respect to this basis is given by the matrix in Equation (2.4.2). With respect to these basis the big period matrix of A is of the form

$$\Pi = (Z, I_g) \tag{2.7.1}$$

for some $Z \in \mathrm{Mat}_g(\mathbb{C})$ such that $Z^t = Z$ and $\mathfrak{Im}\, Z > 0$, and where I_g is the identity matrix, see [4, page 210]. We call the matrix Z a *(small) period matrix* of A.

Definition 2.7.1. We define the *Siegel upper half space* by

$$\mathcal{H}_g = \left\{ Z \in \mathrm{Mat}_g(\mathbb{C}) : Z^t = Z,\ \mathfrak{Im}(Z) > 0 \right\}. \tag{2.7.2}$$

Definition 2.7.2. We say that a principally polarized abelian variety $(A = V/\Lambda, E)$ of dimension g over $\mathbb{C}$ has period matrix $Z \in \mathcal{H}_g$, if

$$A(\mathbb{C}) \cong V/(Z\mathbb{Z}^g + \mathbb{Z}^g),$$

and the matrix representation for Riemann form E with respect to a standard symplectic basis of Λ is given by Equation (2.4.2).

In order to define equivalence classes of principally polarized abelian varieties of dimension g over $\mathbb{C}$, we give the following definition.

Definition 2.7.3. We define the *symplectic group* by

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \left\{ M \in \mathrm{GL}_{2g}(\mathbb{Z}) : M^T J_g M = J_g \right\},$$

where J_g is the matrix in Equation (2.4.2). There is an action (from left) of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on the Siegel upper half-space $\mathcal{H}_g$ given by

$$Z \longmapsto M.Z = (aZ + b)(cZ + d)^{-1}$$

for all $Z \in \mathcal{H}_g$ and $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$.

In the further course of this thesis (especially in Chapter 4), we need an explicit description of the $n_{\geq 2}$-torsion points on $A(\mathbb{C})$.

Lemma 2.7.4. *If $(A = V/\Lambda, E)$ is a (principally) polarized abelian variety of dimension g over $\mathbb{C}$ with a small period matrix $Z \in \mathcal{H}_g$, where $\Lambda = \Pi\mathbb{Z}^g$ and $\Pi = (Z, I_g)$, then for any positive integer n, the group of n-torsion points of A is given by*

$$A[n](\mathbb{C}) = \left\{ \xi = Z \cdot \xi_1 + I_g \cdot \xi_2 \pmod{Z\mathbb{Z}^g + \mathbb{Z}^g} : \xi_i \in \frac{1}{n}\mathbb{Z}^g \right\}.$$

Proof. Clear from Example 2.1.6, together with the identification of points on the torus $A = V/(Z\mathbb{Z}^g + \mathbb{Z}^g)$, given by $\omega = (Z, I_g)\xi = Z \cdot \xi_1 + I_g \cdot \xi_2$ for $\xi = \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \in \mathbb{R}^{2g}$. □

Proposition 2.7.5. *Let (A, E_Z) and $(A', E_{Z'})$ be (principally) polarized abelian varieties of dimension g over $\mathbb{C}$ for some period matrices $Z, Z' \in \mathcal{H}_g$. Then (A, E_Z) and $(A', E_{Z'})$ are isomorphic as (principally) polarized abelian varieties if and only if $Z' = M.Z$ for some $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$.*

Proof. See [4, Chapter 8.2]. □

The above proposition motivates the following definition and remark.

Definition 2.7.6. The *(analytic) moduli space of principally polarized abelian varieties of dimension g over* $\mathbb{C}$ is given by the quotient $\mathcal{A}_g = \mathrm{Sp}_{2g}(\mathbb{Z})\backslash H_g$.

Remark 2.7.7. Via the association

$$Z \mapsto \mathbb{C}^g/(Z, I_g)\mathbb{Z}^g$$

the points of $\mathcal{A}_g$ are in bijective correspondence with the isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$.

Remark 2.7.8. As mentioned in Remark 2.6.4, in the further course of this thesis (especially in the Chapters 8 and 7) we consider the explicit (computational) identification and the classification of a certain locus, the so-called *(hyperelliptic) Jacobian locus* inside $\mathcal{A}_g$, for $g = 3$. Points in the latter space correspond to isomorphism classes of simple principally polarized abelian varieties of dimension g over $\mathbb{C}$.

In Chapter 9 we consider $\mathcal{A}_g$ a as moduli space of principally polarized abelian varieties of dimension g over algebraically closed fields k of $\mathrm{char}(k) = p > 0$. We restrict in this chapter to the *supersingular locus* $\mathcal{S}_g \subset \mathcal{A}_g$ for $g = 2, 3$.

3

Jacobian Varieties

It is well known that for $g > 4$ most $Z \in \mathcal{H}_g$ does not gives rise to a small period matrix of a Jacobian of a smooth projective curve of genus g. The identification of these period matrices is an old problem in arithmetic geometry known as the *Schottky problem*. We briefly recall in this chapter the (analytic) construction of the Jacobian and the Abel-Jacobi map on X. We follow the discussion in [4, Chapter 11] and [51], respectively.

3.1 Definitions

In this chapter we fix our ground field to be $\mathbb{C}$ (for the reason, see Footnote 1). A special type of simple polarized abelian varieties (A, E) of dimension g over $\mathbb{C}$ are Jacobians of smooth projective curves X of genus g. In this chapter we construct for a given smooth projective curve X of genus g over $\mathbb{C}$ a principally polarized abelian variety of dimension g over $\mathbb{C}$, called the *Jacobian* of X and denoted by

$$(\mathrm{Jac}(X), E). \tag{3.1.1}$$

3.2 The analytic construction of the Jacobian

Let X be a smooth projective curve of genus g over $\mathbb{C}$. Let $\lambda_1, \ldots, \lambda_{2g}$ be a basis of the *first homology group*

$$H_1(X, \mathbb{Z}).$$

It is free of rank $2g$. Let $\omega_1, \ldots, \omega_g$ be a basis of the $\mathbb{C}$-space of *holomorphic differentials*

$$V := H^0(\omega_X)$$

on X and let V^* be the dual space with respect to this basis. There is a canonical way to embed $H_1(X, \mathbb{Z}) \hookrightarrow V^*$ by

$$\gamma \mapsto \left\{ \omega \mapsto \int_\gamma \omega \right\}$$

for any $\gamma \in H_1(X, \mathbb{Z})$, see [4, Lemma 11.1.1]. In this way $H_1(X, \mathbb{Z})$ is a lattice in V^* and the quotient

$$\mathrm{Jac}(X) = V^*/H_1(X, \mathbb{Z})$$

is a complex torus of dimension g, called the Jacobian of X.

If $l_1, \ldots, l_g$ is a dual basis of V^* with respect to $\omega_1, \ldots, \omega_g$, then we describe $\lambda_1, \ldots, \lambda_{2g}$ of $H_1(X, \mathbb{Z})$ as linear forms in V by $\lambda_i = \sum_{j=1}^{g} \left(\int_{\lambda_i} \omega_j \right) l_j$ for $1 \leq i \leq 2g$. With respect to Definition 2.1.2, the big period matrix to the complex torus $\mathrm{Jac}(X)$ is given by

$$\Pi = \begin{bmatrix} \int_{\lambda_1} \omega_1 & \cdots & \cdots & \int_{\lambda_{2g}} \omega_1 \\ \vdots & & & \vdots \\ \int_{\lambda_1} \omega_g & \cdots & \cdots & \int_{\lambda_{2g}} \omega_g \end{bmatrix}. \tag{3.2.1}$$

We choose a standard symplectic basis $\lambda_1,\dots,\lambda_g,\mu_1,\dots,\mu_g$ for $H_1(X,\mathbb{Z})$, such that the intersection matrix with respect to this basis is given by the matrix J_g in Equation 2.4.2. Then $\lambda_1,\dots,\lambda_g,\mu_1,\dots,\mu_g$ is a basis of the dual space V^* as an $\mathbb{R}$-space, see [4, page 317]. Denote by

$$E : V^* \times V^* \to \mathbb{R}$$

the non-degenerate alternating form on V^* with matrix representation J_g with respect to this basis. Use it to define a form

$$\begin{aligned} H : V^* \times V^* &\to \mathbb{C} \\ (v,w) &\mapsto H(v,w) = E(iv,w) + iE(v,w). \end{aligned}$$

Then H is a positive definite hermitian form on V^* with Riemann form E, which induces an ample line bundle $\mathscr{L} = \mathscr{L}(H,\chi)$ on $\mathrm{Jac}(X)$, see [4, Proposition 11.12].

Let $(\mathrm{Jac}(X),E)$ be the Jacobian of a smooth projective curve of genus g. Let Π be a big period matrix for $\mathrm{Jac}(X)$ as in Equation (3.2.1), with respect to a basis $\omega_1,\dots,\omega_g$ of $H^0(\omega_X)$ and to a standard symplectic basis $\lambda_1,\dots,\lambda_g,\mu_1,\dots,\mu_g$ of $H_1(X,\mathbb{Z})$, such that the representation matrix of E with respect to this basis is given by the matrix in Equation (2.4.2). We write

$$\Pi = (\Pi_1, \Pi_2) \tag{3.2.2}$$

to denote by Π_1 the first half formed by the first g columns of Π, and by Π_2 the second half. By considering a second basis of $H^0(\omega_X)$, the new big period matrix to $\mathrm{Jac}(X)$ with respect to this basis is given by

$$\Pi = (Z, I_g) \tag{3.2.3}$$

for some small period matrices Z in the Siegel upper half-space $\mathcal{H}_g$ (see Definition 2.7.2), and where I_g is the identity matrix (see Section 2.7).

Regarding to Definition 2.7.2, we get the following definition.

Definition 3.2.1. We say that a Jacobian variety $(\mathrm{Jac}(X),E)$ of dimension g over $\mathbb{C}$ has small period matrix $Z \in \mathcal{H}_g$, if

$$\mathrm{Jac}(X) \cong \mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g),$$

and where the matrix representation of Riemann form E with respect to a standard symplectic basis for $H_1(X,\mathbb{Z})$ is given by Equation (2.4.2).

3.3 The Abel-Jacobi map

Theorem 3.3.1 (Abel-Jacobi)**.** *Let* $\mathrm{Pic}^0(X)$ *be the group of equivalence classes of degree-*0 *divisors modulo principal divisors (or line bundles, respectively) on* X*. Then the* Abel-Jacobi map *yields a canonical isomorphism*

$$\begin{aligned} AJ\colon \mathrm{Pic}^0(X) &\xrightarrow{\sim} \mathrm{Jac}(X) \\ \sum_i [Q_i - P_i] &\mapsto \left(\sum_i \int_{P_i}^{Q_i} \omega_j \right)_j . \end{aligned} \tag{3.3.1}$$

Proof. See [4, Theorem 11.1.3]. □

Corollary 3.3.2. *For any $g \geq 1$ the Abel-Jacobi map $\alpha : X \to \mathrm{Jac}(X)$ is an embedding.*

Proof. See [4, Corollary 11.1.5]. □

Theorem 3.3.3 (Torelli's Theorem)**.** *Let $(\mathrm{Jac}(X), E_X)$ and $(\mathrm{Jac}(X'), E_{X'})$ be Jacobians of smooth projective curves of genus g. If $(\mathrm{Jac}(X), E_X)$ and $(\mathrm{Jac}(X'), E_{X'})$ are isomorphic as polarized abelian varieties, then X is isomorphic to X'.*

Proof. See [4, Theorem 11.17]. □

3.4 The genus-3 case

Most of the time in this thesis we restrict to principally polarized abelian varieties of dimension 3. In Chapter 5 we give necessary and sufficient conditions on the matrix $Z \in \mathcal{H}_3$ to be a small period matrix of a Jacobian of a hyperelliptic curve of genus 3 over $\mathbb{C}$ (or over some number fields, respectively). This identification is based on the *theta constants* (see Theorem 5.4.14) of Z which determines hyperelliptic small period matrices among all period matrices in $\mathcal{H}_3$.

The general characterization of principally polarized abelian varieties of *dimension* 3 is based on the following theorem.

Theorem 3.4.1. *Simple principally polarized abelian varieties of dimension* 3 *are Jacobian of smooth projective curves of genus* 3*.*

Proof. See [57]. □

4 Smooth Projective Curves

4.1 Definitions

For the rest of this chapter we denote by k an arbitrary field that we assume to be algebraically closed and of $\mathrm{char}(k) \neq 2$. We follow the discussion in [50, 76].

Definition 4.1.1. A *smooth projective curve* is a irreducible non-singular closed subvariety of dimension 1 in some projective space $\mathbb{P}^n_k$.

There are several methods to define the (topological, arithmetic, and the analytic) genus of smooth projective curves, see e.g. discussion before Theorem 3.11 in [50, Chapter 6]. All of these genera are equal. Since in the Chapters 7 and 8, our curves are all defined over $\mathbb{C}$ (or over some CM fields, respectively), we restrict in this thesis to the definition of their topological genus.

Definition 4.1.2. If X is a smooth projective curve over $\mathbb{C}$, then we define the *genus* of X to be the number of handles in the Riemann surface $X(\mathbb{C})$.

In this thesis, especially in the Chapters 7 and 8, we are interested in certain *models* describing (smooth projective) curves of genus g. Given an affine equation for a curve (which we will specify in the next sections), we will identify it with the smooth projective curve that has the same function field.

4.2 Smooth projective curves of genus 3

The theory (and the algorithms) we will develop in the Chapters 7 and 8, restricts to Jacobians of smooth projective curves of genus 3. It is well known that the genus-3 case is the first case where there are two types of smooth (projective) curves of genus 3 over k, namely hyperelliptic curves and non-hyperelliptic curves.

We give here the following classification of smooth projective curves of genus 3 over k.

Proposition 4.2.1. *Let X be a smooth projective curve of genus 3 over k. Then:*

(i) Either X is hyperelliptic over k defined by an equation of the form $y^2 = f(x)$ where f has degree 7 or 8, or

(ii) There is an injective map $\varphi : X \hookrightarrow \mathbb{P}^2_k$, that embeds X into the projective plane $\mathbb{P}^2_k$ as a smooth curve defined by the vanishing of a quartic polynomial.

Proof. See [50, Chapter 7, Proposition 2.5]. □

4.3 Hyperelliptic curves of genus 3

In this section we consider hyperelliptic curves X of genus 3 over k. We introduce the Rosenhain model for X.

Let X be a hyperelliptic curve of genus 3 over k. Then X is fully determined by the *canonical* map

$$\begin{aligned} \pi : X(k) &\to \mathbb{P}^1_k \\ (x,y) &\mapsto x. \end{aligned} \tag{4.3.1}$$

The map π is ramified in $2g+2$ points. Any automorphism of $\mathbb{P}^1_k$ permutes the $2g+2$ ramification points, see [50, Page 243].

Definition 4.3.1. If X is a hyperelliptic curve, then we call the ramification points of the map π in Equation 4.3.1, the *Weierstrass points* of X. See [50, Pages 204 and 243].

Remark 4.3.2. Let X be a hyperelliptic curve of genus 3 over an algebraically closed field k. By Proposition 4.2.1, X is given by an affine model of the form $X : y^2 = f(x)$ where $\deg(f) = 7, 8$. If $\deg(f) = 8$, then there are fractional linear transformations, $\mathbb{P}^1_k \to \mathbb{P}^1_k$ that sends the set of brach values $\{a_1, \ldots, a_8\} \subset \mathbb{P}^1_k$ with $(a_i, 0) \in X(k)$ the Weierstrass points on X, to a set of branch values $\{a'_1, \ldots, a'_7, \infty\} \subset \mathbb{P}^1_k$ with $(a'_i, 0) \in X'(k)$ the Weierstrass points on a hyperelliptic curve X' over k for $0 \leq i \leq 7$ with an affine model $X' : y^2 = g(x)$ where $\deg(g) = 7$, and where as hyperelliptic curves X and X' are isomorphic. See e.g. [26, Example 1.83].

More general, we get the following explicit expression for isomorphisms $\varphi : X \to X'$ between hyperelliptic curves of genus 3 over k (see [42], for general genus $g > 1$).

Proposition 4.3.3. *Let $X : y^2 = f(x)$ and $X' : y^2 = g(x)$ be hyperelliptic curves of genus 3 over k. Every isomorphism $\varphi : X \to X'$ is given by an expression of the form*

$$(x,y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^4} \right)$$

for some $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$ and $e \in k^*$. The pair (M, e) is unique up to some multiplications given by $(\lambda M, \lambda^4 e)$ for $\lambda \in k^*$. The composition of the isomorphisms (M, e) and (M', e'), is $(M'M, e'e)$.

Proof. See [42]. □

In Chapter 8, one of our focus is the computation of a certain model for hyperelliptic curves, the so-called normalized Rosenhain form.

Definition 4.3.4. Let X be a hyperelliptic curve of genus 3 over k. We say that X is in *generalized Legendre form* if

$$X : y^2 = x(x-1)\prod_{i=3}^{7}(x - \lambda_i) \tag{4.3.2}$$

where $\lambda_1 = 0, \lambda_2 = 1, \lambda_\infty = \infty$. The coefficients $\lambda_i \in k \backslash \{0, 1, \infty\}$ are called *Rosenhain invariants* of the curve X.

Remark 4.3.5. A normalization as in Definition 4.3.4 is *not* unique. That is due to the choice of some indices in the formula of Takase (see Equation (5.5.1)). In the paper [17], we have chosen a different normalization, see Remark 8.5.8.

Remark 4.3.6. We will see in Chapter 5, (see Proposition 5.5.5) that the coefficients λ_i in the normalized Rosenhain form for X are (modular) invariants of (hyperelliptic) curves.

Example 4.3.7. Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus 3 over $\mathbb{C}$, where $f(x) \in k[\mathbb{C}]$ is a non-singular and separable polynomial given by the equation $f(x) = x^7 - x$. A normalized Rosenhain model for X is given by

$$X : y^2 = x(x-1)(x+\lambda)(x-\lambda)(x+\lambda^2)(x-\lambda^2)(x+\lambda^3),$$

where $\lambda = \zeta_3$ is a primitive third root of unity. We can descend X to be the cyclotomic field $k = \mathbb{Q}(\zeta_3) \subset \mathbb{C}$. There is an automorphism $X \to X$ given by

$$(x, y) \mapsto \left(\zeta_3^2 x, \zeta_3 y\right).$$

Remark 4.3.8. In Chapter 7, we introduce general methods for descending (non)-hyperelliptic curves of genus 3 (with complex multiplication).

We give an example of a hyperelliptic curve of genus 3 defined over number fields after descending. The information about the field of definition of the curve is based on the knowledge of complex multiplication theory. See Chapters 6 and 7.

4.4 Non-hyperelliptic curves

Let X be a smooth projective curve of genus g over k. If X is non-hyperelliptic, then by Proposition 4.2.1, there is a map $\varphi_{\mathscr{K}} : X \hookrightarrow \mathbb{P}^2_k$, depending on a canonical divisor $\mathscr{K}$ on X, such that $\varphi_{\mathscr{K}}$ embeds X into the projective plane $\mathbb{P}^2_k$, and X is a smooth plane quartic curve defined by the vanishing of a quartic polynomial. We give here some examples of non-hyperelliptic curves of genus 3 over $\mathbb{C}$ and over some number fields, respectively.

Example 4.4.1. Let $X : y^3 = f(x)$ be a non-hyperelliptic curve of genus 3 over $\mathbb{C}$, where $f(x) \in k[x]$ is a non-singular and separable polynomial given by the equation $f(x) = x^4 - x$. By computing the roots r_i of f, we find out that $r_1 = 0$, $r_2 = 1$, $r_3 = \zeta_9^3$, and that $r_4 = -(1 + \zeta_9^3)$, where ζ_9 is a primitive ninth root of unity. We get a model of the curve given by

$$X : y^3 = \prod_{i=1}^{4} (x - r_i)$$

There is a $(3:1)$-map $\pi : X(\mathbb{C}) \to \mathbb{P}^1_k$, $(x, y) \mapsto x$, ramified in the 4-Weierstrass points, $(r_i, 0) \in X(\mathbb{C})$. By looking at the roots of f, there is an automorphism $X \to X$ given by

$$(x, y) \mapsto \left(\zeta_9^3 x, \zeta_9 y\right).$$

This is an example of an CM curve where k is a CM field (see Definition 6.1.3) of degree six given by the cyclotomic polynomial $x^6 + x^3 + 1$ and with maximal ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_9]$.

5 The Hyperelliptic Locus

The *Schottky problem* is the problem of characterizing Jacobian varieties among all abelian varieties. Another Schottky-type problem which we consider in this chapter, is the characterization of *hyperelliptic Jacobian varieties* among all abelian varieties. We give a brief introduction in the latter characterization. We will use this theory in the Chapters 7 and 8, where we (computationally and heuristically) identify hyperelliptic (CM) points inside the moduli space $\mathcal{A}_g$ for $g = 3$. In this chapter we follow the theory described in the articles [55, 61, 1].

5.1 Definitions

In this chapter we consider principally polarized abelian varieties of dimension g over $\mathbb{C}$ given by tuples $(A = \mathbb{C}^g/\Lambda, E)$ together with some (small) period matrices $Z \in \mathcal{H}_g$. By Definition 2.7.2 (and after identifying the complex vector space V by $\mathbb{C}^g$), we get

$$A(\mathbb{C}) \cong \mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g), \tag{5.1.1}$$

and where the matrix representation of Riemann form E with respect to a standard symplectic basis of Λ is given by Equation (2.4.2).

5.2 Riemann theta functions

If (A, E) is a polarized abelian abelian variety of dimension g over $\mathbb{C}$, and if $\mathscr{L}$ is a class of ample line bundle on A (see Definition 2.4.3) determining E, then there is an embedding of A into some projective space $\mathbb{P}^n_{\mathbb{C}}$ given by

$$\iota_{\mathscr{L}}(\overline{\omega}) = (\vartheta_0(\omega) : \ldots : \vartheta_n(\omega))$$

for any $\overline{\omega} \in A(\mathbb{C})$, and where ϑ_i are so-called *canonical theta functions* evaluated at the point zero on $A(\mathbb{C})$. See [4, Chapters 3.2, 7.5 and 8.5]. In the further course of this thesis it is more convenient, in order to determine hyperelliptic period matrices instead to work with so-called Riemann theta functions.

Definition 5.2.1. Let $Z \in \mathcal{H}_g$. The *Riemann theta function* is a holomorphic function on $\mathbb{C}^g \times \mathcal{H}_g$, given by

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t Z n + 2\pi i \omega^t n)$$

for any $\omega \in \mathbb{C}^g$. See [4, Page 223 and Proposition 8.5.4].

5.3 Theta functions with half-integer characteristics

In order to to determine hyperelliptic points in $\mathcal{A}_g$, we introduce in this section theta functions with half-integer characteristics evaluated at the point $\omega = 0$. After Lemma 2.7.4, any point of the form $\xi = Z\xi_1 + I_g\xi_2 \pmod{Z\mathbb{Z}^g + \mathbb{Z}^g}$ with $\xi_i \in \frac{1}{2}\mathbb{Z}^g$ is a point of order two on $A(\mathbb{C})$. Therefore, we focus on studying the equivalence class $[\xi] \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ of ξ.

Definition 5.3.1. Let $Z \in \mathcal{H}_g$ and $\xi = \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}$. We define the *Riemann theta function with half-integer characteristic* ξ by

$$\vartheta[\xi](0,Z) = \exp(\pi i \xi_1^t Z \xi_1 + 2\pi i \xi_1^t \xi_2)\vartheta(0,Z). \tag{5.3.1}$$

In this context we call ξ an *even (an odd, respectively) theta characteristic* if $e_*(\xi) = 1$ ($e_*(\xi) = 0$, respectively), where

$$e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2). \tag{5.3.2}$$

If ξ is an even (respectively an odd) theta characteristic we call the value of $\vartheta[\xi](0,Z)$ an *even (respectively an odd) theta constant*.

Lemma 5.3.2. *For any positive integer g there are $2^{g-1}(2^g+1)$ even theta (and $2^{g-1}(2^g-1)$ odd theta) functions with half-integer characteristics ξ.*

Proof. See e.g. [61]. □

Example 5.3.3. If $g = 3$, then there are (up to equivalence modulo $\mathbb{Z}^6$) exactly 36 even theta characteristics and 28 odd theta characteristics to a matrix $Z \in \mathcal{H}_3$.

Proposition 5.3.4. *For any $\xi \in \frac{1}{2}\mathbb{Z}^{2g}$ and $\omega \in \mathbb{C}^g$ we have*

$$\vartheta[\xi](-\omega,Z) = e_*(\xi)\vartheta[\xi](\omega,Z). \tag{5.3.3}$$

Proof. See [54, Chapter 2, Proposition 3.14]. □

Because of the following Corollary, we turn our attention on even theta characteristics.

Corollary 5.3.5. *If ξ is an odd theta characteristic, then the theta constant $\vartheta[\xi](0,Z)$ vanishes on Z.*

Proof. Follows from Equation (5.3.3). □

At the end of this section we describe an action of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ on theta characteristics, and the theta transformation formula. We will use this formula, especially in Chapter 8, in order to compute *Rosenhain class polynomials* (see Equation 8.5.8).

Definition 5.3.6. There is an action of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ on theta characteristics $\xi \in \frac{1}{2}\mathbb{Z}^{2g}$ given by

$$M.\xi = M^* \cdot \xi + \frac{1}{2}\delta_0 \tag{5.3.4}$$

for $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$, $M^* = (M^{-1})^t$, and $\delta_0 = \begin{bmatrix} (c^t d)_0 \\ (a^t b)_0 \end{bmatrix}$ where $(c^t d)_0$ and $(a^t b)_0$ are the diagonal vectors of $c^t d$ and $a^t b$, respectively. See [4, Chapter 8].

Formula 5.3.7 (Theta transformation formula)**.** For any $Z \in \mathcal{H}_g$ and characteristics $\xi \in \frac{1}{2}\mathbb{Z}^{2g}$ we have

$$\vartheta[M.\xi](0,M.Z) = \zeta(M) \cdot \exp(k(M,\xi)) \cdot \sqrt{\det(cZ+d)} \cdot \vartheta[\xi](0,Z), \tag{5.3.5}$$

where:

(i) $\zeta(M)$ is an eighth root of unity depending on M with the same sign as $\sqrt{\det(cZ+d)}$.

(ii) $k(M,\xi) = \pi i\,(d\xi_1 - c\xi_2)^t\left(-b\xi_1 + a\xi_2 - \left(a^t b\right)_0\right) - \xi_1^t \xi_2$,

and where $M.Z$ corresponds to the action of M on Z in Equation (2.7.3). See [4, Formula 8.6.1].

5.4 η-maps

In this section we turn our attention on a certain class of maps, so-called *η-maps*. These maps are crucial in order to understand hyperelliptic Jacobian varieties. Let

$$\mathrm{Jac}(X) \cong \mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g)$$

be a hyperelliptic Jacobian variety with (small) period matrix $Z \in \mathcal{H}_g$. In order to introduce the main theorem in this chapter (see Theorem 5.4.14), we recall here the basis properties of these maps, by following the papers [55, 61, 1, 17].

We begin this section with the following abstract construction of an symplectic $\mathbb{F}_2$-vector spaces.

Proposition 5.4.1. *Let $\mathcal{B}$ be a set with $2g+2$ elements. For any subsets S_1, S_2 of $\mathcal{B}$, let*

$$S_1 + S_2 = (S_1 \cup S_2) \backslash (S_1 \cap S_2)$$

Let $S^c \subset \mathcal{B}$ be the complement of S in $\mathcal{B}$. There is an equivalence relation $\sim$ on subsets S in $\mathcal{B}$ given by $S_1 \sim S_2$ if $S_2 = S_1^c$. Then the set

$$G_{\mathcal{B}} = \{S \subset \mathcal{B} : \ \#S \equiv 0 \pmod 2\}/\sim \tag{5.4.1}$$

forms an $(g+1)$-dimensional $\mathbb{F}_2$-vector space under the operation $+$. There is a bilinear pairing on $G_{\mathcal{B}}$ given by

$$\langle S_1, S_2 \rangle_{G_{\mathcal{B}}} = \#(S_1 \cap S_2) \pmod 2 \tag{5.4.2}$$

which turns $(G_{\mathcal{B}}, \langle , \rangle_{G_{\mathcal{B}}})$ into a symplectic vector space. See [55, Lemma 2.4 and Proposition 6.3].

Lemma 5.4.2. *Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus g, where f is a monic polynomial of degree $2g+1$. Let $\{\lambda_1, \ldots, \lambda_{2g+1}\}$ be the roots of f and let $\lambda_\infty = \infty$. Define $\mathcal{B} = \{\lambda_1, \ldots, \lambda_{2g+1}, \lambda_\infty\}$ and take let $\mathcal{O} = (\lambda_\infty, 0)$. Let $G_{\mathcal{B}}$ be the group to $\mathcal{B}$ in Proposition 5.4.1. Let $\psi : G_{\mathcal{B}} \to \mathrm{Pic}^0(X)$ be given by*

$$[S] \mapsto e_S = \psi(S) := \sum_{i \in S} [(\lambda_i, 0)] - [(\#S)\mathcal{O}]. \tag{5.4.3}$$

Then ψ is an isomorphism of symplectic vector spaces $(G_{\mathcal{B}}, \langle S_1, S_2 \rangle_{G_{\mathcal{B}}})$ and $(\mathrm{Pic}^0(X), \langle , \rangle_2)$.

Proof. See [55, Lemma 2.2, Corollary 2.11 and Proposition 6.3] or [61, Lemma 1.4.4], respectively. □

Remark 5.4.3. A similar statement can be made for the case where $\deg(f) = 2g+2$, see [61, Page 822].

The following lemma gives a parametrization of the 2-torsion points on $\mathrm{Pic}^0(X)$ as elements in the abstract group $G_{\mathcal{B}}$, and equivalence classes of theta characteristics.

Lemma 5.4.4. *Let* $\mathrm{Jac}(X)$ *be the Jacobian of a hyperelliptic curve*

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

of genus g, where $\deg(f) = 2g+1$. *Let $\mathcal{B} = \{\lambda_1, \ldots, \lambda_{2g+1}, \lambda_\infty\}$ where λ_i, $1 \le i \le 2g+1$ are the roots of f and $\lambda_\infty = \infty$. For any $\lambda_i \in \mathcal{B}$, define $e_i = [(\lambda_i, 0) - \mathcal{O}]$ in* $\mathrm{Pic}^0(X)$. *Then by the Abel-Jacobi map*

$$\eta_i = AJ(e_i),$$

and where $\eta_i = Z \cdot (\eta_i)_1 + I_g \cdot (\eta_i)_2$ is a vector in $\frac{1}{2}\mathbb{Z}^{2g}$, where $Z \in \mathcal{H}_g$ is a small period matrix to $\mathrm{Jac}(X)$. *For any subset $S \subset G_{\mathcal{B}}$, define $\eta_S = \sum_{i \in T} \eta_i$. Then:*

(i) $2\eta_S = 0$.

(ii) $\eta_{S_1} + \eta_{S_2} = \eta_{S_1+S_2}$.

(iii) $\eta_{S_1} = \eta_{S_2}$ *if and only if* $S_1 \sim S_2$.

(iv) A group isomorphism $G_{\mathcal{B}} \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, *given by the map* $S \mapsto \eta_S$.

Proof. See [61, Definition 1.4.5 and Lemma 1.4.6]. □

Remark 5.4.5. Similar statements can be made for the case where $\deg(f) = 2g+2$, see [61].

Definition 5.4.6. We define by Ξ_g to be the set of equivalence classes of maps

$$\eta : P(\mathcal{B}) \to \frac{1}{2}\mathbb{Z}^{2g}, \tag{5.4.4}$$

where $P(\mathcal{B})$ is the *power set* of $\mathcal{B}$, satisfying the following properties:

(i) $\eta_\infty = \vec{0}$.

(ii) For any $S \subseteq \mathcal{B}$, $\eta_S = \sum_{i\in S} \eta_i$.

(iii) η induces an symplectic isomorphism $\eta : G_{\mathcal{B}} \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, given by the map $S \mapsto \eta_S$.

(iv) There is a set $U_\eta \subset \mathcal{B}$ such that $\#U_\eta \equiv g+1 \pmod 2$ and for all even subsets $S \subset \mathcal{B}$ we have

$$e_*(\eta_S) = (-1)^{\frac{1}{2}(g+1-\#(S+U_\eta))}$$

and where e_* was defined in Equation (5.3.1).

We call two maps in Ξ_g *equivalent* if they are equal as maps into $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$. See [61, Definition 1.4.11].

Remark 5.4.7. The set U_η in the above definition plays a crucial role in theorem 5.4.14. It has beed explicitly computed by the authors in [1], for the case where $g = 3$.

Any hyperelliptic curve X of genus g is fully characterized by the ramification points of the map $\pi : X(\mathbb{C}) \to \mathbb{P}^1_{\mathbb{C}}, (x, y) \mapsto x$ (see Equation 4.3.1). After fixing $\lambda_\infty = \infty$, there are $(2g+1)!$ different ways to order the $2g+1$ branch values of the map π, which leads to the following definition.

Remark 5.4.8. Because of the several combinatorial possibilities of of the ordering of the branch values of the map π, there are several ways to assign a class of maps in Ξ_g to a matrix $Z \in \mathcal{H}_g$, see [61, Page 825].

Definition 5.4.9. Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus g over $\mathbb{C}$, where f is a monic polynomial of degree $2g+1$. Let $\lambda_1, \ldots, \lambda_{2g+1}$ be the roots of f as branch values of the map $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$. By a *marking* of X we understand a certain ordering of the set $\{\lambda_1, \ldots, \lambda_{2g+1}, \lambda_\infty\}$ where $\lambda_\infty = \infty$. If a hyperelliptic curve X of genus g admits a marking, then we call X a *marked* hyperelliptic curve of genus g.

By following [61, Pages 823 and 825], we consider in the rest of this section marked hyperelliptic curves X of genus g.

Definition 5.4.10. We say that the class of maps $[\eta] \in \Xi_g$ is associated to a matrix $Z \in \mathcal{H}_g$ if there is a marking $\mathcal{B}$ of the hyperelliptic curve X to Z, such that for all $S \subseteq \mathcal{B}$ even, we have $\eta_S = AJ(e_S) \pmod{\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}}$.

Before stating the main theorem of this chapter, we introduce the action of some subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on the set equivalence classes of maps Ξ_g. It is induced by the action on theta characteristics in Definition 5.3.6.

Definition 5.4.11. For any positive integer n, we define the *principal congruence subgroups*

$$\Gamma_n = \left\{ M \in \mathrm{Sp}_{2g}(\mathbb{Z}) : M \equiv I_{2g} \pmod{n} \right\}, \tag{5.4.5}$$

where I_{2g} is the identity matrix, and the *Igusa intermediate normal subgroups*

$$\Gamma_{n,2n} = \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_n : (a^t b)_0 \equiv (c^t d)_0 \equiv 0 \pmod{2n} \right\}, \tag{5.4.6}$$

where $(a^t b)_0$ and $(c^t d)_0$ are the diagonal vectors of $a^t b$ and $c^t d$, respectively. For any positive integer n we have $\Gamma_{2n} \subset \Gamma_{n,2n} \subset \Gamma_n$, see [61, Page 813].

Proposition 5.4.12. *The group* $\mathrm{Sp}_{2g}(\mathbb{F}_2) \cong \mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_2$ *acts freely and transitively on the set of equivalence classes of maps in* Ξ_g *by*

$$\eta' = M^* \cdot \eta$$

for $[\eta] \in \Xi_g$ *and* $M^* = (M^{-1})^t$, *and* $M \in \mathrm{Sp}_{2g}(\mathbb{F}_2)$.

Proof. See [61, Page 826]. □

Remark 5.4.13. Knowing about the free and transitive action of the group $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on the set Ξ_g, together with the explicit computation of Mumford's equivalence class of maps $[\eta] \in \Xi_g$ in [55, Chapter 5], and with the description of these η-maps in [2, Chapter 5.2], we have computed with the code in [2] equivalence classes of maps $[\eta'] \in \Xi_g$ to Galois conjugate hyperelliptic curves of genus $g = 3$. For a detailed description, see Chapter 8.

Theorem 5.4.14 (The Vanishing Criterion)**.** *Let* $Z \in \mathcal{H}_g$ *and let* $[\eta] \in \Xi_g$. *The following two statements are equivalent:*

(i) Z is the period matrix of a simple principally polarized abelian variety of dimension g over $\mathbb{C}$ *satisfying the following equations for a map* η*:*

$$\text{For } S \subseteq \mathcal{B},\ \#S \equiv 0 \pmod 2,\quad \vartheta[\eta_S](0,Z) = 0 \quad \text{if and only if} \quad \#(S \circ U_\eta) \neq g+1.$$

(ii) There is a marked hyperelliptic curve of genus g over $\mathbb{C}$ *whose Jacobian has period matrix Z and* $[\eta] \in \Xi_g$ *is one of the equivalence classes of maps associated to Z.*

Proof. See [61, Main Theorem 2.6.1]. □

5.5 The genus-3 case

We restrict in this section to the main case we mostly consider in this thesis, the case where $g = 3$. By following Theorem 5.4.14, given a hyperelliptic (small) period matrix $Z \in \mathcal{H}_g$ and one of its associated equivalence classes of maps $[\eta] \in \Xi_g$, we can construct a (normalized Rosenhain) model for the hyperelliptic curve via *Thomae's formulae*. Conversely, if $Z \in \mathcal{H}_g$ is a matrix satisfying the criteria in Theorem 5.4.14 for some $[\eta] \in \Xi_g$, then Z is a (small) period matrix of a hyperelliptic Jacobian.

For the case where $g = 3$, Theorem 5.4.14 reduces to the following theorem. It was stated and proven by Igusa, (see [31, Lemmata 10 and 11]) and proven by the authors in [1, Theorem 4].

Theorem 5.5.1 (Igusa)**.** *If $Z \in \mathcal{H}_3$ is (small) period matrix of an Jacobian (variety) of dimension* 3 *over* $\mathbb{C}$*, then Z is a (small) period matrix of an hyperelliptic Jacobian (variety) if and only if $\vartheta[\xi](0, Z)$ vanishes on Z for a single equivalence class $[\xi] \in \frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$ with $e_*(\xi) = 1$.*

Proof. See [1, Theorem 4]. □

To state the formula of Takase-Vincent-Somoza, we set up some notation. We follow here the notation in the articles [1, 17]. We define a set

$$T = \{1, \dots, 2g + 1, \infty\}.$$

As stated in [17, Page 5], Poor defined for an equivalence class of maps $[\eta] \in \Xi_g$, the set U_η (see Definition 5.4.6) to be the set of indices $i \in T$ such that η_i is even (as a theta characteristic, see Lemma 5.4.4).

Theorem 5.5.2 (Takase)**.** *Let $Z \in \mathcal{H}_g$ be a (small) period matrix and $[\eta] \in \Xi_g$ such that the Vanishing Criterion in Theorem 5.4.14 is satisfied. Then with notation as above, for any disjoint decomposition $T - \{\infty\} = \mathcal{V} \sqcup \mathcal{W} \sqcup \{k, \ell, m\}$ where $\#\mathcal{V} = \#\mathcal{W} = 2$ we have:*

$$\frac{\lambda_m - \lambda_\ell}{\lambda_m - \lambda_k} = \exp(4\pi i(\eta_k + \eta_\ell)_1(\eta_m)_2)\left(\frac{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{m,\ell\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{m,\ell\})}]}{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{k,m\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{k,m\})}]}(Z)\right)^2. \tag{5.5.1}$$

Proof. See [72, Theorem 1.1]. For a generalization of the formulae in Equation (5.5.1), see [40, Appendix] . □

Remark 5.5.3. In [17], we have chosen the period matrix $Z \in \Gamma_2 \backslash \mathcal{H}_3$. We restricted to these period matrices in [17], since in this case one can choose the same equivalence classes of η-maps for the computation of equivalence classes of η-maps attached to hyperelliptic Galois orbits under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$.

Remark 5.5.4. We can fix a normalized Rosenhain model (see Definition 4.3.4) of the hyperelliptic curve X to the (small) period matrix $Z \in \mathcal{H}_g$ in Theorem 5.5.2, by using e.g. a normalization given by $\lambda_1 = 0, \lambda_2 = 1$. Then

$$X : y^2 = x(x-1)\prod_{l=3}^{7}(x - \lambda_\ell),$$

where λ_ℓ for $3 \leq \ell \leq 7$ are computed by the formula in Equation (5.5.1) for $k = 1$ and $m = 2$.

Proposition 5.5.5. *The Rosenhains coefficients of hyperelliptic curves of genus g are modular invariants with respect to the modular group* $\Gamma_{4,8}$.

Proof. This follows from the fact that theta constants are modular forms of weight 1/2 for the modular group $\Gamma_{4,8}$. See e.g. [61, Theorem 1.1.7]. □

6

Abelian Varieties with Complex Multiplication

In this chapter we recall the construction and some basic properties of principally polarized abelian varieties with complex multiplication (CM), due to Shimura and Taniyama. We follow here the discussion in [63, Chapter 2] and in [39, Chapter 1], respectively. Further we restrict our attention to simple principally polarized abelian varieties with CM. More precisely, a restriction to dimension 3 simple principally polarized abelian varieties with CM is, according to Theorem 3.4.1, equivalent to considering Jacobian varieties of smooth projective curves of genus 3 with CM. By Shimura and Taniyama's theory of CM, the invariants of these curves generate certain abelian extensions of CM fields.

6.1 Definitions

Let V be a g-dimensional complex vector space. To conform to the literature in [39, Chapter 1], we define $V = \mathbb{C}^g$. Let $(A = \mathbb{C}^g/\Lambda, E)$ be a principally polarized abelian variety of dimension g over $\mathbb{C}$. From the discussion in Chapter 2.7, there exist a basis of V and a standard symplectic basis of Λ, such that the matrix representation of the Riemann form E with respect to the basis of Λ is given by matrix in Equation (2.4.2). Further by discussion in the same chapter there are matrices Z in the Siegel upper half space $\mathcal{H}_g$, such that $A(\mathbb{C}) \cong V/(Z\mathbb{Z}^g + \mathbb{Z}^g)$.

In this chapter we construct for a given triple $(\Phi, \mathfrak{a}, \xi)$ related to a CM field K a principally polarized abelian variety of dimension g over $\mathbb{C}$,

$$A(\Phi, \mathfrak{a}, \xi). \tag{6.1.1}$$

Let $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of A (see Definition 2.6.4).

Definition 6.1.1. Let $A = \mathbb{C}^g/\Lambda$ be a an abelian variety of dimension g over $\mathbb{C}$. We say that A has *complex multiplication (CM)* by a number field K if there exists an embedding

$$\iota : K \hookrightarrow \mathrm{End}^0(A). \tag{6.1.2}$$

Let $\mathcal{O}_K$ be the ring of integers of K. We say A has *CM by* $\mathcal{O}_K$ (or *maximal CM*, respectively), if $\iota^{-1}(\mathrm{End}(A)) \cong \mathcal{O}_K$.

Remark 6.1.2. Let $(\mathrm{End}^0(A), \dagger)$ be a tuple where $\dagger$ is the Rosati involution on $\mathrm{End}^0(A)$ (see Definition 2.6.5). If $(\mathrm{End}^0(A), \dagger)$ is of the second kind then K is an CM field and the restriction of the Rosati involution to K is complex conjugation (see Lemma 2.6.10).

Definition 6.1.3. A *Complex Multiplication (CM) field* K is a totally imaginary quadratic extension of a totally real number field K_0.

Example 6.1.4. The simplest example of CM fields are imaginary quadratic extensions of $\mathbb{Q}$ as, e.g. $K = \mathbb{Q}(i)$ where i is a roof of the polynomial $f(x) = x^2 + 1$.

Definition 6.1.5. Let K be a CM field. A *CM type of* K is a subset $\Phi \subset \mathrm{Hom}(K, \mathbb{C})$ such that

$$\mathrm{Hom}(K, \mathbb{C}) = \Phi \amalg \Phi\rho \tag{6.1.3}$$

where $\rho \in \mathrm{Aut}(K)$ is a unique element such that $\iota(\rho(x)) = \overline{\iota(x)}$ for all $x \in K_0$ the totally real subfield of K, for all embeddings $\tau : K \hookrightarrow \mathbb{C}$. We call ρ the *complex conjugation* on K. We call a CM type *primitive* if it is not induced by a proper CM subfield. We call two CM types Φ, Φ' *equivalent* if there exists an automorphism $\alpha \in \mathrm{Aut}(K)$ such that $\Phi' = \Phi\alpha$. See [39, Page 6].

Definition 6.1.6. A *CM type* is a tuple (K, Φ) if K is a CM field and Φ is a CM type of K.

Remark 6.1.7. We can see by the above definition that for any CM field K where e.g. $\mathbb{Q}(i) \subset K$, there are some non-primitive CM types Φ on K which are induced by CM subfield $\mathbb{Q}(i)$. In Chapter 7 we will give a complete description of (non) primitive CM types of sextic CM fields up to (Galois) equivalence.

6.2 Ideals and polarizations

In this section we briefly recall the construction of principally polarized abelian varieties with complex multiplication due to Shimura and Taniyama. It is well known (see Chapter 2) that any complex abelian variety $A(\mathbb{C})$ is a complex torus $A = V/\Lambda$ admitting a Riemann form E on the lattice. Let (K, Φ) be a CM type where K is a CM field of degree $2g$. We can use Φ to define a map $K \to \mathbb{C}^g$ given by

$$x \mapsto \Phi(x) = (\varphi_1(x), \ldots, \varphi_g(x)).$$

Then any fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ gives rise to a full lattice $\Phi(\mathfrak{a}) \subset \mathbb{C}^g$, and $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a g-dimensional complex torus of type (K, Φ). More precisely, the following theorem gives a correspondence between g-dimensional complex tori of type (K, Φ) and fractional $\mathcal{O}_K$-ideals.

Theorem 6.2.1. *Let (K, Φ) be a CM type and let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal. Then*

(i) $\Phi(\mathfrak{a})$ is a full lattice in $\mathbb{C}^g$ for any $g \geq 1$ and $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus of type (K, Φ).

(ii) Two complex tori $\mathbb{C}^g/\Phi(\mathfrak{a})$ and $\mathbb{C}^g/\Phi(\mathfrak{a}')$ of type (K, Φ) are isomorphic if and only if $\mathfrak{a}' = (\alpha)\mathfrak{a}$ for some α in K^*.

(iii) For any g-dimensional complex torus (A, ι) of type (K, Φ) there exists some fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ such that A is isomorphic to $\mathbb{C}^g/\Phi(\mathfrak{a})$.

Proof. See [39, Theorem 4.1]. □

According to Definition 2.4.3, a polarization is a certain class of ample line bundle $\mathscr{L} = \mathscr{L}(H, \chi)$ on $\mathbb{C}^g/\Lambda$. Let (K, Φ) be a CM type. To be consistent with the literature, we denote by

$$(\mathfrak{a}, \xi) \tag{6.2.1}$$

a pair where:

(i) $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal.

(ii) ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K, $\varphi(\xi)$ is an positive imaginary element for any $\varphi \in \Phi$, and

$$(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$$

where $\mathfrak{D}_{K|\mathbb{Q}}^{-1} = \{\alpha \in K : \mathrm{Tr}_{K|\mathbb{Q}}(\alpha\mathcal{O}_K) \subseteq \mathbb{Z}\}$ is the *different* of $K|\mathbb{Q}$.

Define $E = E_{\Phi,\xi} : \Phi(K) \times \Phi(K) \to \mathbb{Q}$ by

$$E(\Phi(v), \Phi(w)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi \overline{v} w) \tag{6.2.2}$$

for any $v, w \in K$. Then E is a positive definite Riemann form on the lattice $\Phi(\mathfrak{a})$ and it can be uniquely extended to a positive definite hermitian form $H = E(iv, w) + iE(v, w)$ on $\mathbb{C}^g$, see [39, Theorem 4.5].

Theorem 6.2.2. *Let (K, Φ) be a CM type where K is a CM field of degree $2g$ over $\mathbb{Q}$. Then the following holds.*

(i) Any triple $(\Phi, \mathfrak{a}, \xi)$ as above defines a principally polarized abelian variety

$$A(\Phi, \mathfrak{a}, \xi) = (\mathbb{C}^g / \Phi(\mathfrak{a}), E) \tag{6.2.3}$$

of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ).

(ii) Any principally polarized abelian variety of dimension g over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type (K, Φ) is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triples $(\Phi, \mathfrak{a}, \xi)$ as in (i).

(iii) The abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is simple if and only if Φ is primitive. In this case the embedding $\iota : K \to \mathrm{End}^0(A)$ in Equation (6.1.2) is an isomorphism.

(iv) For any pair of triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ as above, $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi, \mathfrak{a}', \xi')$ are isomorphic as principally polarized abelian varieties with CM if there is an element $\gamma \in K^*$ such that $(\mathfrak{a}', \xi') = (\gamma\mathfrak{a}, (\gamma\overline{\gamma})^{-1}\xi)$. Is Φ primitive, then the converse holds.

Proof. See [69, Chapter 1, Theorem 5.2]. □

This section corresponds to the section of the same name in the paper [19], apart from a few changes that are appropriate for this thesis, such as definitions and some other explanations.

Let $(A, E) = A(\mathfrak{a}, \xi) = A(\Phi, \mathfrak{a}, \xi)$ be a principally polarized abelian variety of dimension g over $\mathbb{C}$ of type (K, Φ) whose endomorphism ring is isomorphic to $\mathcal{O}_K$. We can consider the representation of K on the tangent space after choosing some isomorphism

$$\iota : K \to \mathrm{End}^0(A)$$

as in Theorem 6.2.2. The set of embeddings that thus appear yield a primitive CM type Φ of K. It is important to note that the representation of K depends on the chosen isomorphism ι, which means that given the principally polarized abelian variety A, only the *equivalence class* of the CM type Φ is well-defined. We characterize in Section 7.5, CM types of sextic CM fields K up to (Galois) equivalence. This characterization in connection with an explicit description of the image of the map $\mathcal{N}_{\Phi^r}$ (see Definition 7.6.5) in the Shimura class group $\mathcal{C}_K$ (see Definition 7.6.1) of K, is crucial in order to determine a minimal set of representatives of of principally polarized abelian varieties of dimension 3 over $\mathbb{C}$ with primitive CM up to Galois conjugation over the reflex field K^r (see Definition 7.5.1) of K with respect to a primitive CM type Φ. We will discuss this in detail in the Sections 7.5, 7.6, and we describe explicit algorithms which determine such minimal sets in Section 7.9.

Proposition 6.2.3. *Let K be a CM field of degree $2g$, and let Φ be a* primitive *CM type of K. Then the association*

$$(\mathfrak{a}, \xi) \mapsto A(\mathfrak{a}, \xi) = (\mathbb{C}^g / \Phi(\mathfrak{a}), E)$$

defined above yields a bijection between the set of pairs $(\mathfrak{a}, \xi)$ *up to the equivalence given by*

$$(\mathfrak{a}, \xi) \sim (\mathfrak{a}', \xi') \tag{6.2.4}$$

if $(\mathfrak{a}', \xi') = (\gamma\mathfrak{a}, (\gamma\overline{\gamma})^{-1}\xi)$ *for* $\gamma \in K^*$*, and the set of isomorphism classes of principally polarized abelian varieties that admit CM by* $\mathcal{O}_K$ *of type* Φ *up to equivalence.*

Proof. See [70, Theorem 4.2]. □

Definition 6.2.4. We say that two pairs $(\mathfrak{a}, \xi)$ and $(\mathfrak{a}', \xi')$ are *equivalent* if there exists an element $\alpha \in \mathrm{Aut}(K)$ such that $(\alpha^{-1}(\mathfrak{a}), \alpha(\xi))$ and $(\mathfrak{a}', \xi')$ are equivalent in the sense of Proposition 6.2.3.

Proposition 6.2.5. *Two pairs* $(\mathfrak{a}, \xi)$ *and* $(\mathfrak{a}', \xi')$ *are equivalent if and only if* $A(\mathfrak{a}, \xi)$ *and* $A(\mathfrak{a}', \xi')$ *are isomorphic as principally polarized abelian varieties.*

Proof. See [70, Proposition 4.11]. □

Notation 6.2.6. In the rest of this thesis we denote the Galois closure of a CM field K by L. Further we denote by $\iota_L : L \to \mathbb{C}$ a fixed embedding.

Proposition 6.2.7. *Let* A *be a principally polarized abelian variety over* $\mathbb{C}$ *with CM by* K *of type* (K, Φ) *up to equivalence, and let* $\sigma \in \mathrm{Aut}(\mathbb{C})$*. Denoting the restriction of* σ *to* L *by* σ *again, we have that the conjugate principally polarized abelian variety* σA *has CM by* K *of type* $(K, \sigma\Phi)$ *up to equivalence.*

Proof. This follows from the fact that the formation of the tangent space is functorial. Alternatively, if $T \in M_g(\mathbb{C})$ is the tangent representation of a given endomorphism α with respect to a basis of differentials B of A, then σT is a representation of an endomorphism of σA with respect to σB. This means that if after our choice of embedding $K \hookrightarrow \mathrm{End}^0(A)$ we can write the representation ρ of K on the tangent space of A as a direct sum

$$\rho \cong \varphi_1 \oplus \cdots \oplus \varphi_g,$$

we also obtain a representation $\sigma\rho$ of K on the tangent space of σA given by

$$\sigma\rho \cong \sigma\varphi_1 \oplus \cdots \oplus \sigma\varphi_g,$$

which proves the proposition. □

Remark 6.2.8. In the further course of this thesis we identify depending on the context, simple principally polarized abelian varieties of dimension g over $\mathbb{C}$ of type (K, Φ) whose endomorphism ring is isomorphic to $\mathcal{O}_K$ by tuples

$$(A, E) \cong A(\mathfrak{a}, \xi) = A(\Phi, \mathfrak{a}, \xi) \tag{6.2.5}$$

for some pairs $(\Phi, \mathfrak{a}, \xi)$, where:

(i) $(\mathfrak{a}, \xi)$ is a pair up to equivalence as in Equation (6.2.1). It is uniquely determined by a CM type Φ. As mentioned above, it consists of those embeddings $\varphi : K \hookrightarrow \mathbb{C}$ for which the imaginary part of $\varphi(\xi)$ is positive. Therefore, in what follows, we will consider the pairs $(\mathfrak{a}, \xi)$ and the corresponding triples $(\Phi, \mathfrak{a}, \xi)$ interchangeably.

(ii) $A = \mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus of dimension g and where $E = E_{\Phi,\xi}$ is the Riemann form in Equation 6.2.2 induced by the element ξ.

7

Isogenous Hyperelliptic and Non-Hyperelliptic Jacobians with Maximal Complex Multiplication

This chapter corresponds to the paper in [19], apart from some changes that are appropriate for this thesis, such as definitions and some further explanations. We analyze in this chapter complex multiplication (CM) for Jacobians of smooth projective curves of genus 3 over $\mathbb{C}$, as well as the resulting Shimura class groups and their subgroups corresponding to Galois conjugation over the reflex field. In this chapter, we give a list of all sextic CM fields K in the *L-functions and modular forms database* (LMFDB) for which (heuristically) Jacobians of both types of smooth projective curves of genus 3 with CM by $\mathcal{O}_K$ exist. It turns out that there are 14 such fields among the 547,156 sextic CM fields that the LMFDB contains. We determine invariants of the corresponding curves, and in the simplest case we also give an explicit defining equation.

Because of their arithmetic properties and their cryptographic applications, curves of low genus whose Jacobian admits CM have historically been at the forefront of research on algebraic curves. By Shimura and Taniyama's theory of CM, it is well known that the invariants of these curves generate certain abelian extensions of CM fields.

In order to achieve our goals, the third author in [19] and I developed and implement calculation methods that given a CM field K and a primitive CM type Φ, determine a small set of period matrix representatives of the corresponding isomorphism classes of principally polarized abelian threefolds, up to Galois conjugation over the reflex field K^r of K with respect to Φ. A calculation with theta-null values (using [38]) then allows us to determine with the computer which of these representatives correspond to hyperelliptic or non-hyperelliptic curves. A full implementation of these techniques in Magma [6] is an essential part of these results. It is available online at [18].

Chronologically, this chapter (the paper [19], respectively) is a further development of the Chapter 8 (the paper [17], respectively) in this thesis. It arose from the observation I made during the preparation of the paper [17]. There are some sextic CM fields K (apart from the cyclotomic field what was already known, given by the minimal polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$), where (heuristically) exists a hyperelliptic curve whose Jacobian variety has endomorphism ring isomorphic to the maximal order $\mathcal{O}_K$, and where K does *not* include $\mathbb{Q}(i)$. Further we asked ourselves whether there are sextic CM fields K for which there exist both a hyperelliptic *and* a non-hyperelliptic curve whose Jacobian variety has endomorphism ring isomorphic to $\mathcal{O}_K$. Based on this observation, I discussed at this time with the third author of [19] a possible joint project. This developed into the current chapter of this thesis.

7.1 Definitions

Let K be a CM field of degree $2g$ and let $\rho \in \mathrm{Aut}(K)$ be the unique element identifying complex conjugation on K (see Definition 6.1.5). For the rest of this chapter, we denote by L the Galois closure of K and we fix once for all an embedding

$$\iota_L : L \to \mathbb{C}. \tag{7.1.1}$$

The main objects in this chapter are simple principally polarized abelian varieties of dimension 3 over $\mathbb{C}$ of type (K,Φ) whose endomorphism ring is isomorphic to the maximal order $\mathcal{O}_K$. According to Remark 6.2.8, these are given by tuples (triples, respectively)

$$(A,E) \cong A(\mathfrak{a},\xi) = A(\Phi,\mathfrak{a},\xi), \tag{7.1.2}$$

where Φ is a primitive CM type of K, where $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal and where ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K and where $\varphi(\xi)$ is an positive imaginary element for any $\varphi \in \Phi$, and where $(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$. By Theorem 3.4.1, (A,E) is as a simple principally polarized abelian variety with CM by $\mathcal{O}_K$ isomorphic to the Jacobian variety $(\mathrm{Jac}(X),E)$ of a smooth projective curve of genus 3. In order to be compliant with the paper in [19], we say in this case that $(\mathrm{Jac}(X),E)$ is a Jacobian variety with *primitive* CM by $\mathcal{O}_K$. In this chapter, projective curves X are (as in Definition 4.1.1) defined over some algebraically closed fields k, where $\mathrm{char}(k) \neq 2$.

Definition 7.1.1. Let K be a CM field of degree 6. We call K *hyperelliptic*, if there exists (heuristically) a hyperelliptic curve whose Jacobian variety has *primitive* CM by $\mathcal{O}_K$. We call a hyperelliptic CM field K that does *not* include $\mathbb{Q}(i)$ *exceptional hyperelliptic*. We call a CM field K of degree 6 a *mixed* CM field if there (heuristically) exists both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has primitive CM by $\mathcal{O}_K$.

Remark 7.1.2. As was already known, and as can be deduced from the classification in [47], if a CM field K contains $\mathbb{Q}(i)$, then any curve whose Jacobian has primitive CM by $\mathcal{O}_K$ is automatically hyperelliptic.

7.2 The main results

Theorem 7.2.1. *Heuristically, there are 14 sextic CM fields K in the LMFDB for which there exist both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathcal{O}_K$ of K. All these fields have Galois groups* $\mathrm{Gal}(K|\mathbb{Q}) \simeq C_2^3 \rtimes S_3$.

CM field	h_K	d_K
$x^6+10x^4+21x^2+4$	4	$-2^8\cdot 359^2$
$x^6-3x^5+14x^4-23x^3+28x^2-17x+4$	4	$-3^3\cdot 2351^2$
$x^6-2x^5+12x^4-31x^3+59x^2-117x+121$	4	$-7^3\cdot 11^2\cdot 67^2$
$x^6-3x^5+9x^4+4x^3+12x^2+84x+236$	4	$-2^6\cdot 3^6\cdot 31^3$
$x^6-2x^5+x^4-4x^3+5x^2-50x+125$	4	$-2^8\cdot 3^2\cdot 839^2$
$x^6-3x^5+10x^4+8x^3+x^2+90x+236$	4	$-11^2\cdot 17^2\cdot 47^3$
$x^6+21x^4+60x^2+4$	4	$-2^8\cdot 3^2\cdot 23^2\cdot 67^2$
$x^6+30x^4+169x^2+200$	4	$-2^9\cdot 3847^2$
$x^6+26x^4+177x^2+128$	4	$-2^9\cdot 5^4\cdot 199^2$
$x^6+29x^4+226x^2+252$	4	$-2^6\cdot 3^2\cdot 7^3\cdot 281^2$
$x^6-2x^5-7x^4+45x^3-63x^2-162x+729$	4	$-7^3\cdot 12347^2$
$x^6-2x^5+11x^4+42x^3-11x^2+340x+950$	8	$-2^9\cdot 3^2\cdot 3391^2$
$x^6-2x^5+12x^4-44x^3+242x^2-672x+1224$	12	$-2^8\cdot 5^2\cdot 1367^2$
$x^6-3x^5+29x^4-53x^3+200x^2-174x+71$	12	$-7^4\cdot 23^3\cdot 43^2$

Table 7.1: CM fields in Theorem 7.2.1, where h_K is the class number of K, and where d_K is its discriminant.

Remark 7.2.2. Though we cannot seriously formulate a conjecture in this direction for lack of mathematical rigor, circumstantial evidence does to some extent suggest that the sextic CM fields obtained in Theorem 7.2.1 are in fact all of their kind. Indeed, the largest absolute value of the discriminant of the fields in Theorem 7.2.1 equals $5.40 \cdot 10^{10}$, whereas the largest such value for the 494,386 sextic CM fields in the LMFDB with $\mathrm{Gal}(K|\mathbb{Q}) \simeq C_2^3 \rtimes S_3$ equals $1.78 \cdot 10^{17}$. Sorted by discriminant, the index of the field with largest discriminant in Theorem 7.2.1 equals $35,447$.

Our result on the second goal concerning hyperelliptic curves is as follows. For more detailed information, see Section 7.9, and in particular Table 9.1.

Theorem 7.2.3. *Heuristically, including the fields mentioned in Theorem 7.2.1, there are 3.422 CM fields K in the LMFDB for which there exists a hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathcal{O}_K$ of K. Of these fields:*

(i) 348 *have Galois group isomorphic to C_6.*

(ii) $3,057$ *have Galois group isomorphic to D_6.*

(iii) 17 *have Galois group isomorphic to $C_2^3 \rtimes S_3$.*

We have $\mathbb{Q}(i) \subset K$ for all but 19 of these fields K. Among the exceptional cases, 2 (resp. 17) have Galois group isomorphic to C_6 (resp. $C_2^3 \rtimes S_3$).

Remark 7.2.4. Considering the Galois groups in Theorem 7.2.3, and comparing these groups with the groups in Theorem 7.3.1, we notice that for the case where $\mathrm{Gal}(K|\mathbb{Q}) \cong C_2^3 \rtimes C_3$, there are no sextic CM fields K, for which there exists a hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathcal{O}_K$ of K. One of the possible further works based on this thesis is to examine these Galois group more detailed, in order to determine whether we can specify necessary and sufficient conditions which exclude this Galois group in our case. Also, another possible task related to this phenomena could be to extend the genus to be $g = 4, 5$ and to examine for these cases the corresponding Galois groups for which there exists a hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathcal{O}_K$ of K, where $\deg(K|\mathbb{Q}) = 8, 10$ in these cases.

Remark 7.2.5. Note that the classification of possible automorphism groups of hyperelliptic and non-hyperelliptic curves of genus 3 (for example in [47]) shows that if the sextic CM field K contains $\mathbb{Q}(i)$, then any curve whose Jacobian has primitive CM by K is automatically hyperelliptic. This was already used in [79]. Moreover, families of such fields are quickly found, for example by considering those defined by polynomials of the form $x^6 + d^2$. In this sense the exceptional cases with $\mathbb{Q}(i) \not\subset K$ are also the more interesting ones. For the 2 cyclic cases among them, equations for corresponding hyperelliptic curves were already determined in [1]. By contrast, our 3 new exceptional cases with Galois group $C_2^3 \rtimes S_3$ are completely new, as are the fields in Theorem 7.2.1.

Besides determining the fields involved, we can also find corresponding invariants (see Chapter 7.10). Our final main result even gives a defining equation for the field in Theorem 7.2.1 with the smallest discriminant.

Theorem 7.2.6. *Let K be the CM field of discriminant $-1 \cdot 2^8 \cdot 359^2$ defined by the polynomial $t^6 + 10t^4 + 21t^2 + 4$, and let r be a zero of the polynomial $t^4 - 5t^2 - 2t + 1$. Consider the hyperelliptic curve*

$$\begin{aligned} X: \quad y^2 = {} & x^8+(-28r^3-4r^2+132r+84)x^7+(-600r^3-160r^2+2920r+2044)x^6 \\ & +(-3532r^3-940r^2+17224r+11944)x^5+(9040r^3+2890r^2-44860r-31460)x^4 \\ & +(167536r^3+49480r^2-824532r-576212)x^3+(-226976r^3-64932r^2+1113648r+776872)x^2 \\ & +(-244204r^3-69572r^2+1197716r+835300)x+(319956r^3+94725r^2-1575062r-1100801) \end{aligned} \tag{7.2.1}$$

and the smooth plane quartic curve

$$\begin{aligned} Y: \quad & (14106r^3-150652r^2+185086r+292255)x^4+(-171112r^3+44200r^2+916008r+93360)x^3y \\ & +(-120788r^3+49032r^2+382244r+300708)x^3z+(467744r^3-209864r^2-2160704r+183416)x^2y^2 \\ & +(-72248r^3+64768r^2+347488r-362984)x^2yz+(5720r^3-12378r^2-15628r+50692)x^2z^2 \\ & +(-512608r^3+349824r^2+2423616r-580448)xy^3+(202192r^3-151024r^2-1180320r+403568)xy^2z \\ & +(6512r^3-11272r^2+178120r-71336)xyz^2+(-11832r^3+12268r^2-844r+1376)xz^3 \\ & +(263424r^3-176880r^2-1159232r+335040)y^4+(-201216r^3+100448r^2+856096r-249632)y^3z \\ & +(62112r^3+1984r^2-226512r+71624)y^2z^2+(-12520r^3-13112r^2+27736r-5360)yz^3 \\ & +(1526r^3+2411r^2-658r+197)z^4 = 0. \end{aligned} \tag{7.2.2}$$

Heuristically, there exists an isogeny of degree 2 between the Jacobians of X and Y, and both have CM by the maximal order $\mathcal{O}_K$.

7.3 Structure of sextic CM fields

In this section we recall the possible Galois groups of sextic CM fields. For all these possible groups, we give examples of minimal polynomials generating CM fields with smallest absolute discriminant in the LMFDB with corresponding Galois groups.

Theorem 7.3.1. *Let K be sextic CM field, with Galois closure L. Then $G = \mathrm{Gal}(L|\mathbb{Q})$ is isomorphic to one of the following groups:*

(i) C_6.

(ii) D_6.

(iii) $C_2^3 \rtimes C_3$.

(iv) $C_2^3 \rtimes S_3$.

In the latter two cases, the action of C_3 and S_3 on C_2^3 is given by permutation of the indices. Each possible group G above admits a unique embedding $\iota : G \to S_6$ up to conjugation in S_6 under which they become the groups 6T1, 6T3, 6T6, 6T11 from [3].

Proof. The first part follows from [20, Sec. 5.1.1] (see also [7, Proposition 2.1]). The second is a one-off calculation with the conjugacy classes of subgroups of S_6, for example by using GAP [3]. □

Remark 7.3.2. The notation 6TX for the groups in Theorem 7.3.1 can be used when searching for corresponding fields in the LMFDB [73].

Remark 7.3.3. The second part of Theorem 7.3.1 in combination with Galois theory shows that we may assume that under the chosen embedding $\iota : G \to S_6$ the subgroup $H = \mathrm{Gal}(L|K)$ is the stabilizer of 1.

Example 7.3.4. The following are the sextic CM field of smallest absolute discriminant in the LMFDB with given Galois group:

(i) C_6 is $\mathbb{Q}(\zeta_7)$.

(ii) D_6 is $x^6 - 3x^5 + 10x^4 - 15x^3 + 19x^2 - 12x + 3$.

(iii) $C_2^3 \rtimes C_3$ is $x^6 - 2x^5 + 5x^4 - 7x^3 + 10x^2 - 8x + 8$.

(iv) $C_2^3 \rtimes S_3$ is $x^6 - 3x^5 + 9x^4 - 13x^3 + 14x^2 - 8x + 2$.

7.4 CM types

In this section we restrict to the identification and classification of CM types of (sextic) CM fields K. If Φ is a CM type of K, then by Definition 6.1.5, Φ is characterized by the property

$$\mathrm{Hom}(K, \mathbb{C}) = \Phi \amalg \Phi\rho$$

where $\rho \in \mathrm{Aut}(K)$ the unique element identifying complex conjugation on K. In the further course of this thesis it is more convenient (from the computational point of view for the algorithms in this chapter, and in Chapter 8) to consider CM types on K with values in the Galois closure L of K.

Definition 7.4.1. A *CM type of K (with values in L)* is a subset $\Phi \subset \mathrm{Hom}(K, L)$ such that

$$\mathrm{Hom}(K, L) = \Phi \amalg \Phi\rho.$$

As in the classical case, we call a CM type of K *primitive* if it is not induced by a CM type of a strict CM subfield. Similarly, we call two CM types Φ, Φ' *equivalent* if there exists an automorphism $\alpha \in \mathrm{Aut}(K)$ such that $\Phi' = \Phi\alpha$.

Definition 7.4.2. As in the classical case, we call a tuple (K, Φ) a *CM type* if K is a CM field and Φ is a CM type of K.

Remark 7.4.3. Our choice of an embedding $\iota_L : L \to \mathbb{C}$ yields a map

$$\Phi \mapsto \{\iota_L \circ \tau : \tau \in \Phi\}$$

which furnishes a bijection between the CM types in Definition 7.4.1 and the CM types in Definition 6.1.5.

Lemma 7.4.4. *Let (K, Φ) be a CM type with values in the Galois closure L of K. There is a unique CM subfield $F \subset K$ and a unique CM type Φ' of F with values in L, such that Φ' is primitive, and Φ is lifted from Φ'. Then*

$$\mathrm{Gal}(L|F) = \{\sigma \in \mathrm{Gal}(L|\mathbb{Q}) : \ \sigma\Phi'_L = \Phi'_L\}.$$

Proof. See [39, Lemma 2.2] or, alternatively [69, Lemma 3.5]. □

Remark 7.4.5. Let $N = N_G(H)$ be the normalizer of H in G. Then N acts on the set of sections

$$s : \langle\rho\rangle\backslash G/H \to G/H$$

via right multiplication, and using the natural isomorphism $N/H \cong \mathrm{Aut}(K)$ induced by restriction, we see that the corresponding quotient is in bijection with the set of CM types up to equivalence. We determine this normalizer in the following proposition.

Proposition 7.4.6. *Let $G = \mathrm{Gal}(L|\mathbb{Q})$ be one of the Galois groups in Theorem 7.3.1 and let $H = \mathrm{Gal}(L|K)$. Let $N = N_G(H)$ be the normalizer of H in G. Then we have*

$$N = \begin{cases} G, & \text{if } G = C_6, \\ \langle H, \rho\rangle, & \text{else.} \end{cases}$$

Proof. We have realized our Galois groups as the explicit subgroups 6T1, 6T3, 6T6, 6T11 of S_6, and Remark 7.3.3 shows that we may take H to be the stabilizer of 1. We can choose our embeddings $G \to S_6$ in such a way that we have the following

(i) $G = C_6 = \langle\sigma\rangle$: $H = 1$, $\rho = \sigma^3$.

(ii) $G = D_6 = \langle\sigma, \tau\rangle$: $H = \langle\tau\rangle$, $\rho = \sigma^3$, where $e \in D_6$ is the identity.

(iii) $G = C_2^3 \rtimes C_3$: $H = \langle((1,0,0),e),((0,1,0),e)\rangle$, $\rho = ((1,1,1),e)$, where $e \in C_3$ is the identity.

(iv) $G = C_2^3 \rtimes S_3$: $H = \langle((1,0,0),e),((0,1,0),e),((0,0,0),(1,2))\rangle$, $\rho = ((1,1,1),e)$, where $e \in S_3$ is the identity.

The result is now a straightforward calculation. □

Definition 7.4.7. There is a natural left action of the Galois group $G = \mathrm{Gal}(L|\mathbb{Q})$ on CM types Φ of K, given by:

(i) As subsets $\Phi \subset G/H$, we have $\sigma\Phi = \{\sigma\varphi : \varphi \in \Phi\}$, for $\sigma \in G$.

(ii) On CM types considered as sections s of the projection map $G/H \to \langle\rho\rangle\backslash G/H$, the action is defined by $(\sigma s)(\langle\rho\rangle cH) = \sigma \cdot s(\langle\rho\rangle\sigma^{-1}cH)$ for $c \in G$. Note that this action is well-defined since ρ is central in G.

We call the resulting equivalence on the set of CM types of K the *Galois equivalence*.

In the following three propositions, we give an explicit description of (Galois) equivalent CM types of sextic CM fields K, depending on their Galois groups (see Theorem 7.3.1).

Proposition 7.4.8. *Let K be a sextic CM field with Galois group C_6. Then K admits:*

(i) 2 *CM types up to equivalence*, 1 *primitive and* 1 *imprimitive.*

(ii) 2 *CM types up to Galois equivalence*, 1 *primitive and* 1 *imprimitive.*

Proof. We can identify a CM type on K with a subset $S \subset C_6 = \mathbb{Z}/6\mathbb{Z}$ of cardinality 3 such that S and $3 + S$ cover $\mathbb{Z}/6\mathbb{Z}$. By Proposition 7.4.6, two such CM types S, S' are equivalent if they are related by a translation, so that $S' = i + S$ for some $i \in \mathbb{Z}/6\mathbb{Z}$, and the same is true for Galois equivalence. As is readily verified, representatives up to equivalence are given by $\{0,1,2\}$ and $\{0,2,4\}$. The latter CM type is imprimitive, since it is induced from the quotient $\mathbb{Z}/2\mathbb{Z}$ of $\mathbb{Z}/6\mathbb{Z}$ that corresponds to the unique CM quadratic subfield of K. The former type is primitive. See [7, §3.1] for a different point of view. □

Proposition 7.4.9. *Let K be a sextic CM field with Galois group D_6. Then K admits:*

(i) 4 *CM types up to equivalence,* 3 *primitive and* 1 *imprimitive.*

(ii) 2 *CM types up to Galois equivalence,* 1 *primitive and* 1 *imprimitive.*

Proof. In this case we can choose a standard representation $D_6 = \langle \sigma, \tau \rangle$. As mentioned in Remark 7.3.3, we embed D_6 it into S_6 by identifying σ with $(1\,2\,3\,4\,5\,6)$ and τ with $(2\,6)(3\,5)$. As we have seen in Proposition 7.4.6, the complex conjugation ρ is given by the central element σ^3 and $\mathrm{Gal}(L|K) = \langle \tau \rangle$. The embeddings of K into L can therefore be identified with powers σ^i, or for that matter with elements i of $\mathbb{Z}/6\mathbb{Z}$. We are in a similar situation as Proposition 7.4.8, except that the notion of equivalence is stricter. As Proposition 7.4.6 shows, this time the only other CM type equivalent to a given type $\{a, b, c\}$ is $\{a+3, b+3, c+3\}$, which corresponds to applying complex conjugation.

(i): Up to equivalence, we obtain the 4 CM types $\{0,1,2\}$, $\{0,1,5\}$, $\{0,2,4\}$, $\{0,4,5\}$. Of these types, $\{0,2,4\}$ is induced by the unique quadratic CM subfield of K and is therefore imprimitive, while the other types are primitive.

(ii): Applying Galois equivalence allows us to multiply with σ, so as in Proposition 7.4.8 we can apply arbitrary shifts to our subsets of $\mathbb{Z}/6\mathbb{Z}$ to our CM types. Once more this reduces us to the two types $\{0,1,2\}$ and $\{0,2,4\}$, the former primitive and the latter imprimitive. See [7, §3.2] for a different point of view. □

Proposition 7.4.10. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$. Then K admits:*

(i) 4 *CM types up to equivalence, which are all primitive.*

(ii) 1 *CM type up to Galois equivalence.*

Proof. (i): The statement follows as in Proposition 7.4.9, since in light of Proposition 7.4.6 applying equivalence once again comes down to identifying complex conjugate CM types, leaving 4 equivalence classes of the original 8 types. All of these types are primitive because the group H corresponding to K in the notation of Proposition 7.4.6 is not contained in any subgroup of G of index 2, or in other words because K has no proper quadratic subfields, let alone proper CM subfields.

(ii): As for working up to Galois equivalence, in the case $G = C_2^3 \rtimes C_3$ we have that

$$\begin{aligned} H &= \{((*,*,0),e)\}, & \sigma H &= \{((0,*,*),(1\,2\,3))\}, & \sigma^2 H &= \{((*,0,*),(1\,3\,2))\}, \\ \rho H &= \{((*,*,1),e)\}, & \sigma\rho H &= \{((1,*,*),(1\,2\,3))\}, & \sigma^2\rho H &= \{((*,1,*),(1\,3\,2))\}, \end{aligned} \tag{7.4.1}$$

where $*$ denotes an element of C_2 that can be chosen freely, and where $\sigma = ((0,0,0),(1\,2\,3))$. We see that $\Phi_0 = \left\{H, \sigma H, \sigma^2 H\right\}$ is a CM type. Moreover, the definition of the Galois action along with that of the group structure on G implies that for $n_1 = ((1,0,0),e)$ we have

$$n_1 H = H = \{((*,*,0),e)\} \qquad n_1\sigma H = \sigma\rho H = \{((1,*,*),(1\,2\,3))\} \qquad n_1\sigma^2 H = \sigma^2 H = \{((*,*,0),(1\,3\,2))\}. \tag{7.4.2}$$

Similarly, $n_2 = ((0,1,0),e)$ sends Φ_0 to $\left\{H, \sigma H, \sigma^2\rho H\right\}$ and $n_0 = ((0,0,1),e)$ sends Φ_0 to $\left\{\rho H, \sigma H, \sigma^2 H\right\}$. Combining the action of these three elements is enough to obtain transitivity of the Galois action on the full set of CM types $\left\{\rho^*, \sigma\rho^*, \sigma^2\rho^*\right\}$.

The considerations for $G = C_2^3 \rtimes S_3$ are completely identical, with the small difference that

$$\begin{aligned} H &= \{((*,*,0), e \text{ or } (1\,2))\}, \quad \sigma H = \{((0,*,*), (1\,2\,3) \text{ or } (1\,3))\}, \quad \sigma^2 H = \{((*,0,*), (1\,3\,2) \text{ or } (2\,3))\}, \\ \rho H &= \{((*,*,1), e \text{ or } (1\,2))\}, \quad \sigma\rho H = \{((1,*,*), (1\,2\,3) \text{ or } (1\,3))\}, \quad \sigma^2\rho H = \{((*,1,*), (1\,3\,2) \text{ or } (2\,3))\}. \end{aligned} \tag{7.4.3}$$

□

7.5 Reflex CM types

Let (K,Φ) be a CM type, where Φ is a CM type of K with values in the Galois closure L of K. In this section we recall the construction of the reflex CM type (K^r,Φ^r), where K^r is the reflex field of (K,Φ) and where Φ^r is the reflex CM Type of (K,Φ).

Let Φ_L be the unique CM type on L induced by Φ, where elements in Φ_L are identified by elements in $\mathrm{Gal}(L|\mathbb{Q})$. Inverting elements in Φ_L gives rise to a unique CM type on L given by

$$\Phi_L^{-1} = \{\varphi^{-1} : \varphi \in \Phi_L\}.$$

One can show that Φ_L^{-1} is a CM type if and only if Φ_L is a CM type. By Lemma 7.4.4 there is a unique primitive CM type (K^r,Φ^r) that induces (L,Φ_L^{-1}).

Definition 7.5.1. The CM field K^r is the fixed field of the group

$$H^r = \{\sigma \in \mathrm{Gal}(L|\mathbb{Q}) : \sigma\Phi_L = \Phi_L\}$$

and

$$\Phi^r = \Phi_L^{-1}|_{K^r} = \left\{\varphi|_{K^r} :\ \varphi \in \Phi_L^{-1}\right\}$$

is the unique CM type on K^r that induces Φ_L^{-1}. We call (K^r,Φ^r) the *reflex CM type* of (K,Φ). See [39, Chapter 1.5]or, alternatively [69, Page 30].

Proposition 7.5.2. *Let (K,Φ) be a CM type with reflex CM type (K^r,Φ^r). Then Φ^r is a primitive CM type on K^r. If (K^{rr},Φ^{rr}) is the reflex CM type of (K^r,Φ^r) then :*

(i) $K^{rr} \subset K$, and Φ is induced by Φ^{rr}.

(ii) If Φ is primitive, then $(K^{rr},\Phi^{rr}) = (K,\Phi)$.

Proof. See [39, Theorem 5.2] or [69, Lemma 7.2], respectively. □

A characterization of the reflex CM types (K^r,Φ^r) of (K,Φ) depending on the Galois groups of K (see Theorem 7.3.1), is given by the following propositions.

Proposition 7.5.3. *Let (K,Φ) be a sextic CM type where K has Galois group isomorphic to C_6. Then:*

(i) If Φ is primitive, then $(K^r,\Phi^r) = (K,\Phi)$.

(ii) If Φ is imprimitive, then (K^r,Φ^r) is the restriction of (K,Φ) to the quadratic CM subfield of K.

Proof. As we have seen in Proposition 7.4.8, there are 2 equivalence classes of CM types, namely $\{0,1,2\}$ and $\{0,2,4\}$ and where the latter is imprimitive. An easy calculation shows that in case (i), $H^r = H = \{1\}$, in case (ii), $H^r = \{1,\sigma^2,\sigma^4\}$, and this shows the claim. □

To deal with the case $G = D_6$, we first prove the following general statement.

Proposition 7.5.4. *Let Φ, Ψ be two CM types of a given field K, and suppose that $\Psi = \sigma\Phi$ for $\sigma \in G = \mathrm{Gal}(L|\mathbb{Q})$. Let (K^r, Φ^r) be the reflex CM type of (K, Φ). Then the reflex CM type of (K, Ψ) is given by*

$$(\sigma(K^r), \Phi^r\sigma^{-1}),$$

where

$$\Phi^r\sigma^{-1} = \left\{(\varphi\sigma^{-1})|_{\sigma(K^r)} : \varphi \in \Phi^r\right\}.$$

Proof. For the extensions of Φ and Ψ to L we have $\Psi_L = \sigma\Phi_L$. For the corresponding left stabilizers H_Φ and H_Ψ we therefore have $H_\Psi = \sigma H_\Phi \sigma^{-1}$, which already shows that the reflex field of Ψ equals $\sigma(K)$. By construction, we have

$$\Phi_L^{-1} = \coprod_{\varphi \in \Phi^r} \varphi H_\Phi,$$

so that

$$\Psi_L^{-1} = \Phi_L^{-1}\sigma^{-1} = \coprod_{\varphi \in \Phi^r} \varphi H_\Phi \sigma^{-1} = \coprod_{\varphi \in \Phi^r} \varphi\sigma^{-1} H_\Psi.$$

Restricting to the reflex field of Ψ, we obtain the statement of the proposition. □

Proposition 7.5.5. *Let (K, Φ) be a sextic CM type where K has Galois group isomorphic to D_6.*

(i) If Φ is primitive, then write $\Phi = \sigma\Phi_0$, where Φ_0 corresponds to the set $\{0, 1, 5\}$ in the notation of Proposition 7.4.9. Then $(K^r, \Phi^r) = (\sigma(K^r), \Phi_0^r\sigma^{-1})$.

(ii) If Φ is imprimitive, then (K^r, Φ^r) is the restriction of (K, Φ) to the quadratic CM subfield of K.

Proof. This follows from 7.5.4 because the left stabilizer of Φ_0 is again generated by the element τ in Proposition 7.4.9. □

The reflex fields for the remaining Galois groups are described in the upcoming propositions.

Proposition 7.5.6. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$, and let $\sigma = ((0,0,0),(1\,2\,3))$ and $\rho = ((1,1,1), e)$ as in Proposition 7.4.6. Let*

$$\Phi_1 = \{\mathrm{id}|_K, \sigma|_K, \sigma^2|_K\}, \quad \Phi_2 = \{\mathrm{id}|_K, \sigma\rho|_K, \sigma^2|_K\}, \quad \Phi_3 = \{\mathrm{id}|_K, \sigma|_K, \sigma^2\rho|_K\}, \quad \Phi_4 = \{\mathrm{id}|_K, \sigma\rho|_K, \sigma^2\rho|_K\}$$

be representatives of the primitive CM types of K up to equivalence. Then the reflex field K^r of (K, Φ_i) is fixed by the group $H_i^r \subset \mathrm{Gal}(L|\mathbb{Q})$, where

$$H_1^r = \langle\sigma\rangle,\ H_2^r = \langle\sigma n_0 n_1\rangle,\ H_3^r = \langle\sigma n_1 n_2\rangle,\ H_4^r = \langle\sigma n_0 n_2\rangle,$$

with n_i as defined in the proof of Proposition 7.4.10. We have

$$K_2^r = n_1(K_1^r),\ K_3^r = n_2(K_1^r),\ K_4^r = n_1 n_2(K_1^r).$$

The reflex CM types Φ_i^r are all given by

$$\Phi_1^r = \Phi_2^r = \Phi_3^r = \Phi_4^r = \{\mathrm{id}|_{K_i^r}, n_1|_{K_i^r}, n_2|_{K_i^r}, n_1 n_2|_{K_i^r}\}.$$

Proof. Let $H = \{e, n_1, n_2, n_1 n_2\}$ be the subgroup of the Galois group corresponding to K. First consider the CM type Φ_1. The induced CM type $\Phi_{1,L}$ on L is the union

$$H \cup \sigma H \cup \sigma^2 H = \{((*,*,0), e)\} \cup \{((0,*,*), (1\,2\,3))\} \cup \{((*,0,*), (1\,3\,2))\}.$$

From this explicit presentation, one obtains that the left stabilizer H_1^r of $\Phi_{1,L}$ is generated by σ. Using equalities similar to (7.4.2) shows that $\Phi_2 = n_1\Phi_1$, $\Phi_3 = n_2\Phi_1$, and $\Phi_4 = n_1 n_2 \Phi_1$. The corresponding stabilizers are therefore given generated by $n_1 \sigma n_1^{-1} = \sigma n_0 n_1$, $n_2 \sigma n_2^{-1} = \sigma n_1 n_2$, and $n_1 n_2 \sigma (n_1 n_2)^{-1} = \sigma n_0 n_2$.

The embeddings in the reflex CM type of Φ_1 are in bijective correspondence with the elements of

$$\Phi_{1,L}^{-1} = H^{-1} \cup H^{-1}\sigma^{-1} \cup H^{-1}\sigma^{-2} = H \cup H\sigma^{-1} \cup H\sigma^{-2}$$

up to the action of the right stabilizer $H_1^r = \langle \sigma \rangle$. These are therefore represented by the elements of H, which yields the second statement of the proposition for Φ_1. Since $\Phi_2 = n_1\Phi_1$, $\Phi_3 = n_2\Phi_1$, and $\Phi_4 = n_1 n_2 \Phi_1$, representatives of the corresponding inverse CM types up to the right action of the corresponding stabilizers are furnished by $n_1 H, n_2 H$, and $n_1 n_2 H$. These are all equal to H, and therefore we obtain the second statement for all CM types Φ_i. □

Proposition 7.5.7. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes S_3$, let $\sigma = ((0,0,0),(1\,2\,3))$, let $\tau = ((0,0,0),(1\,2))$, let $\rho = ((1,1,1), e)$, and let*

$$\Phi_1 = \{\mathrm{id}|_K, \sigma|_K, \sigma^2|_K\}, \quad \Phi_2 = \{\mathrm{id}|_K, \sigma\rho|_K, \sigma^2|_K\}, \quad \Phi_3 = \{\mathrm{id}|_K, \sigma|_K, \sigma^2\rho|_K\}, \quad \Phi_4 = \{\mathrm{id}|_K, \sigma\rho|_K, \sigma^2\rho|_K\}$$

be representatives of the primitive CM types of K up to equivalence. Then the reflex field K^r of (K, Φ_i) is fixed by the group $H_i^r \subset \mathrm{Gal}(L|\mathbb{Q})$, where

$$H_1^r = \langle \sigma, \tau \rangle, \; H_2^r = \langle \sigma n_0 n_1, \tau n_1 n_2 \rangle, \; H_3^r = \langle \sigma n_1 n_2, \tau n_1 n_2 \rangle, \; H_4^r = \langle \sigma n_0 n_2, \tau \rangle,$$

with n_i as defined in the proof of Proposition 7.4.10. We have

$$K_2^r = n_1(K_1^r), \; K_3^r = n_2(K_1^r), \; K_4^r = n_1 n_2 (K_1^r).$$

The reflex CM types Φ_i^r are all given by

$$\Phi_1^r = \Phi_2^r = \Phi_3^r = \Phi_4^r = \{\mathrm{id}|_{K_i^r}, n_1|_{K_i^r}, n_2|_{K_i^r}, n_1 n_2|_{K_i^r}\}.$$

Proof. The proof is similar to that of the previous proposition. □

Corollary 7.5.8. *Let K be a sextic CM field. Then all primitive CM types of K are Galois equivalent.*

Proof. We proved this result in Propositions 7.4.8, 7.4.9, and 7.4.10, which cover all individual cases in Theorem 7.3.1. □

Remark 7.5.9. In genus 4, it is no longer true that all primitive CM types are Galois equivalent. Let K be an octic CM field with Galois group C_8, for example $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{15})$. Then (with notation as in the case C_6 above) the CM types $\{0,1,2,3\}$ and $\{0,1,2,6\}$ are primitive, yet they are not related even when combining the two equivalences.

Remark 7.5.10. Depending of the possible Galois groups of sextic CM fields (see Theorem 7.3.1), the next lemma gives a description of the so-called *field of moduli* of principally polarized abelian varieties A over $\mathbb{C}$ with primitive CM by K. In a naive way, the field of moduli of A is the average of all fields of definition of A. For a detailed discussion about fields of moduli, see e.g. [39, Chapter 5].

Lemma 7.5.11. *Let A be a principally polarized abelian variety over $\mathbb{C}$ with* primitive *CM by K up to equivalence, and let $G = \mathrm{Gal}(L|\mathbb{Q})$, Then:*

(i) If $G \cong D_6$, then the degree of the field of moduli of A over $\mathbb{Q}$ is a multiple of 3.

(ii) $G \cong C_2^3 \rtimes C_3, C_2^3 \rtimes S_3$, then the degree of the field of moduli of A over $\mathbb{Q}$ is a multiple of 4.

Proof. This follows because the subgroup of $\mathrm{Aut}(\mathbb{C})$ that fixes the field of moduli has to fix the primitive CM type up to equivalence of A by Proposition 6.2.7, combined with the transitivity of the Galois action which we will prove in Corollary 7.5.8. □

7.6 The Shimura class group and the Galois action

A crucial role in understanding one of the main structures in this chapter, the locus $\mathcal{M}_{\mathcal{O}_K}(\Phi) \subset \mathcal{A}_3(\overline{\mathbb{Q}})$ (see Definition 7.7.1) of principally polarized abelian varieties with primitive CM by $\mathcal{O}_K$ of type (K, Φ), is to understand the Shimura class group $\mathcal{C}_K$ of K, as well as the image of the map $\mathcal{N}_{\Phi^r}$ (see Definition 7.6.5) inside $\mathcal{C}_K$. By the Main Theorem of CM (see Theorem 7.8.1), orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$ correspond to the elements of the quotient $\mathcal{C}_K/\mathrm{im}(\mathcal{N}_{\Phi^r})$. We start this section with the following definition.

Definition 7.6.1. Let K be a CM field. The *Shimura class group* $\mathcal{C}_K$ of K is the abelian group of equivalence classes

$$\mathcal{C}_K = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \text{ is fractional } \mathcal{O}_K\text{-ideal, } \beta \in K_0^* \text{ totally positive with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathcal{O}_K\right\}/\sim \tag{7.6.1}$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$. The multiplication of two equivalence classes $(\mathfrak{b}, \beta)$ and $(\mathfrak{b}', \beta')$ is given by

$$(\mathfrak{b}, \beta) \cdot (\mathfrak{b}', \beta') = (\mathfrak{b}\mathfrak{b}', \beta\beta')$$

and the identity element is given by $(\mathcal{O}_K, 1)$. See [63, Page 107].

Notation 7.6.2. Let K be a CM field with totally real number field $K_0 \subset K$. We denote by $\mathrm{Cl}^+(K_0)$ the *narrow class group* of K_0, where elements in $Cl^+(K_0)$ correspond to equivalence classes of fractional K_0-ideals modulo totally positive principal fractional K_0-ideals, for any embedding of K_0 into $\mathbb{R}$.

The structure of $\mathcal{C}_K$ is given by the sequence

$$1 \to (\mathcal{O}_{K_0}^*)^+/N_{K|K_0}(\mathcal{O}_K^*) \xrightarrow{u \longmapsto (\mathcal{O}_K, u)} \mathcal{C}_K \xrightarrow{(\mathfrak{b},\beta) \longmapsto \mathfrak{b}} \mathrm{Cl}(K) \xrightarrow{N_{K|K_0}} \mathrm{Cl}^+(K_0), \tag{7.6.2}$$

where $(\mathcal{O}_{K_0}^*)^+ \subset \mathcal{O}_{K_0}^*$ is the group of totally positive units, and $\mathrm{Cl}^+(K_0)$ is the narrow class group of K_0. See [9, Theorem 3.1].

Remark 7.6.3. As is discussed in [9], the final map in (7.6.2) is surjective if a finite prime ramifies in the extension $K|K_0$. This turns out to be the case for all fields considered in [17, 19], as follows by checking that the relative different $\mathcal{D}_{K|K_0} = \{\alpha - \rho(\alpha) : \alpha \in \mathcal{O}_K\}$ is a proper ideal (also see the proof of [70, Proposition 4.4]). Under this hypothesis, denoting $h(K) = |\mathrm{Cl}(K)|$ and $h^+(K_0) = |\mathrm{Cl}^+(K_0)|$, we have

$$|\mathcal{C}_K| = \frac{h(K)}{h^+(K_0)} \cdot \left|(\mathcal{O}_{K_0}^*)^+/N_{K|K_0}(\mathcal{O}_K^*)\right|. \tag{7.6.3}$$

Definition 7.6.4. Let (K,Φ) be a CM type with reflex CM type (K^r,Φ^r). The *reflex type norm* map is given by

$$\begin{aligned} N_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathrm{Cl}(K) \\ [\mathfrak{a}] &\mapsto \left[\mathcal{O}_K \cap \prod_{\varphi\in\Phi^r} \varphi(\mathfrak{a})\mathcal{O}_L\right]. \end{aligned} \tag{7.6.4}$$

Definition 7.6.5. Let $N = N_{K^r|\mathbb{Q}}$ be the extension of the absolute norm-map to fractional $\mathcal{O}_{K^r}$-ideals. Combining this map with the reflex type norm in Equation (8.3.2), we obtain a map from the regular class group of K^r to the Shimura class group of K, namely

$$\begin{aligned} \mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathcal{C}_K \\ [\mathfrak{a}] &\mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})). \end{aligned} \tag{7.6.5}$$

7.7 Torsor and moduli spaces

Definition 7.7.1. We define by $\mathcal{M}_{\mathcal{O}_K}$ the set of isomorphism classes of principally polarized abelian varieties with primitive CM by $\mathcal{O}_K$. Given a primitive CM type Φ, we define by $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ the set of isomorphism classes of principally polarized abelian varieties that admit CM of type Φ.

Proposition 7.7.2. *There is a disjoint union $\mathcal{M}_{\mathcal{O}_K} = \bigcup_\Phi \mathcal{M}_{\mathcal{O}_K}(\Phi)$, where Φ runs over a set of representatives of the equivalence classes of primitive CM types of K.*

Proof. This follows from the fact that given a principally polarized abelian variety (A,E) with primitive CM by K, the CM type of (A,E) is uniquely determined up to equivalence, as recapitulated at the end of Section 6.2. □

Definition 7.7.3. We define the abelian group

$$C = \left\{(\mathfrak{b},\beta) : \mathfrak{b} \text{ is fractional } \mathcal{O}_K\text{-ideal},\ \beta \in K^* \text{ with } \mathfrak{b}\bar{\mathfrak{b}} = \beta\mathcal{O}_K\right\}/\sim$$

where $(\mathfrak{b},\beta) \sim (\mathfrak{b}',\beta')$ if $(\mathfrak{b}',\beta') = (x\mathfrak{b}, x\bar{x}\beta)$ for $x \in K^*$. The multiplication of two equivalence classes $(\mathfrak{b},\beta)$ and $(\mathfrak{b}',\beta')$ is given by

$$(\mathfrak{b},\beta)\cdot(\mathfrak{b}',\beta') = (\mathfrak{b}\mathfrak{b}',\beta\beta')$$

and the identity element is given by $(\mathcal{O}_K,1)$. There is an inclusion of groups $\mathcal{C}_K \hookrightarrow C$ induced by the identity-map. The group C acts (from left) on pairs

$$(\mathfrak{a},\xi), \tag{7.7.1}$$

where $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal and where ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K, and where $\varphi(\xi)$ is an positive imaginary element, for any $\varphi \in \Phi$ and any CM type Φ of K, and where $(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$ (see Section 6.2), via

$$(\mathfrak{b},\beta)\cdot(\mathfrak{a},\xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi).$$

Proposition 7.7.4. *Let $c = (\mathfrak{b},\beta) \in C$, and let*

$$(\mathfrak{b},\beta)\cdot(\mathfrak{a},\xi) = (\mathfrak{a}',\xi'),$$

for $(\mathfrak{a},\xi)$ as in Equation (7.7.1) (Section 6.2, respectively). Let Φ' be the CM type of $(\mathfrak{a}',\xi')$. Then $\Phi' = \Phi$ if and only if $c \in \mathcal{C}_K$.

Proof. This follows because the imaginary parts of ξ and ξ' have positive signs at the same complex embeddings if and only if β is totally positive. □

Remark 7.7.5. Let $c = (\mathfrak{b}, \beta) \in C$ and $(\mathfrak{a}, \xi)$ be as in Equation (7.7.1). If $\mathfrak{b}$ is integral, then $\mathfrak{b}^{-1}\mathfrak{a}$ properly contains $\mathfrak{a}$. Proposition 7.7.4 shows that if $c \in \mathcal{C}_K$, the pairs $(\mathfrak{a}, \xi)$ and $c(\mathfrak{a}, \xi)$ have the same CM type Φ. This means that for $c \in \mathcal{C}_K$ the inclusion $\Phi(\mathfrak{a}) \subset \Phi(\mathfrak{b}^{-1}\mathfrak{a})$ furnishes a canonical isogeny

$$A(\mathfrak{a}, \xi) \to A((\mathfrak{b}, \beta) \cdot (\mathfrak{a}, \xi))$$

between principally polarized abelian varieties with primitive CM by $\mathcal{O}_K$ given by

$$(a, \xi) \mapsto A(\mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E_\xi)$$

and

$$((\mathfrak{b}, \beta) \cdot (\mathfrak{a}, \xi)) \mapsto A((\mathfrak{b}, \beta) \cdot (\mathfrak{a}, \xi)) = A(\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi) = (\mathbb{C}^g/\Phi(\mathfrak{b}^{-1}\mathfrak{a}), E_{\beta\xi}).$$

Notation 7.7.6. Let K be a CM field with totally real subfield $K_0 \subset K$. We denote by H the *Hilbert class field* of K and, by H_0^+ the *narrow Hilbert class field* of K_0, respectively. Then $H_0^+ \subset H$ by construction, H is the maximal unramified abelian extension of K, and H_0^+ is the maximal unramified abelian extension outside the set containing of all the real infinite primes of K_0 corresponding to the set of real embeddings $K_0 \hookrightarrow \mathbb{R}$. See e.g. [16, Chapters 2 and 8].

Proposition 7.7.7. *Let K be a sextic CM field, and let Φ be a fixed primitive CM type. Then the set $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is a torsor under the action of $\mathcal{C}_K$.*

Proof. Proposition 6.2.3 shows that $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is a torsor if it is non-empty. Since $\mathcal{M}_{\mathcal{O}_K} = \bigcup_\Phi \mathcal{M}_{\mathcal{O}_K}(\Phi)$, where Φ runs over the primitive CM types of K up to equivalence, and since the Galois action on the components is transitive by Corollary 7.5.8, it suffices to prove that $\mathcal{M}_{\mathcal{O}_K} \neq \emptyset$ in order to show that that one, and hence all, of the $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ with Φ primitive are torsors under $\mathcal{C}_K$.

For this, let $(\mathfrak{a}_0, \xi_0)$ be the pair explicitly constructed in [70, Proposition 4.4], which has CM by $\mathcal{O}_K$. If the CM type Φ_0 associated to $(\mathfrak{a}_0, \xi_0)$ is primitive, then we are done. So suppose that Φ_0 is imprimitive. Then we consider the narrow Hilbert class field H_0^+ of the totally real subfield K_0 of K and the Hilbert class field H of K. The final map in the sequence in Equation (7.6.2) fits into a commutative diagram

$$\begin{array}{ccc} \mathrm{Cl}(K) & \xrightarrow{N_{K|K_0}} & \mathrm{Cl}^+(K_0) \\ \downarrow\sim & & \downarrow\sim \\ \mathrm{Gal}(H|K) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(H_0^+|K_0) \end{array} \tag{7.7.2}$$

where the map on the bottom is restriction. The inclusion $KH_0^+ \subset H$ yields a surjective restriction map $\mathrm{Gal}(H|K) \to \mathrm{Gal}(KH_0^+|K)$. By Galois theory, the latter group is isomorphic to $\mathrm{Gal}(H_0^+|K \cap H_0^+)$. Since $K \cap H_0^+$ is an at most quadratic extension of K_0, we see that the image N of $N_{K|K_0}$ is of index at most 2 in $\mathrm{Cl}^+(K_0)$.

Let $\mathrm{I}\mathfrak{d}(K_0)$ be the group of fractional $\mathcal{O}_{K_0}$-ideals. Fix an enumeration of the real embeddings of K_0, and given an element $\alpha \in K_0^*$, let $\mathrm{sgn}_i(\alpha)$ denote the sign of α under the ith embedding. Then under the map

$$[\mathfrak{a}] \mapsto [(\mathfrak{a}, (1, 1, 1))]$$

the narrow class group $\mathrm{Cl}^+(K_0)$ becomes isomorphic to the group $\mathfrak{Id}(K_0)\times\langle -1\rangle^3$ modulo the equivalence relation

$$(\mathfrak{a},(s_1,s_2,s_3))\sim(\mathfrak{a}',(s_1',s_2',s_3'))$$

if there exists $\alpha\in K_0^*$ such that $\mathfrak{a}'=\alpha\mathfrak{a}$ and $s_i'=\mathrm{sgn}_i(\alpha)s_i$. The exact sequence

$$0\to\langle -1\rangle^3\to\mathfrak{Id}(K_0)\times\langle -1\rangle^3\to\mathfrak{Id}(K_0)\to 0$$

induces

$$0\to S\to\mathrm{Cl}^+(K_0)\to\mathrm{Cl}(K_0)\to 0 \tag{7.7.3}$$

where S is the quotient of $\langle -1\rangle^3$ by the image of $\mathcal{O}_{K_0}^*$ under the sign maps.

As before, let N be the image of $\mathrm{Cl}(K)$ in $\mathrm{Cl}^+(K_0)$ under the norm map. Since [77, Theorem 10.1] shows that the norm map $\mathrm{Cl}(K)\to\mathrm{Cl}(K_0)$ is surjective, and N is of index at most 2 in $\mathrm{Cl}^+(K_0)$, we see that $N\cap S$ is of index at most 2 in S. By (7.7.3) this implies that there exists a $\mathcal{O}_K$-ideal $\mathfrak{b}$ such that $\mathfrak{b}\overline{\mathfrak{b}}$ is generated by an element $\beta\in K_0$ whose signs at the infinite places of K_0 do not all coincide.

Now let $(\mathfrak{a},\xi)=(\mathfrak{b},\beta)\cdot(\mathfrak{a}_0,\xi_0)$. Then because of the sign property of β, the CM type Φ corresponding to $(\mathfrak{a},\xi)$ differs from both Φ_0 and $\overline{\Phi}_0$. Our classification of the CM types of sextic CM fields in Section 7.4 then shows that Φ is primitive. Therefore $\mathcal{M}_{\mathcal{O}_K}$ is non-empty, since it contains the ppav corresponding to $(\mathfrak{a},\xi)$. □

Definition 7.7.8. We define the number of pairs (Φ,A), where Φ is a CM type of K (not necessarily primitive), and where A is an isomorphism class of principally polarized abelian varieties that admits Φ as a CM type, by the quotient

$$s_K=\frac{\mathrm{Cl}(K)}{\mathrm{Cl}(K_0)}\left|\mathcal{O}_{K_0}^*/N_{K|K_0}(\mathcal{O}_K^*)\right|,$$

where K_0 is the totally real subfield of K and where $N_{K|K_0}$ is the relative norm-map on fractional $\mathcal{O}_K$-ideals. See [70, Proposition 4.4].

Proposition 7.7.9. *Let K be a sextic CM field with Galois closure L. Then we have*

$$\left|\mathcal{M}_{\mathcal{O}_K}\right|=\begin{cases}|\mathcal{C}_K|=\frac{1}{8}s_K & \text{if } K \text{ is Galois},\\ 3\,|\mathcal{C}_K|=\frac{3}{8}s_K & \text{if } \mathrm{Gal}(L|\mathbb{Q})\cong D_6,\\ 4\,|\mathcal{C}_K|=\frac{1}{2}s_K & \text{if } \mathrm{Gal}(L|\mathbb{Q})\cong C_2^3\rtimes C_3 \text{ or } C_2^3\rtimes S_3.\end{cases}$$

Proof. The first equalities involving $|\mathcal{C}_K|$ follow by combining Proposition 7.7.2, 7.4.8, 7.4.9, and 7.4.10.

As for the second equalities, if $\mathrm{Gal}(L|\mathbb{Q})$ is isomorphic to either $C_2^3\rtimes C_3$ or $C_2^3\rtimes S_3$, then all CM types Φ of K are primitive and Proposition 7.7.7 shows that $s_K=8\,|\mathcal{C}_K|$.

If $\mathrm{Gal}(L|\mathbb{Q})$ is isomorphic to C_6 or D_6, then Proposition 7.7.7 shows that $|M_K(\Phi)|=|\mathcal{C}_K|$ for all 6 primitive CM types of K. If $|M_K(\Phi)|=0$ for one (and hence both) of the imprimitive CM types of K, then we would have $s_K=6\,|\mathcal{C}_K|$. On the other hand, comparing the exact sequence in [70, Proposition 4.4] with (7.6.2) shows that $s_K/|\mathcal{C}_K|$ is a power of 2. This contradiction shows that $s_K=8\,|\mathcal{C}_K|$ for all cases, which yields the statement. □

Corollary 7.7.10. *The statement of Proposition 7.7.7 also holds for imprimitive CM types Φ of sextic CM fields.*

Proof. This follows from the proof of Corollary 7.7.9. □

7.8 Representatives up to Galois conjugacy

For the rest of this section we fix a primitive CM type Φ of K. The set $\mathcal{M}_K(\Phi)$ of isomorphism classes of principally polarized abelian varieties with primitive CM by $\mathcal{O}_K$ of type Φ (see Definition 7.7.1) is stable under the action of $G^r = \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$ (see [69, Chapter 3, Lemma 1.1]), and the orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the action of the group G^r correspond to the elements of the quotient $\mathcal{C}_K/\mathrm{im}(\mathcal{N}_{\Phi^r})$. More precisely, we have the following result.

Theorem 7.8.1 (Main Theorem of Complex Multiplication)**.** *Let $(A,E) \cong A(\mathfrak{a},\xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$, and let $\sigma \in G^r$. Suppose that under the Artin map, the element σ correspond the class of the ideal $\mathfrak{b}$. Then*

$$\sigma(A(\mathfrak{a},\xi)) \cong A(\mathcal{N}_{\Phi^r}(\mathfrak{b})(\mathfrak{a},\xi)). \tag{7.8.1}$$

Proof. See [39, Theorem 6.1]. □

Remark 7.8.2. We will use this reciprocity law to prove Theorem 7.8.10, which shows that given $A(\mathfrak{a}_0,\xi_0)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$, we can obtain any other isomorphism class $A(\mathfrak{a},\xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ as a Galois conjugate of an abelian variety

$$A(\mathfrak{b}\mathfrak{a}_0,\eta_0),$$

where $\mathfrak{b}$ runs through a fixed (small) set of representatives of the quotient

$$\frac{G_2}{eG_2},$$

where $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$ and where $e|4$. The usefulness of this result stems from the fact that G_2/eG_2 is usually far smaller than G_2 itself. We start with a general observation.

Proposition 7.8.3. *Let Φ and Ψ be Galois equivalent CM types. Then there is an equality of double reflex maps*

$$N_{\Phi^r} \circ N_\Phi = N_{\Psi^r} \circ N_\Psi.$$

Proof. Let $\Psi = \sigma(\Phi)$ for $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$. Then we have

$$N_\Psi(\mathfrak{a}) = \prod_{\psi\in\Psi} \psi(\mathfrak{a}) = \prod_{\varphi\in\Phi} \sigma(\varphi(\mathfrak{a})) = \sigma(\prod_{\varphi\in\Phi} \varphi(\mathfrak{a})) = \sigma(N_\Phi(\mathfrak{a}))$$

for all ideals $\mathfrak{a}$ of $\mathcal{O}_K$. Moreover, by Proposition 7.5.4 we have

$$N_{\Psi^r}(\mathfrak{b}) = \prod_{\psi\in\Psi^r} \psi(\mathfrak{b}) = \prod_{\varphi\in\Phi^r} \varphi(\sigma^{-1}(\mathfrak{b}))$$

for all ideals $\mathfrak{b}$ of $\mathbb{Z}_{K^r}$. Therefore

$$N_{\Psi^r}(N_\Psi(\mathfrak{a})) = N_{\Psi^r}(\sigma(N_\Phi(\mathfrak{a}))) = \prod_{\varphi\in\Phi^r} \varphi(\sigma^{-1}(\sigma(N_\Phi(\mathfrak{a})))) = \prod_{\varphi\in\Phi^r} \varphi(N_\Phi(\mathfrak{a})) = N_{\Phi^r}(N_\Phi(\mathfrak{a}))$$

for all ideals $\mathfrak{a}$ of $\mathcal{O}_K$, which proves our claim. □

Lemma 7.8.4. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6. Then there exists a primitive CM type Ψ such that for all primitive CM types Φ and for all fractional $\mathcal{O}_K$-ideals $\mathfrak{a}$ we have an equality of fractional $\mathbb{Z}_L$-ideals*

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1} N_\Psi(\mathfrak{a}).$$

If Φ is imprimitive, then $N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_\Phi(\mathfrak{a})$.

Proof. We prove the statement for the case where the Galois group is isomorphic to D_6. The Galois case is similar. Using the notation in Proposition 7.4.9, let $H = \mathrm{Gal}(L|K) = \langle\tau\rangle$, and let σ be the generator of the set of embeddings of K into L. By Proposition 7.8.3, it suffices to consider the case $\Phi_L = \{0,1,2\}$ where the entries in Φ_L are the exponents i of σ^i in the representation of the extension of the primitive CM type Φ to L. Then $\Phi_L^r = \{0,5,4\}$, and the double norm computation gives rise to the element

$$(1+\sigma^5+\sigma^4)(1+\sigma+\sigma^2) = 3+2\sigma+\sigma^2+\sigma^4+2\sigma^5$$

in the group algebra of $\mathrm{Gal}(L|\mathbb{Q})$. If we consider the elements in this sum up to right multiplication by elements of the group H, we get

$$\begin{aligned}3H+2\sigma H+\sigma^2 H+\sigma^4 H+2\sigma^5 H = (H+\sigma H+\sigma^2 H+\sigma^3 H+\sigma^4 H+\sigma^5 H)\\ +(H-\sigma^3 H)+(H+\sigma H+\sigma^5 H).\end{aligned}$$

The first two terms correspond to $N_{K|\mathbb{Q}}(\mathfrak{a})$ and $\mathfrak{a}\overline{\mathfrak{a}}^{-1}$, respectively. The last sum corresponds to the CM type $\Psi_L = \{0,1,5\}$, and is independent of the choice of Φ_L.

In the imprimitive case we can take $\Phi_L = \{0,2,4\}$. The reflex field is then the unique quadratic CM subfield of K, and the reflex type its canonical inclusion, which shows our claim. □

Proposition 7.8.5. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6, and let Φ be a primitive CM type of K. If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathcal{O}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^2]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$ in Equation* (8.3.2).

Proof. First let Ψ be the distinguished primitive CM type in Lemma 7.8.4. If $\mathfrak{a} = N_\Psi(\mathfrak{b})\mathbb{Z}_L$, then by Lemma 7.8.4 we have an equality of fractional $\mathbb{Z}_L$-ideals

$$N_{\Psi^r}(\mathfrak{a}) = N_{\Psi^r}(N_\Psi(\mathfrak{b})) = N_{K|\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1}N_\Psi(\mathfrak{b}) = N_{K|\mathbb{Q}}(\mathfrak{b})\beta^{-1}N_{\Psi^r}(\mathfrak{b})\mathfrak{b}^2. \tag{7.8.2}$$

We therefore have that $N_{\Psi^r}([\mathfrak{a}]) = N_{\Psi^r}([\mathfrak{b}])[\mathfrak{b}^2]$ and $[\mathfrak{b}^2] = N_{\Psi^r}([\mathfrak{a}\mathfrak{b}^{-1}]) \in \mathrm{im}(N_{\Psi^r})$. But Proposition 7.5.4 implies that if $\Phi = \sigma(\Psi)$, then $\Phi^r = \Psi^r\sigma^{-1}$, so that N_{Φ^r} and N_{Ψ^r} have equal images in $\mathrm{Cl}(K)$. (Indeed, if $\mathfrak{b} = N_{\Psi^r}(\mathfrak{c})$, then $\mathfrak{b} = N_{\Phi^r}(\sigma(\mathfrak{c}))$.) Since all primitive CM types are Galois equivalent, we obtain our claim. □

Proposition 7.8.6. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6. For any primitive CM type Φ of K and any equivalence class $(\mathfrak{b},\beta)$ in $\mathcal{C}_K$ the equivalence class of $(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2)$ is in the image of the map $\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K$ in Equation* (8.3.3). *Furthermore, if $N_\Psi(\mathfrak{b}) = \mu\mathcal{O}_K$ is a principal $\mathcal{O}_K$-ideal, then said image $(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2)$ is equivalent to $(\mathfrak{b}^2,\beta^2)$.*

Proof. With $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$ and Proposition 7.8.5 we get that

$$\begin{aligned}\mathcal{N}_{\Phi^r}(\mathfrak{a}) &= (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})) = (N_{\Phi^r}(N_\Phi(\mathfrak{b})), N(N_\Phi(\mathfrak{b})))\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^{-1}N_\Phi(\mathfrak{b})\mathfrak{b}^2\overline{N(\mathfrak{b})\beta^{-1}N_\Phi(\mathfrak{b})\mathfrak{b}^2})\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^2N_\Phi(\mathfrak{b})\overline{N_\Phi(\mathfrak{b})})\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^3),\end{aligned}$$

where

$$\begin{aligned}N_{K|K_0}(N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2) &= N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2\overline{N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2}\\ &= N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}})^{-1}\overline{(\mathfrak{b}\overline{\mathfrak{b}})^{-1}}N_\Psi(\mathfrak{b})\overline{N_\Psi(\mathfrak{b})}\mathfrak{b}^2\overline{\mathfrak{b}}^2\\ &= N(\mathfrak{b})^3\mathcal{O}_K.\end{aligned}$$

Then since $\beta \in K_0$, the equivalence relation (7.6.1) yields

$$(N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^3) \sim (\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})) \sim (N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2),$$

This shows the first claim. If $N_\Psi(\mathfrak{b}) = \mu\mathcal{O}_K$ is a principal ideal, then

$$(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2) \sim (\mu\mathfrak{b}^2, N(\mathfrak{b})\beta^2) \sim (\mathfrak{b}^2, (\mu\overline{\mu})^{-1}N(\mathfrak{b})\beta^2) \sim (\mathfrak{b}^2, \beta^2)$$

which shows the second claim. □

Lemma 7.8.7. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. Then for all fractional $\mathcal{O}_K$-ideals $\mathfrak{a}$ we have an equality of fractional $\mathbb{Z}_L$-ideals*

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})^2(\mathfrak{a}\overline{\mathfrak{a}}^{-1})^2.$$

Proof. We prove this for the CM type Φ_1 and Galois group $C_2^3 \rtimes C_3$ (see Proposition 7.5.6): The statement for the other CM types follows from Proposition 7.8.3, and the argument for the group $C_2^3 \rtimes S_3$ is similar. Using the notation in Proposition 7.5.6, the extensions of Φ_1 and Φ_1^r to L are given by $\left\{1, \sigma, \sigma^2\right\}$ and $\{1, n_1, n_2, n_1n_2\}$, respectively. Considering the given double norm comes down to studying the element

$$(1+n_1+n_2+n_1n_2)(1+\sigma+\sigma^2) = 1+n_1+n_2+n_1n_2+\sigma+n_1\sigma+n_2\sigma+n_1n_2\sigma+\sigma^2+n_1\sigma^2+n_2\sigma^2+n_1n_2\sigma^2$$

in the group algebra of $\mathrm{Gal}(L\,|\,\mathbb{Q})$, where we consider the elements in this sum up to right multiplication by elements of the subgroup $H = \langle n_1, n_2\rangle$ corresponding to the field K. In terms of the cosets in (7.4.1), this yields

$$\begin{aligned}
&H + n_1H + n_2H + n_1n_2H + \sigma H + n_1\sigma H + n_2\sigma H + n_1n_2\sigma H + \sigma^2H + n_1\sigma^2H + n_2\sigma^2H + n_1n_2\sigma^2H\\
=&H + H + H + H + \sigma H + \sigma\rho H + \sigma H + \sigma\rho H + \sigma^2H + \sigma^2H + \sigma^2\rho H + \sigma^2\rho H\\
=&4H + 2\sigma H + 2\sigma^2H + 2\sigma\rho H + 2\sigma^2\rho H\\
=&(2H + 2\sigma H + 2\sigma^2H + 2\rho H + 2\sigma\rho H + 2\sigma^2\rho H) + (2H - 2\rho H),
\end{aligned}$$

which shows the claim. □

Proposition 7.8.8. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathcal{O}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^4]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$ in Equation (8.3.2).*

Proof. Once more we only give the proof for the Galois group $C_2^3 \rtimes C_3$. If $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$, then by Lemma 7.8.7 we have an equality of fractional $\mathbb{Z}_L$-ideals

$$N_{\Phi^r}(\mathfrak{a}) = N_{\Phi^r}(N_\Phi(\mathfrak{b})) = N_{K|\mathbb{Q}}(\mathfrak{b})^2\left(\mathfrak{b}\overline{\mathfrak{b}}^{-1}\right)^2 = N_{K|\mathbb{Q}}(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4. \tag{7.8.3}$$

We therefore have that $N_{\Phi^r}([\mathfrak{a}]) = [\mathfrak{b}^4]$, which shows the claim. □

Proposition 7.8.9. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$. For any CM type Φ of K and any equivalence class $(\mathfrak{b}, \beta)$ in $\mathcal{C}_K$, the equivalence class of $(\mathfrak{b}^4, \beta^4)$ is in the image of the map $\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K$ in Equation (8.3.3).*

Proof. With $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$ and Proposition 7.8.8 we get

$$\begin{aligned}\mathcal{N}_{\Phi^r}(\mathfrak{a}) &= (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})) = (N_{\Phi^r}(N_\Phi(\mathfrak{b})), N(N_\Phi(\mathfrak{b}))) = (N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}}^{-1})^2\overline{N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}}^{-1})^2}) \\ &= (N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^4),\end{aligned}$$

Since $\beta \in K_0$, using the equivalence relation in the Shimura class group yields that

$$(N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^4) \sim (\beta^{-2}\mathfrak{b}^4, 1) \sim (\mathfrak{b}^4, \beta^4),$$

which shows the claim. □

We can state the main result of this section.

Theorem 7.8.10. *Let $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$ be the subgroup of classes $[\mathfrak{b}]$ with the property that $\mathfrak{b}\overline{\mathfrak{b}}$ is generated by a totally positive element of K_0. Let B be a set of ideals that furnishes representatives of the quotient*

$$Q = \frac{G_2}{eG_2},$$

(i) where $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$ and

(ii) where $e = 4$ if $\mathrm{Gal}(K) \in \left\{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\right\}$.

Similarly, let V be a set of units that furnishes representatives of the quotient

$$(\mathcal{O}_{K_0}^*)^+ / N_{K|K_0}(\mathcal{O}_K^*).$$

Fix $A(\mathfrak{a}_0, \xi_0)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$, and let $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ be given. Then the Galois orbit of $A(\mathfrak{a}, \xi)$ under the action of $G^r = \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$ contains an abelian variety isomorphic to

$$A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0),$$

where $\mathfrak{b} \in B$, where $\beta \in K_0$ generates $\mathfrak{b}\overline{\mathfrak{b}}$, and where $v \in V$.

Proof. Proposition 7.7.7 along with (7.6.2) shows that $A(\mathfrak{a}, \xi)$ is isomorphic to $A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$ for some ideal $\mathfrak{b}$ with $[\mathfrak{b}] \in G_2$ and for some $v \in V$. Propositions 7.8.5 and 7.8.8 show that the first component of the map $\mathcal{N}_{\Phi_r}$ surjects onto eG_2. Applying a corresponding Galois conjugation to $A(\mathfrak{a}, \xi)$ if needed, we may therefore assume that $\mathfrak{b} \in B$, after which another invocation of (7.6.2) shows our claim. □

7.9 The algorithms

In this section we present the main algorithms in [19, Chapter 3.1]. Let K be a sextic CM field. The considerations in chapter 8.4 give rise to a method to determine representatives of the set of principally polarized abelian threefolds with CM by $\mathcal{O}_K$ up to isomorphism and Galois conjugacy.

We split up the steps of this method into several algorithms. Throughout, we fix a primitive CM type (K, Φ). It is in fact not essential that Φ be primitive, but this is the case that interests us in the article [19]. Similar algorithms were considered in lower genus in the previous works [22] and [70]. We discuss differences in our approach in passing. For a better understanding, we split this section in several subsections corresponding to the algorithms in the these subsections.

The precomputation step

Let (K,Φ) be a primitive CM type. Regarding to the discussion in Chapter 8.4, in order to compute representatives of isomorphism classes in

$$\mathcal{M}_{\mathcal{O}_K}(\Phi)$$

up to Galois conjugacy over the reflex field, we need to identify equivalence classes in the quotient

$$\mathcal{C}_K/\mathrm{im}(\mathcal{N}_{\Phi^r}).$$

Following the discussion after Theorem 7.8.1, given $A(\mathfrak{a}_0,\xi_0)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$, we obtain any other isomorphism class $A(\mathfrak{a},\xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ as a Galois conjugate abelian variety

$$A(\mathfrak{b}\mathfrak{a}_0,\eta_0),$$

where $\mathfrak{b}$ runs through a fixed small set of representatives of the quotient G_2/eG_2, where $G_2 = \ker(N_{K|K_0})$, and where e is a power of 2 (see Theorem 7.8.1). The following algorithm determines the data from the discussion in Chapter 8.4.

Algorithm 1
INPUT: A sextic CM field K.
OUTPUT: Precomputed data used in the later Algorithms 2, 3, and 4.

(i) Determine:

  (a) The class group and unit group $\mathrm{Cl}(K)$, $\mathcal{O}_K^*$ of K, and

  (b) The class group, narrow class group and unit group $\mathrm{Cl}(K_0)$, $\mathrm{Cl}^+(K_0)$, $\mathcal{O}_{K_0}^*$ of the totally real subfield $K_0 \subset K$.

(ii) Determine the subgroup $G_1 \subset \mathrm{Cl}(K)$ of classes $[\mathfrak{a}] \in \mathrm{Cl}(K)$ with the property that $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by an element of K_0.

(iii) Determine the subgroup $G_2 \subset \mathrm{Cl}(K)$ of classes $[\mathfrak{a}] \in G_1$ with the property that $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by a totally positive element of K_0;

(iv) Let $Q = G_2/eG_2$, where:

  (a) $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$, and

  (b) $e = 4$ if $\mathrm{Gal}(K) \in \left\{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\right\}$.

(v) Determine set of ideals:

  (a) C of $\mathcal{O}_K$ that furnishes representatives of the quotient G_1/G_2, and

  (b) B of $\mathcal{O}_K$ that furnishes representatives of the quotient $Q = G_2/eG_2$.

(vi) Determine the subgroup $U_1 \subset \mathcal{O}_{K_0}^*$ of totally positive units in $\mathcal{O}_{K_0}^*$;

(vii) Determine the subgroup $U_2 \subset U_1$ of units in $\mathcal{O}_{K_0}^*$ that are norms from $\mathcal{O}_K^*$;

(viii) Determine set of units:

  (a) W that furnishes representatives of the quotient $\mathcal{O}_{K_0}^*/U_1$, and

  (b) V that furnishes representatives of the quotient U_1/U_2.

Remark 7.9.1. The steps in Algorithm 1 can be performed by using classical algorithms for class and unit groups.

We restrict ourselves to some remarks on steps that are somewhat less standard.

Remark 7.9.2. (i) Under the generalized Riemann hypothesis, the calculation of the class und unit group of K and K_0 in Step (1) speeds up tremendously. We have therefore used this assumption while performing our calculations.

(ii) We can determine the subgroup G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by

$$[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}],$$

and G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$. Similar considerations apply to the determination of U_1 and U_2 in Steps (6) and (7).

(iii) It is important that the representatives returned by Algorithm 1 be minimized, since otherwise large precision loss will occur in later steps. In [22, §4.1], this minimization is also mentioned as being useful when working with the Shimura class group in the genus-2 case. For our purposes this is not merely useful, but also indispensable in practice, as the class groups involved are of considerable size and working with large powers of ideal class generators without reducing these already causes unacceptable precision loss when determining the corresponding lattices in $\mathbb{C}^3$ in Algorithm 4. We therefore spend a few lines on this reduction step.

For an ideal representative in B and C, this observation means that it should be multiplied with a principal ideal in such a way that the norm of the resulting product is smaller than the Minkowski bound M of K. This can be done as follows. Given an ideal $\mathfrak{r}a$ to be minimized, one computes the lattice Γ in $\mathbb{C}^3$ that is the image of $\mathfrak{r}a^{-1}$ under the complex embeddings of K. One then determines a short vector α in Γ, and the corresponding element α of $\mathfrak{r}a^{-1}$ will satisfy $N_{K|\mathbb{Q}}(\alpha) \leq M N_{K|\mathbb{Q}}(\mathfrak{r}a^{-1})$. Therefore the norm of the ideal $\alpha\mathfrak{r}a$ is at most M, and we use this product as a minimized ideal representative.

For a unit that furnishes a representative in V, resp. W, being small means the following. Let $\ell : \mathcal{O}_{K_0}^* \to \mathbb{R}^2$ be the log map whose image is the Dirichlet lattice of the unit group $\mathcal{O}_{K_0}^*$. Then given an element u of V (resp. W) to be minimized, we can use closest vector algorithms to find an element u_1 (resp. u_2) of U_1 (resp. U_2) such that that $\ell(u) + \ell(u_1)$ (resp. $\ell(u) + \ell(u_2)$) is small, and we use the corresponding product $u \cdot u_1$ (resp. $u \cdot u_2$) as a minimized unit representative.

(iv) Note that in contrast to the methods in [22], our precomputation does not require the computation of the Shimura class group or the image of the reflex norm, which simplifies its description.

Determining an initial triple $(\Phi, \mathfrak{a}, \xi)$

After following the discussion before Algorithm 1, the next algorithm determine a triple $(\Phi, \mathfrak{a}, \xi)$ which represents an isomorphism class in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$.

Algorithm 2
INPUT: A sextic CM field K and a primitive CM type Φ of K.
OUTPUT: A single triple $(\Phi, \mathfrak{a}, \xi)$, with $\mathfrak{a}$ a fractional $\mathcal{O}_K$-ideal and with $\xi \in K$ totally imaginary, such that $(\Phi, \mathfrak{a}, \xi)$ represents a principally polarized abelian threefold A with CM by $\mathcal{O}_K$ of type Φ.

(i) Determine a pair $(\mathfrak{a}_0, \xi_0)$ such that $(\xi_0) = (\mathfrak{a}_0\overline{\mathfrak{a}_0}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$. If the imaginary part of ξ_0 is positive for all embeddings in Φ, then return $(\Phi, \mathfrak{a}_0, \xi_0)$. Otherwise, proceed to the next step.

(ii) Let C be the set computed with Algorithm 1. Run through the elements $\mathfrak{c} \in C$, and let $\gamma \in K_0$ be a generator of $\mathfrak{c}\overline{\mathfrak{c}}$.

(iii) Within the previous loop, let W be the set computed with Algorithm 1. Run through the elements $w \in W$, and consider

$$(\mathfrak{a}, \xi) = (\mathfrak{c}\mathfrak{a}_0, w\gamma^{-1}\xi_0).$$

If $(\mathfrak{a}, \xi)$ admits Φ as a CM type, or in other words, if ξ has positive imaginary part for the embeddings in Φ, then return $(\Phi, \mathfrak{a}, \xi)$.

Theorem 7.9.3. *Algorithm 2 terminates and the output is correct.*

Proof. If the algorithm returns a triple, then it is correct by construction. It therefore remains to show that the algorithm does always furnish an output.

First note that the existence of a triple $(\Phi, \mathfrak{a}, \xi)$ as in the Output step follows from Proposition 7.7.7. Now suppose that we have determined a pair $(\mathfrak{a}_0, \xi_0)$ as in Step (1) of the algorithm. Then since both $\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}}^{-1}$ and $\mathfrak{a}_0\overline{\mathfrak{a}}_0\mathfrak{D}_{K|\mathbb{Q}}^{-1}$ are principal, and generated by totally imaginary elements of K, we have that the class of $\mathfrak{a}\mathfrak{a}_0^{-1}$ belongs to G_1. Let $\mathfrak{c} \in C$ be an element representing this class, and let $\gamma \in K_0$ be the chosen generator of $\mathfrak{c}\overline{\mathfrak{c}}$. We can then write $\mathfrak{a} = \delta\mathfrak{c}\mathfrak{a}_0$ with $\delta \in K^*$. Let $\mathfrak{b} = \mathfrak{c}\mathfrak{a}_0$. Then

$$(\delta\overline{\delta}\xi) = ((\delta\overline{\delta})^{-1}\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1} = (\mathfrak{b}\overline{\mathfrak{b}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$$

and

$$(\gamma^{-1}\xi_0) = ((\mathfrak{c}\overline{\mathfrak{c}})\mathfrak{a}_0\overline{\mathfrak{a}}_0\mathfrak{D}_{K|\mathbb{Q}})^{-1} = (\mathfrak{b}\overline{\mathfrak{b}}\mathfrak{D}_{K|\mathbb{Q}})^{-1},$$

so since ξ and ξ_0 are totally imaginary, we have $\delta\overline{\delta}\xi = u\gamma^{-1}\xi_0$ for a unit $u \in \mathbb{Z}_{K_0}^*$. Let $w \in W$ be a representative of the class corresponding to u. Then $(\mathfrak{c}\mathfrak{a}_0, w\gamma^{-1}\xi_0)$ has the property that the imaginary parts of $w\gamma^{-1}\xi_0$ has the same signs as $\delta\overline{\delta}\xi$, and hence as ξ. These are exactly the signs compatible with Φ. Therefore since the algorithm encounters this triple as it runs, it is indeed guaranteed to return the requested output. □

Remark 7.9.4. (i) Finding a pair $(\mathfrak{a}_0, \xi_0)$ as in Step (1) of Algorithm 2 is possible by using the methods of [70, Proposition 4.4]: In fact the pair $(\mathfrak{a}_0, yz)$ in *loc. cit.* can be used.

(ii) For all cases in the LMFDB, Algorithm 2 did in fact find a triple $(\Phi, \mathfrak{a}, \xi)$. This is the case because the final condition in Corollary 7.5.8 is satisfied for all sextic CM fields in the LMFDB.

Determining all triples $(\Phi, \mathfrak{a}, \xi)$

Given an initial triple $(\Phi, \mathfrak{a}, \xi)$ returned by Algorithm 2, the others can be determined by using the precomputed data from Algorithm 1

Algorithm 3
INPUT: A sextic CM field K and a primitive CM type Φ of K.
OUTPUT: A set S of triples $(\Phi, \mathfrak{a}, \xi)$ as in [70, Theorem 4.2], so that $(\mathfrak{a}, \xi)$ represents a principally polarized abelian threefold A that admits CM by K of Φ. Moreover, S satisfies the following property: Up to Galois conjugacy over the reflex field K^r, any pair (Φ, A), where A is a principally polarized abelian threefold that admits CM by $\mathcal{O}_K$, is isomorphic over $\mathbb{C}$ to an abelian variety corresponding to one of the elements of S.

(i) Let $(\Phi, \mathfrak{a}_0, \xi_0)$ be the triple from Algorithm 2.

(ii) Run through the elements $\mathfrak{a}$ of B, and let $\beta \in K_0$ be a generator of $\mathfrak{a}\overline{\mathfrak{a}}$.

(iii) Within the previous loop, run through the elements v of V, and add $(\mathfrak{a}, \xi) = (\mathfrak{a}\mathfrak{a}_0, v\beta^{-1}\xi_0)$ to S.

(iv) Return S once the loops above have terminated.

Theorem 7.9.5. *Algorithm 3 terminates and the output is correct.*

Proof. Since the set B is finite, Algorithm 3 terminates. The correctness of Algorithm 3 follows from Theorem 7.8.10. □

Remark 7.9.6. (i) We do *not* claim that the given set S is in actual bijection with the set of isomorphism classes of pairs

$$(A, \Phi)$$

up to Galois conjugacy, and indeed this is not the case in general. For our purposes, it suffices that the abelian varieties associated map surjectively to the latter set of equivalence classes, and we do not impose additionally that this natural map be injective.

(ii) As was shown in Equation (7.6.3), the size of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ is well approximated by $h(K)/h^+(K_0)$. When $G = C_2^3 \rtimes S_3$, the largest size of the quotient $h(K)/h^+(K_0)$ in (7.6.3) was 11287, whereas the largest size of the group Q was 128, thus showing the speed gain that our taking into account Galois conjugacy provides.

Determining period matrices

Regarding to one of the initial questions in this chapter: Given a primitive CM type (K, Φ), determine a small set of period matrix representatives of the corresponding isomorphism classes of principally polarized abelian threefolds, up to Galois conjugation over the reflex field K^r of K with respect to Φ. By a calculation with theta-null values, using [38], then identify these representatives correspond to hyperelliptic or non-hyperelliptic curves.

Algorithm 4
INPUT: A sextic CM field K and a primitive CM type Φ of K.
OUTPUT: The small period matrices τ corresponding to the elements of the set S in Algorithm 3, sorted into two sets T_H and T_N that (heuristically) give rise to hyperelliptic and non-hyperelliptic curves, respectively.

(i) Determine the set S from Algorithm 3, and initialize T_H and T_N to be empty sets.

(ii) Let $(\Phi, \mathfrak{a}, \xi)$ be in S. Calculate the corresponding principally polarized abelian threefold (A, E) in the usual manner [70, §4], setting $A = \mathbb{C}^3/\Phi(\mathfrak{a})$ and letting E be the $\mathbb{R}$-linear extension of the trace pairing $(\alpha, \beta) \mapsto \mathrm{Tr}_{K|\mathbb{Q}}(\xi\alpha\overline{\beta})$.

(iii) Determine a Frobenius alternating form of E to find some big period matrix $P \in M_{3,6}(\mathbb{C})$ for A, and from it, a small period matrix $\tau \in M_{3,3}(\mathbb{C})$.

(iv) Reduce τ by using the methods from [37, §2].

(v) Use algorithms, for example those by Labrande [38], to determine whether τ has 1 or 0 vanishing even theta-null values to some high precision (typically 100 digits). In the former case, add τ to T_H; in the latter, add it to T_N.

Theorem 7.9.7. *If Algorithm 4 terminates, then the output is (computationally) correct.*

Proof. First of all we notice, that computing theta-null values as in step (v) of the Algorithm 4 is valid, only in the case where τ is small period matrix of a non-hyperelliptic Jacobian. In the case where τ is small period matrix of a hyperelliptic Jacobian, the exactness of the result in step (v) has its limitation, which is bounded by the precision of the computation. We have noticed in passing that the available implementation of the algorithm in [38] does not always function, but still managed to get by in the cases that interested us, either by using the naive method from [38] to lower precision, or by determining the even theta-null values for only a single element of a given Galois orbit and conjugating afterwards.

Under these assumptions, and by the finiteness of the set S in step (i), this shows the claim. □

Remark 7.9.8. (i) Note that our algorithms differ from those in [70], as we fix our primitive CM type Φ throughout. When considering CM curves up to Galois conjugacy, we are justified in doing so because of Corollary 7.5.8.

(ii) Because we have insisted that Φ be a primitive CM type, the associated abelian threefolds are indeed Jacobians of genus-3 curves. The criterion for said Jacobian to be hyperelliptic in terms of even theta-null values is [31, Lemmata 10 and 11].

(iii) Like the minimization of representatives in Algorithm 1, Steps (4) of Algorithm 4 is essential to keep its running time short.

(iv) Our own run of Algorithm 4 used the native MAGMA implementation in Step (5) instead of the algorithms from [38]. The even theta values were computed to 100 digits of precision, and decided to be numerically equal to zero when their absolute value is at most 10^{-50}. Setting `Labrande := true` in the implementation at [18] allows for an alternative verification of these results using [38] instead.

(v) Using interval arithmetic or the fast decay of the terms intervening in the sum that define a even theta-null value, it is in principle possible to prove rigorously that all such values are non-zero. This enables one to prove that a ppav A that Algorithm 4 suspects to come from a non-hyperelliptic indeed comes from such a curve. By contrast, showing that A comes from a hyperelliptic curve is more involved. For the moment, we see no other rigorous method to check this than to calculate an equation for a corresponding curve X as in Section 7.11 and to show that $\mathrm{Jac}(X)$ has CM using the algorithms in [15]. We discuss some further sanity checks in the next section.

Fields

With the algorithms from Section 7.9 in hand, we considered the sextic CM fields in the LMFDB [73]. We list our results, which imply the Theorems 7.2.1 and 7.2.3, Table 9.1. Its first column lists the possible Galois groups, whereas its second column gives the corresponding number of sextic CM fields in the LMFDB.

We have applied our algorithms, implemented in Magma [6] and available at [18], to all of these 547,156 fields, except for 2 fields with Galois group D_6 whose root discriminant exceeds 10^{12} and for which the calculation of the class and unit group did not finish in a timely fashion even when assuming the generalized Riemann hypothesis. The total computation required 4 days on 20 cores when working to relatively high precision to absolutely exclude rounding errors.

The second column of Table 9.1 indicates the number of CM fields K in the database whose Galois group is isomorphic to that indicated in the first column. The third column of Table 9.1 indicates the number of CM fields K considered for which the set T_H from Algorithm 4 is non-empty, or in other words those fields K are hyperelliptic CM fields (see Definition 7.1.1), i.e. the sextic CM fields K for which there (heuristically) exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathcal{O}_K$.

Further, the fourth column of Table 9.1 lists the number of hyperelliptic fields K that are exceptional (see Definition 7.1.1), i.e. the hyperelliptic CM fields K that does not include $\mathbb{Q}(i)$.

The fifth column of Table 9.1 indicates the number of mixed sextic CM fields (see Definition 7.1.1) fields, i.e. sextic CM fields for which both sets H and N from Algorithm 4 there heuristically exists both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has CM by $\mathcal{O}_K$.

Galois group	$\#K$	# hyp. K	# exc. hyp. K	# mixed K
C_6	10,067	348	2	0
D_6	32,544	3,057	0	0
$C_2^3 \rtimes C_3$	10,159	0	0	0
$C_2^3 \rtimes S_3$	494,386	17	17	14
Total	547,156	3,422	19	14

Table 7.2: CM fields in the LMFDB

7.10 Invariants

Let $Z \in M_g(\mathbb{C})$ be a small period matrix. This section briefly recapitulates what is known on calculating and algebraizing the invariants of the curve over X associated to Z, as well as verifying the correctness of the resulting curve.

Algorithm 4 shows that we can calculate an approximation to Z to a given high precision, as all that we need to do is to determine the image of a basis of a (minimized) representative $\mathfrak{a}$ under the given CM type Φ. What is considerably more complicated is to calculate the even theta-null values associated to Z. Here it is in general essential to use the more sophisticated algorithms by Labrande [38] to keep the running time within reasonable bounds. We have noticed in passing that the available implementation of this algorithm does not always function, but still managed to get by in the cases that interested us, either by using the naive method from [38] to lower precision or by determining the even theta-null values for only a single element of a given Galois orbit and conjugating afterwards.

Given the even theta-null values, we can determine a model of X over $\mathbb{C}$ to the given precision, either by using the Rosenhain invariants as in [1] or by using the Weber model from [37]. We can then calculate a normalized weighted representative I of the corresponding invariants (using the Shioda invariants in the hyperelliptic case and the Dixmier–Ohno invariants in the non-hyperelliptic case). The field of moduli of X then coincides with the field generated by the entries of I.

Algebraization.

It remains to algebraize the invariants I. A first possible method is the usual application of the LLL algorithm to determine putative minimal polynomials of the entries of I over $\mathbb{Q}$ and thus to obtain I as elements of a number field.

One corresponding implementation is `NumberFieldExtra` in [14].

A second method is to symmetrize and use class polynomials, as in [17, 22]. Both of these methods became prohibitive in the cases that we considered because of the large heights of the algebraic numbers that were involved. Indeed, one of the mixed fields, defined by the polynomial $x^6 - 2x^5 + 11x^4 + 42x^3 - 11x^2 + 340x + 950$, gives rise to a tuple of normalized Dixmier–Ohno invariants whose first non-trivial entry I_6 has height $\approx 2.94 \cdot 10^{431}$, with I_{27} having a height that larger by an exponential factor of about 27/6. Another reason for us not to use the class polynomial method from [22] is that this would necessitate later factorization to determine the Galois orbits, which is superfluous when algebraizing the individual I directly.

Instead we exploited the fact that that the Shimura reciprocity law implies that the entries of I are the complex embeddings of elements of Hilbert class field H of the reflex field K^r. This replaces the problem of determining minimal polynomials to the more tractable one of trying to algebraize the elements of I in H or its subfields, which also reduces to an application of LLL (for example in the form of the routine `AlgebraizeElementsExtra` in [14]). In the aforementioned complicated case we needed 20,000 digits of precision for our algebraization, but usually around 3,000 digits were enough. Incidentally, note that while the reflex K^r itself can be costly to determine via the usual Galois theory, since the closure L becomes quite large, it can still be quickly recovered numerically as a subfield of $\mathbb{C}$, namely by applying the methods from the previous paragraph.

Verification.

Once we have algebraized the elements of I, we have applied heuristic numerical methods twice, both in the determination of I itself and in the algebraization of its elements. One may well ask why one should trust the algebraic invariant values thus obtained to be correct. Here are several reasons:

(i) For all algebraizations I that we found, the resulting invariants satisfy the known algebraic dependencies between the Shioda invariants (which can be found in [44]) or the Dixmier–Ohno invariants (which can be found in [45]). There is no reason whatsoever for this to hold in the case of incorrect or badly algebraized I.

(ii) Reducing the values of I modulo various large primes, one can apply the reconstruction algorithms from [42] or [43] and then calculate Weil polynomials to check that the resulting curves indeed have CM by an order in K for all these primes.

(iii) Conversely, one can bound the primes of bad reduction from I and check that the set thus obtained contains the primes found in [32].

(iv) In principle one can verify all results obtained over $\overline{\mathbb{Q}}$ by using [15]. That said, these algorithms still need substantial speedups for these verifications to be feasible for plane quartic curves over number fields.

This is why we do not harbor any doubts about our results being correct, even though they are by no means mathematically rigorous yet.

The mixed cases

Table 7.3 describes the results for the 17 fields K from Table 9.1 with Galois group $C_2^3 \times S_3$ that are exceptional. Note that there are also 2 exceptional hyperelliptic fields with Galois group C_6, but these were already considered in [33]: Corresponding polynomials are given by $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ and $x^6 - 14x^3 + 63x^2 + 168x + 161$.

The first column of Table 7.3 gives the polynomial defining the CM field K; this column is sorted by the absolute discriminant of the ring of integers $\mathcal{O}_K$. The second column describes the length of the various hyperelliptic Galois orbits under conjugation by $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$; for example, an entry $4^2 8^1$ stands for 2 Galois orbits of length 4 along with single Galois orbit of length 8. Similarly, the third column describes the length of the non-hyperelliptic Galois orbits under $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. An empty entry means that there does not exist such a curve for the field K. Note that Corollary 7.5.11 shows why the length of the Galois orbits in the table are all a multiple of 4. The final column describes the quotient

$$\mathcal{C}_K / \mathrm{im}(\mathcal{N}_\Phi)$$

of the Shimura class group by the image of the reflex type norm. Note that this independent of the chosen primitive CM type Φ because of Proposition 7.5.4 and Corollary 7.5.8.

The invariants obtained for the fields in Table 7.3 are available at [18]. As mentioned above, they are occasionally on the gargantuan side.

CM field	hyp. orbits	non-hyp. orbits	$\mathcal{C}_K/\mathrm{im}(\mathcal{N}_\Phi)$
$x^6+10x^4+21x^2+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-3x^5+14x^4-23x^3+28x^2-17x+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-2x^5+12x^4-31x^3+59x^2-117x+121$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6+14x^4+43x^2+36$	4^1		1
$x^6-3x^5+9x^4+4x^3+12x^2+84x+236$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-2x^5+x^4-4x^3+5x^2-50x+125$	4^1	4^3	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+29x^4+246x^2+512$	4^1		1
$x^6-3x^5+10x^4+8x^3+x^2+90x+236$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+21x^4+60x^2+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+30x^4+169x^2+200$	4^1	4^1	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+23x^4+112x^2+36$	4^1		1
$x^6-2x^5+12x^4-44x^3+242x^2-672x+1224$	12^1	12^3	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+26x^4+177x^2+128$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+29x^4+226x^2+252$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-2x^5-7x^4+45x^3-63x^2-162x+729$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-2x^5+11x^4+42x^3-11x^2+340x+950$	8^1	$8^1 16^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-3x^5+29x^4-53x^3+200x^2-174x+71$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$

Table 7.3: Generic hyperelliptic and mixed fields with Galois group $C_2^3 \rtimes S_3$ and the lengths of the corresponding Galois orbits

7.11 Explicit defining equations

In this section we further consider the mixed CM field K defined by $x^6+10x^4+21x^2+4$, which corresponds to the first entry of Table 7.3. Our goal is to indicate how to obtain the (heuristic) explicit defining equations from Theorem 7.2.6. The actual calculations are performed in [18].

There are two Galois orbits in this case, one containing 4 hyperelliptic curves, and one containing 4 non-hyperelliptic curves. Moreover, Corollary 7.5.8 shows that once we fix a CM type Φ, which we do throughout this section, there is exactly one corresponding hyperelliptic curve X and one non-hyperelliptic curve Y. We start by finding an equation for X.

Hyperelliptic simplification

As in Section 7.10, we determine a normalized tuple S of Shioda invariants corresponding to the curve X, which is defined over the quartic field L corresponding to the polynomial x^4-5x^2-2x+1. The field L is in fact the totally real subfield of the reflex field K^r of K.

One can try to apply the generic reconstruction algorithms in genus 3 that are available in Magma, but this turns out not to be optimal, as the resulting hyperelliptic curve is returned over a random quadratic extension of L with large defining coefficients. Instead, we directly construct the Mestre conic and quartic C and Q over K from the invariants S, as in [42], and then check whether the conic C admits a rational point. This turns out to be the case. Choosing a parametrization $\mathbb{P}^1 \to C$ over K and pulling back the divisor $C \cap Q$ on C, we obtain a degree-8 divisor on $\mathbb{P}^1$ that corresponds to a monic octic polynomial f with the property that

$$X : y^2 = f \tag{7.11.1}$$

is a curve with CM by $\mathcal{O}_K$. This is still far from satisfactory, however, as the coefficients of f are extremely large, namely of height up to $4.92 \cdot 10^{1126}$. We show how to obtain a simpler equation. Our approach is essentially ad hoc; while there are minimization and reduction algorithms in Magma over the rationals due to Cremona–Stoll [68], and over real quadratic number fields due to Bouyer–Streng [8], we do not find ourselves in one of these cases, so that we are forced to use other methods.

The octic polynomial f factors as

$$f = f_1 f_2 f_3,$$

where f_1 and f_2 are quadratic, both defined over a pleasant quadratic extension M of L with defining polynomial $x^8 - 4x^7 + 10x^5 + 7x^4 - 10x^3 - 18x^2 - 6x + 1$ over the rationals. (That this extension is so agreeable is of course no surprise; the extended version of the Main Theorem of Complex Multiplication, applied to the 2-torsion of $\mathrm{Jac}(X)$, shows that we should expect it to be related to the Hilbert class field of L ramifying at its single even prime.)

We now consider f over the quadratic extension M of L, over which field we will construct a simpler polynomial defining the same hyperelliptic curve, which we will the descend back to L. To start our simplification over M, we apply a Möbius transformation in the x-coordinate that sends the roots of f_1 to 0 and ∞ and one of the roots of f_2 to 1. This maps the divisor defined by the octic polynomial f to that defined by a *septic* polynomial g that additionally satisfies $g(0) = g(1) = 0$. We normalize g in such a way that the coefficient of x^4 equals 1, for reasons that will become clear, so that

$$g = c_7 x^7 + c_6 x^6 + c_5 x^5 + x^4 + c_3 x^3 + c_2 x^2 + c_1 x. \tag{7.11.2}$$

Now inspecting the norms of the coefficients c_i shows that we have

$$(c_5) = \mathfrak{p}_2^{-4}(\sigma(c_3))$$

where $\mathfrak{p}_2$ is the unique ideal of $\mathbb{Z}_L$ above 2 and where σ is the involution that generates $\mathrm{Gal}(M\,|\,L)$. Following a hunch, we scale x by α^2, where α generates $\mathfrak{p}_2$. Transforming g accordingly, we obtain an equality of ideals

$$(c_i) = (\sigma(c_{8-i})) \tag{7.11.3}$$

for *all* i between 1 and 4.

Our goal is to make Equation (7.11.3) hold on the level of elements, and not merely between ideals. To achieve this, we consider the unit $u = c_5/\sigma(c_3) \in \mathbb{Z}_M^*$. Consider the polynomial h obtained from g by scaling x by vx, where $v \in \mathbb{Z}_M^*$ is another unit, and normalizing the coefficient of x^4 to equal 1. Then for the coefficients d_i of h we have $d_5 = vc_5$ and $d_3 = v^{-1}d_3$. The straight-up equality $d_5 = \sigma(d_3)$ that we are looking for can be rewritten as

$$vu\sigma(c_3) = vc_5 = d_5 = \sigma(d_3) = \sigma(v^{-1})\sigma(c_3)$$

This is the case if and only if

$$u = v\sigma(v). \tag{7.11.4}$$

Since $\mathbb{Z}_M^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^5$ and v satisfies this equality if and only of $-v$ does, the equality (7.11.4) reduces to integral linear algebra once the representation of σ in terms of a given basis of $\mathcal{O}_K^*$ is known. Performing the corresponding computation shows that we can indeed find a v with the requested properties. Rescaling x accordingly, we find a polynomial g as in (7.11.2) such that

$$(c_i) = (\sigma(c_{8-i})) \tag{7.11.5}$$

is satisfied for all $i = 1, \dots, 4$.

At this point, our manipulations have lead to a polynomial g with coefficients of maximal height $8.64 \cdot 10^{16}$, which is smaller than $4.92 \cdot 10^{1126}$. We can still do a bit better by further scaling x by appropriate units v satisfying $v\sigma(v) = 1$. This does not affect the property (7.11.5). Our goal is to make d_5 as small as possible as an element of the Minkowski lattice up to shifts by units of the indicated type. This reduces to a closest vector problem as in Remark 7.9.2, an approximation for which is quickly furnished by the usual techniques. Applying the corresponding scaling yields a slightly smaller polynomial g with coefficients of height $1.11 \cdot 10^{16}$.

It now remains to descend our polynomial g with coefficients in M to the original field L. For this, let σ be the involution that generates the Galois group $\mathrm{Gal}(M\,|\,L)$, and let $B \in \mathrm{GL}_2(M)$ be such that

$$\sigma(B) = AB, \qquad \text{where} \qquad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For example, we can take

$$B = \begin{pmatrix} 1 & \alpha \\ 1 & \sigma(\alpha) \end{pmatrix}$$

where $\alpha \in M$ is such that $M = L \oplus L\alpha$. The matrix B^{-1} induces a Möbius transformation of the projective line.

Proposition 7.11.1. *Let $D = (g)_0 \cup \{\infty\} \subset \mathbb{P}^1$, where $(g)_0$ is the divisor of zeros of the polynomial g, and let $E_0 = B^{-1}(D)$.*

(i) The divisor $E_0 \subset \mathbb{P}^1$ is defined over L.

(ii) Let f_0 be a polynomial whose divisor of zeros is given by E_0. Then the hyperelliptic curve $X_0 : y^2 = f_0$ over L is isomorphic over $\overline{\mathbb{Q}}$ to the original curve X in (7.11.1).

Proof. (i): The divisor E_0 is defined over M, as B and D are. Moreover, we have

$$\sigma(E_0) = \sigma(B^{-1}D) = \sigma(B)^{-1}\sigma(D) = B^{-1}A^{-1}AD = B^{-1}D = E_0$$

This Galois invariance implies our claim.

(ii) This follows from (i) because two hyperelliptic curves are $\overline{\mathbb{Q}}$-isomorphic if (and only if) the corresponding branch loci are related by a Möbius transformation. □

Alternatively, f_0 is the numerator of the transform of g by B^{-1}. This turns out to be still of reasonable size when α is. Replacing X be X_0, we have achieved our aim of simplifying X. The result is the equation for X in Theorem 7.2.6. The discriminant of the corresponding hyperelliptic polynomial equals $\mathfrak{p}_4^{120}\mathfrak{p}_7^{12}$, where $\mathfrak{p}_4$ (resp. $\mathfrak{p}_7$) is an ideal of norm 4 (resp. 7).

A plane quartic equation

It remains to construct a plane quartic model for the non-hyperelliptic curve Y from the knowledge of its Dixmier–Ohno invariants I. The direct methods from [43] gives a ternary quartic with coefficients whose size is beyond hopeless. Methods to obtain defining equations of smaller size were sketched in [37, §3], using methods due to Elsenhans and Stoll [21, 67], yet like the methods of Cremona–Stoll in Section 7.11, these are specific to the base field $\mathbb{Q}$, and therefore of no use in the current situation.

Fortunately, now that we have found the equation for the hyperelliptic curve X in Theorem 7.2.6, determining the equation for the non-hyperelliptic curve Y becomes tractable.

To see this, let $P_X \in M_{3,6}(\mathbb{C})$ be a big period matrix corresponding to X with respect to the canonical basis of differentials $\left\{dx/y, xdx/y, x^2dx/y\right\}$ corresponding to the equation (7.2.1), and let P_Y be the large period matrix of the Weber model $Y : F(x,y,z) = 0$ over $\mathbb{C}$ for Y obtained in the course of using Algorithm 4. This matrix, and all other big period matrices that follow, should be taken with respect to the canonical basis of differentials

$$\left(xdx(\partial F/\partial y)^{-1}, ydx(\partial F/\partial y)^{-1}, dx(\partial F/\partial y)^{-1}\right).$$

Proposition 7.11.2. *There exist matrices $T \in M_{3,3}(\mathbb{C})$ and $R \in M_{6,6}(\mathbb{Z})$ such that R has determinant 2 and*

$$TP_Y = P_X R.$$

Moreover, the pair (T,R) is uniquely determined up to a minus sign.

Proof. This is a direct consequence of the fact that X and Y are related by an $\mathfrak{a}$-transformation with $N_{K|\mathbb{Q}}(\mathfrak{a}) = 2$. In turn, this statement follows from the fact (see Table 7.3) that $\mathcal{C}_K/\mathrm{im}(\mathcal{N}) \cong \mathbb{Z}/2\mathbb{Z}$, and that if we factor $(2) = \mathfrak{a}^4\mathfrak{b}^2$ in $\mathcal{O}_K$, with $N_{K|\mathbb{Q}}(\mathfrak{a}) = N_{K|\mathbb{Q}}(\mathfrak{b}) = 2$, the ideal $\mathfrak{a}$ represents the non-trivial class in this quotient, which therefore induces an isogeny between the two distinct ppavs with CM by K of a fixed type Φ. The uniqueness claim follows from the fact that $\mathfrak{a}$ is the only ideal of norm 2 whose class in $\mathcal{C}_K/\mathrm{im}(\mathcal{N})$ is non-trivial. □

In what follows, given a matrix $T \in M_{3,3}(\mathbb{C})$ and a ternary quartic form $F \in \mathbb{C}[x,y,z]$, we denote the transformation of F under the natural right action of T by $F \cdot T$.

Proposition 7.11.3. *Let F be the ternary quartic form associated to the Weber model whose big period matrix is P_Y, and F_0 be a multiple of $F \cdot T^{-1}$ that is normalized in such a way that one of its coefficients is in L. Then $Y_0 : F_0(x,y,z) = 0$ is a model of Y over L.*

Proof. We know that Y has field of moduli equal to L. Now since the torsion subgroup of $\mathcal{O}_K^*$ is reduced to $\langle -1 \rangle$, the automorphism group $\mathrm{Aut}(Y)$ is trivial, since $\mathrm{Aut}(Y) = \mathrm{Aut}(\mathrm{Jac}(Y))/\langle -1 \rangle$ for plane quartic curves Y. Therefore there exists a plane quartic curve $Z \subset \mathbb{P}^2$ defined over L that is isomorphic to Y. Let G be a corresponding form, and let P_Z be a corresponding period matrix. The same argument as above shows that there exists a matrix $U \in M_{3,3}(\mathbb{C})$ such that

$$UP_Z = P_X R.$$

Because both X and Z are defined over L, the uniqueness of R up to sign implies that $U \in M_3(\overline{\mathbb{Q}})$ and $\sigma(U) = \pm U$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. Now let $G_0 = G \cdot U^{-1}$, normalized in such a way that one of its coefficients is in L. Since $\sigma(G \cdot U^{-1}) = \sigma(G) \cdot \sigma(U^{-1}) = G \cdot \pm U^{-1}$, we have that the class of $G \cdot U$ up to scalar is Galois stable. Therefore G_0 is defined over L, and its big period matrix is a scalar multiple of $UP_Z = P_X R$. On the other hand, the ternary quartic $F \cdot T$ also has a big period that is a scalar multiple of $TP_Y = P_X R$. Therefore F_0 and G_0 coincide up to a scalar, and because of our normalization F_0 has coefficients in L as well. □

An algebraization in the field L using LLL shows that we can indeed recover the coefficients of the ternary quartic form F_0 defining Y_0 over K. Tweaking its size by scaling x, y, z by units (similar to the closest vector considerations in Section 7.11) makes the equation of Y_0 somewhat

smaller still. Replacing Y by Y_0 gives the equation for Y in Theorem 7.2.6. Its discriminant factors as

$$\mathfrak{p}_4^{312}\mathfrak{p}_7^{36}\mathfrak{p}_{19}^{14}\mathfrak{p}_{277}^{14}\mathfrak{p}_{1753}^{14},$$

where as before subscripts indicate norms.

Remark 7.11.4. We emphasize once more that the equations obtained in this section have not yet been verified by the methods from [15] because of the considerable effort required to run these algorithms over large number fields.

7.12 Around the André–Oort conjecture

General considerations

In this section, we review a certain number of results around the André–Oort conjecture. The André–Oort conjecture was formulated in the general context of Shimura varieties and their special points. A proof of this conjecture under the assumption of the Generalized Riemann Hypothesis (GRH) for CM fields has been given by Klingler and Yafaev [36]. For an extensive survey on Shimura varieties and a general statement of the conjecture, the reader is refered to [52].

Although our focus is on genus 3, we start by stating facts that hold for every $g \geq 1$. We denote by $\mathcal{A}_g$ be the moduli space of ppavs of genus g over $\mathbb{C}$ and by $\mathcal{M}_g$ the moduli space of of smooth genus g curves defined over $\mathbb{C}$. Recall that the Torelli morphism

$$j : \mathcal{M}_g \to \mathcal{A}_g \tag{7.12.1}$$

associates to every curve its principally polarized Jacobian. We denote by $\mathcal{T}_g$ the closed Torelli locus, i.e. $\mathcal{T}_g = \overline{j(\mathcal{M}_g)}$.

As a complex variety, $\mathcal{A}_g = \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g$ is a Shimura variety whose special points are exactly the CM points. Recently, Tsimerman [74] proved a result showing the existence of a lower bound on the size of the Galois orbits of CM points in $\mathcal{A}_g$. Building on joint work with Pila [59], Tsimerman concluded in this way a proof of the André-Oort conjecture for $\mathcal{A}_g$ without the GRH assumption.

Theorem 7.12.1 (André–Oort conjecture [74])**.** *Let Γ be a set of CM points in $\mathcal{A}_g$. Then the Zariski closure of Γ is a finite union of Shimura subvarieties.*

Among the Shimura subvarieties of $\mathcal{A}_g$, a well known example is that of the Hilbert modular variety, whose points are polarized abelian varieties whose endomorphism ring contains the ring of integers of a totally real field of genus g. Hilbert modular varieties play an important role when studying the number of CM points in $\mathcal{T}_g$.

Indeed, let us turn our attention to the case of CM fields with Galois group isomorphic to $C_2^g \rtimes S_g$. Chai and Oort call these fields and their corresponding CM points sufficiently general (see [12, (2.13)] for a justification of this definition). We will use the following result given in [12].

Lemma 7.12.2. *Let Y be an irreducible Shimura subvariety of $\mathcal{A}_g$ of positive dimension. Assume that $Y \neq \mathcal{A}_g$ and that Y contains a sufficiently general CM point y in $\mathcal{A}_g$. Then Y is a Hilbert modular variety attached to the totally real subfield of degree g over $\mathbb{Q}$ contained in the CM field attached to y.*

This lemma allowed the authors of [12] to establish the following result for genus $g > 3$.

Theorem 7.12.3. *Assume the André–Oort conjecture to be true. Then for every $g > 3$ the number of sufficiently general CM points in $\mathcal{T}_g$ is finite.*

When $g = 3$, the closed Torelli locus $\mathcal{T}_3$ coincides with $\mathbb{A}_3$, but we believe that a similar argument can be adapted to genus 3, as soon as we restrict to the hyperelliptic locus. Indeed, let us denote by $\mathcal{M}_3^h$ the image of the subspace of hyperelliptic curves inside the Torelli locus. Then $\mathcal{M}_3^h$ contains infinitely many hyperelliptic curves with CM, since all genus 3 curves with CM by a field containing $\mathbb{Q}(i)$ are hyperelliptic. This is certainly in accordance with the Andre–Oort conjecture, since the Shimura surface parametrising points whose endomorphism ring contains $\sqrt{-1}$ is contained in $\mathcal{M}_3^h$.

Assume now that $\mathcal{M}_3^h$ contains infinitely many sufficiently general CM points. Then by the André–Oort conjecture and Lemma 7.12.2, it contains a Hilbert modular variety attached to a totally real field of degree 3. Recall that among the exceptional hyperelliptic fields listed in Table 7.3, 14 are mixed, i.e. they allow both a hyperelliptic and non-hyperelliptic curve. This quickly disproves the fact that the Hilbert modular variety corresponding to the real multiplication subfield of each of these fields could be contained in the hyperelliptic locus. For the remaining 3 exceptional hyperelliptic fields listed in the Table, we cannot reach a similar conclusion for the corresponding real multiplication subfields and their Hilbert modular varieties. One way to tackle the question experimentally would be to adapt our implementation to compute points with CM by non-maximal orders, which contain the maximal real multiplication order in these fields. Once the period matrices of these points are determined, it would suffice to use Algorithm 4 to check heuristically that some of the corresponding curves are not hyperelliptic.

As stated in the introduction, we do not have enough evidence to support the claim that the list of exceptional hyperelliptic CM fields mentioned in Theorems 7.2.1 and 7.2.3 is complete and we certainly do not claim that. However, the considerations above support the conjecture that the full list of exceptional hyperelliptic CM fields should be finite.

Cryptographic implications

Let us now turn our attention to applications in cryptography. The Discrete Logarithm Problem (DLP) in Jacobians of hyperelliptic curves defined over a finite field $\mathbb{F}_q$ (with $q = p^d$ and p a prime) can be solved in $\widetilde{O}(q^{4/3})$, using the index calculus algorithm of Gaudry, Thériault and Diem [25]. In contrast, Jacobians of non-hyperelliptic curves of genus 3 are amenable to Diem's index calculus algorithm, which requires only $\widetilde{O}(q)$ group operations to solve the DLP [10]. As a consequence, an efficient way of attacking DLP on a genus 3 hyperelliptic Jacobian is by reducing it to a DLP on a non-hyperelliptic Jacobian via an explicit isogeny. Assuming that the kernel of the isogeny will intersect trivially with the subgroup of cryptographic interest, we derive a $\widetilde{O}(q)$ time attack on the hyperelliptic Jacobian (see [66]). So an interesting question is how to find such isogenies.

Idea of the attack. To tackle this question, let us consider A an ordinary ppav defined over $\mathbb{F}_q$ isomorphic to a hyperelliptic Jacobian. The theory of canonical lifts of Serre and Tate allows us to lift A to an ordinary ppav $\widetilde{A}$ defined over $W(\mathbb{F}_q)$, the ring of Witt vectors of $\mathbb{F}_q$, such that $\mathrm{End}(A) \simeq \mathrm{End}(\widetilde{A})$ and $A \to \widetilde{A}$ is functorial (see [5]). After fixing an embedding $W(\bar{\mathbb{F}}_q) \hookrightarrow \mathbb{C}$, we may assume that $\widetilde{A}$ is a ppav defined over $\mathbb{C}$ with CM by the maximal ring of integers of K and CM type Φ. As suggested by the Theorems 7.2.1 and 7.2.3, hyperelliptic Jacobians with CM are

rare, hence most of the times we expect $\widetilde{A}$ to be a non-hyperelliptic Jacobian with hyperelliptic reduction mod p. We now consider the following graph: the vertices are absolutely simple 3-dimensional ppav defined over $\mathbb{C}$ with CM by the maximal order of K and the edges are isogenies between ppavs. In the literature, this is known as the *horizontal isogeny graph* (see for instance [34]). Moreover, by [63, Ch. III, Sec. 11, Prop. 13], the isogenies in this graph will reduce to isogenies defined over $\mathbb{F}_q$ of equal degree.

In this graph, our goal is to find an isogeny from $\widetilde{A}$ to another ppav, which has good quartic reduction at p. The problem is not trivial, since the number of vertices in this graph is $O(\#\mathcal{C}_K)$, hence it grows exponentially with the size of the class group of K. If we construct an isogeny to a p.p.a.v. on the Galois orbit of $\widetilde{A}$ as in Theorem 7.8.1, then the target variety will also have hyperelliptic reduction at p.

Consequently, we will choose an isogeny $\widetilde{I}$ corresponding to a non-trivial element in $\mathcal{C}_K/\mathrm{im}(\mathcal{N})$ (preferably the one which allows an ideal representative of smallest possible norm). We denote by $\widetilde{B}$ the target ppav obtained in this way and by B its reduction $\pmod{p}$. Heuristically, both $\widetilde{B}$ and B are isomorphic to non-hyperelliptic Jacobians. To support this heuristic, we computed all primes of hyperelliptic reduction for all non-hyperelliptic orbits for a given CM field.

Example 7.12.4. As an example, we revisit the case of the CM field of equation $x^6 - 2x^5 + x^4 - 4x^3 + 5x^2 - 50x + 125$, which is the sixth entry in Table 7.3. Recall that for this field there is one hyperelliptic orbit of length 4 and three non-hyperelliptic orbits under conjugation by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The Dixmier-Ohno invariants of plane quartics with CM by this field are defined over a degree 4 extension field of $\mathbb{Q}$ of equation $x^4 - 17x^3 - 24x^2 + 7$. We computed invariants for one curve on each of the non-hyperelliptic orbits (see [18] for the numerical values). With these in hand, we computed the primes of hyperelliptic reduction for these CM points, using the criterion in [41, Theorem 1.10]. We list the results in Table 7.4, where as before the subscripts denote the norms of the ideals. We can see that the lists of primes of hyperelliptic reduction for different orbits are almost disjoint (only $\mathfrak{p}_{29}$ appears in two of these lists).

Orbit	Prime ideals of hyperelliptic reduction
1	$\mathfrak{p}_{29}, \mathfrak{p}_{151}, \mathfrak{p}_{331}, \mathfrak{p}_{15937}, \mathfrak{p}_{2986259}$
2	$\mathfrak{p}_{29}, \mathfrak{p}_{53}, \mathfrak{p}_{409}, \mathfrak{p}_{2251}, \mathfrak{p}_{27509}, \mathfrak{p}_{37423}, \mathfrak{p}_{154757110537}$
3	$\mathfrak{p}_{71}, \mathfrak{p}_{827}, \mathfrak{p}_{2207}, \mathfrak{p}_{3181}, \mathfrak{p}_{6133}$

Table 7.4: Hyperelliptic reduction for non-hyperelliptic curves with CM by the field with defining polynomial $x^6 - 2x^5 + x^4 - 4x^3 + 5x^2 - 50x + 125$.

8

Genus 3 Hyperelliptic Curves with Complex Multiplication via Shimura Reciprocity

This chapter contains the main results in [17]. The paper in [17] based on the previous paper [1] which in turn is based on the paper [79]. We briefly explain the motivation of this chapter.

A we have seen in Theorem 3.4.1, in genus 3 every simple principally polarized abelian variety of dimension 3 is isomorphic to the Jacobian of a smooth projective curve. This is either a hyperelliptic curve or a plane quartic. In [79, Lemma 4.5], *Weng* shows that a simple principally polarized abelian threefold with complex multiplication by a sextic CM field containing $\mathbb{Q}(i)$ is a hyperelliptic Jacobian. In the same paper the author gives an algorithm to compute hyperelliptic curves whose Jacobians have complex multiplication by a sextic field containing $\mathbb{Q}(i)$. In later work, *Balakrishnan, Ionica, Lauter, and Vincent* give an algorithm which removes this restriction on the CM field, by performing a heuristic check, see [1]. This heuristic relies on the so-called *Mumford's Vanishing Criterion* (see Theorems 5.4.14 and 5.5.1), which states that a genus 3 smooth projective curve is hyperelliptic if and only if one of the 36 even theta constants is 0. The authors in [1] developed an algorithm which is available in [2], and which performs as follows: For a given small period matrix $Z \in \mathcal{H}_3$ with complex multiplication, their algorithm first computes the theta constants (see Definition 5.3.1) to Z with enough precision to determine if there is one which approximates zero, and then computes the Rosenhain invariants by the formula in Equation (5.5.1). By class field theory, these invariants generate a certain subfield of the so-called *ray class field* of modulus 2 over the reflex field K^r of K. By approximating them with high precision, we can recognize them as algebraic numbers. This method has its limitations, since as soon the degree of the class field over which the Rosenhains are defined is large, i.e. (≥ 500), the complexity of the algebraic dependence computation becomes a bottleneck. Further, the authors in [1] considered only examples of CM fields with class number 1. In [17], the second author and I considered the action of the group $\mathrm{Gal}(CM_{\mathfrak{m}}(K^r)|K^r)$ on hyperelliptic CM points, where $CM_{\mathfrak{m}}(K^r)$ is a subfield of the ray class field of a given finite modulus $\mathfrak{m}$. After identifying a hyperelliptic curve X by verifying computationally and heuristically the condition in Theorem 5.4.14, we compute the Galois conjugates of its invariants via *Shimura's reciprocity law*. With these in hand we compute the so-called Rosenhain and the Shioda class polynomials.

In order to compute examples for the class polynomials of the Rosenhain and Shioda invariants, I have developed and implemented methods in SageMath and Magma. These methods contain the construction of CM types (K,Φ) and their reflex CM types (K^r,Φ^r). The computation of primitive CM types for genus 3 in [2] is dependent on the group structure of $\mathrm{Gal}(L|\mathbb{Q})$. My implementation of CM types is independent of this group isomorphism, and works for all genera. I also have implemented the reflex type norm, as well as the image of the typenorm as a subgroup in the Shimura class group and the action on CM points in Definition 8.3.11. Since SageMath does not implement ray class groups, I used in SageMath the interface to Magma to compute the group $\mathrm{Cl}_m(K^r)$ and enumerate elements in $\mathcal{N}_{\Phi^r,\mathfrak{m}}(Cl_m(K^r))$.

8.1 Definitions

Let K be a CM field of degree $2g$ and let $\rho \in \mathrm{Aut}(K)$ be the complex conjugation on K (see Definition 6.1.5). For the rest of this chapter, we denote by L the Galois closure of K and we fix once for all, as in the same definition, an embedding

$$\iota_L : L \to \mathbb{C}. \tag{8.1.1}$$

The main objects in this chapter are simple principally polarized abelian varieties of dimension 3 over $\mathbb{C}$ of type (K, Φ) whose endomorphism ring is isomorphic to the maximal order $\mathcal{O}_K$. According to Remark 6.2.8, these are given by tuples (triples, respectively)

$$(A, E) \cong A(\mathfrak{a}, \xi) = A(\Phi, \mathfrak{a}, \xi), \tag{8.1.2}$$

where Φ is a primitive CM type of K, where $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal and where ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K and where $\varphi(\xi)$ is an positive imaginary element for any $\varphi \in \Phi$, and where $(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$. By Theorem 3.4.1, (A, E) is as a simple principally polarized abelian variety with CM by $\mathcal{O}_K$ isomorphic to the Jacobian variety $(\mathrm{Jac}(X), E)$ of a smooth projective curve of genus 3. In this chapter, projective curves X are (as in Definition 4.1.1) defined over some algebraically closed fields $k = \bar{k}$, where $\mathrm{char}(k) \neq 2$.

As in Definition 7.7.1, let $\mathcal{M}_{\mathcal{O}_K}(\Phi) \subset \mathcal{A}_3(\overline{\mathbb{Q}})$ be the set of isomorphism classes of principally polarized abelian varieties with CM by $\mathcal{O}_K$ of type Φ. Let (K^r, Φ^r) be the reflex CM type of (K, Φ). Let $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$ be the reflex type norm map in Definition 7.6.4, given by

$$[\mathfrak{a}] \mapsto \left[\mathcal{O}_K \cap \prod_{\varphi \in \Phi^r} \varphi(\mathfrak{a}) \mathcal{O}_L \right] \tag{8.1.3}$$

for any $[\mathfrak{a}] \in Cl(K^r)$. In order to determine Galois orbits of principally polarized abelian varieties $A(\mathfrak{a}, \xi) \in \mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the action of the group $G^r = \mathrm{Gal}(\overline{\mathbb{Q}} | K^r)$, we introduced in Definition 7.6.5 the map $\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K$ given by

$$[\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})) \tag{8.1.4}$$

where $N = N_{K^r|\mathbb{Q}}$ is the extension of the absolute norm-map to fractional $\mathcal{O}_{K^r}$-ideals. Then by the first Main Theorem of CM (see Theorem 7.8.1), for any $\sigma \in G^r$ which under the Artin map σ correspond to the ideal class $[\mathfrak{b}] \in \mathrm{Cl}(K^r)$. We have

$$\sigma(A(\mathfrak{a}, \xi)) \cong A\left(\mathcal{N}_{\Phi^r}(\mathfrak{b})(\mathfrak{a}, \xi)\right).$$

Therefore the Galois orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under G^r are the orbits of $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ under the action of $\mathrm{im}(\mathcal{N}_{\Phi^r})$.

In order to compute class (Rosenhain) polynomials, we consider the set of isomorphism classes of simple principally polarized abelian varieties with CM by $\mathcal{O}_K$, together with some data related to their 2-torsion points, which we will specify in this chapter. By class field theory, these invariants generate a certain subfield of the so-called ray class field of modulus 2 over the reflex field K^r.

We begin our discussion by introducing some basic properties about class field theory.

8.2 Class field theory

We follow in this section the theory in [16, Chapter 2].

For a number field K and a *finite* modulus $\mathfrak{m}$ (i.e. a product of prime ideals in K), let $I_{\mathfrak{m}}(K)$ be the group of all fractional $\mathcal{O}_K$-ideals coprime to $\mathfrak{m}$. We consider the group

$$P_{\mathfrak{m}}(K) = \{\mathfrak{a} \in I_{\mathfrak{m}}(K) : \mathfrak{a} = \alpha\mathcal{O}_K,\ \alpha \equiv 1 \pmod{^*\mathfrak{m}}\},$$

where the congruence $\alpha \equiv 1 \pmod{^*\mathfrak{m}}$ means that for all primes $\mathfrak{p}$ appearing in the factorisation of $\mathfrak{m}$ we have $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$, where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-valuation.

Remark 8.2.1. As stated above, in this section our modulus $\mathfrak{m} = 2\mathcal{O}_K$ (and $m\mathbb{Z} = \mathfrak{m} \cap \mathbb{Z}$ in K^r, respectively) is finite. In a more general context of class field theory, one may consider a modulus as a formal product of finite and *infinite primes*. The latter are determined by embeddings $K \hookrightarrow \mathbb{R}$ and by (pairs of) embeddings $K \hookrightarrow \mathbb{C}$, respectively. See [16, Page 94].

Definition 8.2.2. We define the *ray class group* of a number field K for a modulus $\mathfrak{m}$ to be the quotient group

$$Cl_{\mathfrak{m}}(K) = I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K).$$

Example 8.2.3. If $\mathfrak{m} = 1\mathcal{O}_K$ then $Cl_{\mathfrak{m}}(K)$ is the ideal class group $Cl(K)$ of K.

Definition 8.2.4. Let K be a number field and let $\mathfrak{m}$ be a modulus of K. There is a unique abelian extension $\mathcal{H}_{\mathfrak{m}}$ of K, whose ramified primes, finite or infinite, divide $\mathfrak{m}$, such that if

$$\Phi_{\mathfrak{m}} : I_{\mathfrak{m}}(K) \to \mathrm{Gal}(\mathcal{H}_{\mathfrak{m}} \,|\, K)$$

is the *Artin Map* of $K \subset \mathcal{H}_{\mathfrak{m}}$, then $P_{\mathfrak{m}}(K) = \ker(\Phi_{\mathfrak{m}})$. We call $\mathcal{H}_{\mathfrak{m}}$ the *ray class field* of K for the modulus $\mathfrak{m}$ (see e.g.[16, Theorem 8.6 and Page 149]).

Example 8.2.5. If K is a number field and $\mathfrak{m} = 1\mathcal{O}_K$ then $\mathcal{H}_{\mathfrak{m}}$ is the *Hilbert class field* H of K. It is the maximal unramified abelian extension of K, see [16, Theorem 8.10].

8.3 The Shimura class group modulus $\mathfrak{m}$ and the Galois action

Let (K, Φ) be a primitive CM type. There is a generalization of the Shimura class group $\mathcal{C}_K$ (see Definition 7.6.1) of K, denoted by $\mathcal{C}_{\mathfrak{m}}(K)$ for a finite modulus $\mathfrak{m}$ of K. Building on this generalization, we construct in this section maps $N_{\Phi^r,\mathfrak{m}}$ and $\mathcal{N}_{\Phi^r,\mathfrak{m}}$ as generalizations of the maps N_{Φ^r} (see Equation (8.1.3)) and $\mathcal{N}_{\Phi^r}$ (see Equation (8.1.4)). There is an action of the Galois group $\mathrm{Gal}(CM_{\mathfrak{m}}(K^r) \,|\, K^r)$ on the set of equivalence classes of principally polarized abelian varieties with CM by $\mathcal{O}_K$ of type Φ, together with some data related to their 2-torsion points, which we will specify in this chapter, where the orbits correspond to elements of the quotient $\mathcal{C}_{\mathfrak{m}}(K)/\mathrm{im}(\mathcal{N}_{\Phi^r,\mathfrak{m}})$. In this section we introduce these structures and we begin this section by the following definition.

Definition 8.3.1. Let K be a CM field and let $\mathfrak{m}$ be a modulus on K. The *Shimura class group* $\mathcal{C}_{\mathfrak{m}}(K)$ of K modulus $\mathfrak{m}$ is the abelian group of equivalence classes

$$\mathcal{C}_{\mathfrak{m}}(K) = \left\{ (\mathfrak{a}, \alpha) : \begin{array}{l} \mathfrak{a} \in I_{\mathfrak{m}}(K) \text{ such that } \mathfrak{a}\bar{\mathfrak{a}} = \alpha\mathcal{O}_K, \\ \alpha \in K_0 \text{ totally positive},\ \ \alpha \equiv 1 \pmod{^*\mathfrak{m}} \end{array} \right\} \Big/ \sim, \tag{8.3.1}$$

where $(\mathfrak{a},\alpha)\sim(\mathfrak{a}',\alpha')$ if $(\mathfrak{a}',\alpha')=(\mu\mathfrak{a},\mu\overline{\mu}\alpha)$ for $\mu\in K^*$ and $\mu\equiv 1 \pmod{{}^*\mathfrak{m}}$. The multiplication of two equivalence classes $(\mathfrak{a},\alpha)$ and $(\mathfrak{a}',\alpha')$ is given by

$$(\mathfrak{a},\alpha)\cdot(\mathfrak{a}',\alpha')=(\mathfrak{a}\mathfrak{a}',\alpha\alpha').$$

Given a pair $(\mathfrak{a},\alpha)$ satisfying the conditions in Equation (8.3.1) we denote by $(\mathfrak{a},\alpha)_{\mathfrak{m}}$ the corresponding equivalence class. The identity element is given by $(\mathcal{O}_K,1)_{\mathfrak{m}}$. See [63, Page 115].

Definition 8.3.2. Let (K,Φ) be a CM type with reflex CM type (K^r,Φ^r). Let $\mathfrak{m}$ be a modulus of K and let $m\mathbb{Z}=\mathfrak{m}\cap\mathbb{Z}$. The *reflex type norm* for $\mathfrak{m}$ is a map $N_{\Phi^r}=N_{\Phi^r,\mathfrak{m}}:\mathrm{Cl}_m(K^r)\to\mathrm{Cl}_{\mathfrak{m}}(K)$ given by

$$[\mathfrak{a}]\mapsto\left[\mathcal{O}_K\cap\prod_{\varphi\in\Phi^r}\varphi(\mathfrak{a})\mathcal{O}_L\right] \tag{8.3.2}$$

for any $[\mathfrak{a}]\in\mathrm{Cl}_m(K^r)$.

Definition 8.3.3. Let $N=N_{K^r|\mathbb{Q}}$ be the extension of the absolute norm-map to fractional $\mathcal{O}_{K^r}$-ideals. Combining this map with the reflex type norm for $\mathfrak{m}$ in Equation (8.3.2), we obtain a map from the ray class group of K^r modulus $m\mathbb{Z}=\mathfrak{m}\cap\mathbb{Z}$ to the Shimura class group of K modulus $\mathfrak{m}$, namely

$$\begin{aligned}\mathcal{N}_{\Phi^r,\mathfrak{m}}:\mathrm{Cl}_m(K^r)&\to\mathcal{C}_{\mathfrak{m}}(K)\\ [\mathfrak{a}]&\mapsto(N_{\Phi^r}(\mathfrak{a}),N(\mathfrak{a}))_{\mathfrak{m}}.\end{aligned} \tag{8.3.3}$$

By following the construction of Shimura in [63, Page 118], we construct the following subgroup of $I_{\mathfrak{m}}(K)$: Let (K,Φ) be a primitive CM type with reflex CM type (K^r,Φ^r). Let $m\in\mathbb{Z}$ such that $m\mathbb{Z}=\mathfrak{m}\cap\mathbb{Z}$ and denote by $I_m(K^r)$ the group of fractional ideals in K^r coprime to m. Following [63, Chapter 16], we consider the group

$$H_{\mathfrak{m}}(K^r)=\left\{\mathfrak{a}\in I_m(K^r):\begin{array}{ll}\exists\alpha\in K^* \text{ with} & N_{\Phi^r}(\mathfrak{a})=\alpha\mathbb{Z}_K,\\ N_{K^r|\mathbb{Q}}(\mathfrak{a})=\alpha\overline{\alpha}, & \alpha\equiv 1 \pmod{{}^*\mathfrak{m}}\end{array}\right\}. \tag{8.3.4}$$

Note that $P_{\mathfrak{m}}(K^r)\subset H_{\mathfrak{m}}(K^r)$. By [16, Theorem 8.6] there is (up to isomorphism) a unique abelian extension $CM_{\mathfrak{m}}(K^r)$ of K^r, such that under the Artin map of $K^r\subset CM_{\mathfrak{m}}(K^r)$,

$$G^r_{\mathfrak{m}}:=\mathrm{Gal}(CM_{\mathfrak{m}}(K^r)|K^r)\cong I_m(K^r)/H_{\mathfrak{m}}(K^r). \tag{8.3.5}$$

Remark 8.3.4. The effective construction of the field $CM_{\mathfrak{m}}(K^r)$ as a subfield of the ray class field $\mathcal{H}_{\mathfrak{m}}$ modulus $\mathfrak{m}$ of the reflex field K^r, relies on *Shimura's Second Main Theorem* (see Thereom 8.4.1). In order to compute Galois conjugates of elements in this number field, which we will explain in this section, we need to compute the right quotient group in Equation (8.3.5).

Lemma 8.3.5. *Let (K,Φ) be a primitive CM type with reflex CM type (K^r,Φ^r). Let $\mathfrak{m}$ be a modulus of K and let $m\mathbb{Z}=\mathfrak{m}\cap\mathbb{Z}$. Consider the map $\mathcal{N}_{\Phi^r,\mathfrak{m}}:Cl_m(K^r)\to\mathcal{C}_{\mathfrak{m}}(K)$ in Definition 8.3.3. Then:*

(i) $\ker(\mathcal{N}_{\Phi^r,\mathfrak{m}})\cong H_{\mathfrak{m}}(K^r)/P_m(K^r)$.

(ii) $\mathrm{im}(\mathcal{N}_{\Phi^r,\mathfrak{m}})\cong I_m(K^r)/H_{\mathfrak{m}}(K^r)$.

Proof. (i) If $\mathfrak{a} \in \ker(\mathcal{N}_{\Phi^r,\mathfrak{m}})$ then $(N_{\Phi^r}(\mathfrak{a}), N_{K^r/\mathbb{Q}}(\mathfrak{a}))_{\mathfrak{m}} = (\mathcal{O}_K, 1)_{\mathfrak{m}}$. Then there exists an element $\mu \in K^*$ such that

$$(N_{\Phi^r}(\mathfrak{a}), N_{K^r|\mathbb{Q}}(\mathfrak{a})) = (\mu\mathcal{O}_K, \mu\bar{\mu})$$

and $\mu \equiv 1 \pmod{{}^*\mathfrak{m}}$. Conversely, by the definition of $P_m(K^r)$ in Equation (8.3.4) and $P_m(K^r) \subset H_{\mathfrak{m}}(K^r)$, any equivalence class in $H_{\mathfrak{m}}(K^r)/P_m(K^r)$ is in $\ker(\mathcal{N}_{\Phi^r,\mathfrak{m}}$.

(ii) It follows from the 3-rd. isomorphism theorem of groups

$$\mathcal{N}_{\Phi^r,\mathfrak{m}}(Cl_m(K^r)) \cong \frac{Cl_m(K^r)}{\ker(\mathcal{N}_{\Phi^r,\mathfrak{m}})} \cong \frac{(I_m(K^r)/P_m(K^r))}{(H_{\mathfrak{m}}(K^r)/P_m(K^r))} \cong \frac{I_m(K^r)}{H_{\mathfrak{m}}(K^r)}.$$

□

Remark 8.3.6. In my implementation in [2], I computed a set of generators for $Cl_m(K^r)$ using Magma, and then implemented an algorithm for enumerating the elements in the set $\mathcal{N}_{\Phi^r,\mathfrak{m}}(\mathrm{Cl}_m(K^r))$. Due to Lemma 8.3.5, this allowed us in [17] to compute the group $I_m(K^r)/H_{\mathfrak{m}}(K^r)$ and enumerate Galois conjugates of a CM points.

In order to introduce the action of the Galois group $G^r_{\mathfrak{m}}$ (see Equation 8.3.5), as a generalization of the action in Theorem 7.8.1, on abelian varieties with CM by $\mathcal{O}_K$ of type Φ, together with some data related to their torsion points, we need to specify these 2-torsion points. This is given by the following definition.

Definition 8.3.7. For a modulus $\mathfrak{m}$ of K, we denote by

$$A[\mathfrak{m}](\mathbb{C}) = \{x \in A : \ \iota(\alpha)x = 0, \forall \alpha \in \mathfrak{m}\},$$

the group of the $\mathfrak{m}$-torsion points of $A(\mathbb{C})$, where $\iota : K \hookrightarrow \mathrm{End}^0(A)$ is the embedding in Definition 6.1.1. We call a point $t \in A(\mathbb{C})[\mathfrak{m}]$ *proper* if for $a \in \mathcal{O}_K$, the equality

$$\iota(a)t = 0$$

implies $a \in \mathfrak{m}$. See [63, Page 56].

Definition 8.3.8. Let (K, Φ) be a primitive CM type. We define by $\mathrm{Princ}(K, \Phi, \mathfrak{m})$ the set of isomorphism classes of principally polarized abelian variety with CM by $\mathcal{O}_K$ of type Φ together with a proper $\mathfrak{m}$-torsion point.

Remark 8.3.9. By Proposition 6.2.3, any tuple $(\mathfrak{a}, \xi)$ where $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal and where ξ is an element in K such that $-\xi^2$ is totally positive in the totally real subfield K_0 of K and where $\varphi(\xi)$ is an positive imaginary element for any $\varphi \in \Phi$, and where $(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$, identifies an abelian variety with CM by $\mathcal{O}_K$ of type Φ, isomorphic to

$$A(\mathfrak{a}, \xi, t) = A(\Phi, \mathfrak{a}, \xi, t)$$

together with a proper $\mathfrak{m}$-torsion point $t \in A[\mathfrak{m}](\mathbb{C})$ up to equivalence. In our computations of Galois conjugates we will extensively use the following action of the class group $I_m(K^r)/H_{\mathfrak{m}}(K^r)$ on $\mathrm{Princ}(K, \Phi, \mathfrak{m})$ given by Shimura [63, Section 16.3].

Remark 8.3.10. There is a surjection $\pi : \mathrm{Princ}(K, \Phi, \mathfrak{m}) \to \mathcal{M}_{\mathcal{O}_K}(\Phi)$ which sends $A(\mathfrak{a}, \xi, t)$ to $A(\mathfrak{a}, \xi)$ by forgetting the proper t-torsion point.

We can now state the action of the Galois group $G_{\mathfrak{m}}^r$ (see Equation 8.3.5), as a generalization of the action in Theorem 7.8.1, on the set

$$\mathrm{Princ}(K, \Phi, \mathfrak{m})$$

of isomorphism classes of principally polarized abelian variety with CM by $\mathcal{O}_K$ of type Φ together with a proper $\mathfrak{m}$-torsion point.

Definition 8.3.11. Let $(A, E) \cong A(\mathfrak{a}, \xi, t)$ in $\mathrm{Princ}(K, \Phi, \mathfrak{m})$, and let $\sigma \in G_{\mathfrak{m}}^r$. Suppose that under the Artin map, the element σ correspond to the class of the ideal $\mathfrak{c}$. Then

$$\sigma(A(\Phi, \mathfrak{a}, \xi, t)) \cong A(\mathcal{N}_{\Phi^r, \mathfrak{m}}(\mathfrak{b})(\mathfrak{a}, \xi, t)), \tag{8.3.6}$$

where $A(\mathcal{N}_{\Phi^r, \mathfrak{m}}(\mathfrak{b})(\mathfrak{a}, \xi, t)) = A(N_{\Phi^r, \mathfrak{m}}(\mathfrak{c})^{-1}\mathfrak{a},\ N(\mathfrak{c})\xi,\ t \pmod{N_{\Phi^r, \mathfrak{m}}(\mathfrak{c})^{-1}\mathfrak{a}})$.

8.4 Shimura's Second Main Theorem of complex multiplication

Let K be a CM field and let (A, E) be a principally polarized abelian variety with CM by $\mathcal{O}_K$. In order to state Shimura's second Main Theorem of complex multiplication, we need to consider the *normalized Kummer variety* of A (see [63, Theorem 3, Section 4.4]). It is given by a tuple

$$(W, h),$$

where W is the quotient of A by its automorphism group. It is defined over the field of moduli k_0 of A (see Remark 7.5.10), and where $h : A \to W$ is the natural projection map.

Theorem 8.4.1. *Let (A, E) be a principally polarized abelian variety with CM by $\mathcal{O}_K$ and CM type Φ and let be (W, h) its normalized Kummer variety. Let $\mathfrak{m}$ be a fractional $\mathcal{O}_K$-ideal and let t be a proper $\mathfrak{m}$-torsion point. Let k_0 be the field of moduli of A, K^r the reflex field of K and $k_0^* = k_0 K^r$. Then $k_0^*(h(t))$ is the class field of K^r corresponding to the ideal group $H_{\mathfrak{m}}(K^r)$.*

Proof. See [63, Main Theorem 2 on Page 118]. □

8.5 Computing class polynomials

We turn our attention now to the main task in the paper [17], the computation of the *Shioda* and *Rosenhain invariants* of hyperelliptic curves of genus 3 with CM by $\mathcal{O}_K$, and more precisely to obtaining their minimal polynomials over the reflex field K^r of K. Let

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

be a hyperelliptic curve of genus 3 over some algebraically close fields k of characteristic $\neq 2$. In Definition 4.3.4, we introduced the Rosenhain coefficients (invariants) of X as the roots λ_i of f, where $\lambda_i \in k \backslash \{0, 1, \infty\}$. Then in Section 5.4 we have seen that, given a small hyperelliptic period matrix Z in the Siegel upper half space $\mathcal{H}_3$, we can compute these invariants as quotients of theta functions with half-integer characteristics by the formula of Takase-Vincent-Somoza (see Theorem 5.5.2).

We begin this section with a brief introduction about the so-called Shioda invariants. For a detailed discussion about invariants of curves of genus 3, see e.g. the papers [42], [33] and [48].

Shioda [64] gave a set of generators for the algebra of invariants of binary octavics over the complex numbers which are now called *Shioda invariants*. Following Shioda's notation (see [64, page 1025]), these are 9 weighted projective invariants

$$(J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9, J_{10}),$$

where $\deg(J_i) = i$. The invariants $J_2, \ldots, J_7$ are algebraically independent, while J_8, J_9, J_{10} depend algebraically on them. Note that over the complex numbers Shioda invariants completely determine points in the moduli space of hyperelliptic curves of genus 3.
Using Igusa's map between the graded ring of Siegel modular forms of degree 3 and the graded ring of invariants of binary octavics, Lorenzo García [48] proposes a set of invariants which can be written as quotients of modular forms. These invariants involve large powers of the modular form χ_{28} (for a definition see e.g. [48]) in the denominators and we do not use them for experiments since they would need too much precision to compute.

Starting from the projective invariants J_i, we consider the following absolute[1] Shioda invariants :

$$\mathrm{Shi} = \left(\frac{J_2^7}{\Delta}, \frac{J_2^4 J_3^2}{\Delta}, \frac{J_2^5 J_4}{\Delta}, \frac{J_5 J_9}{\Delta}, \frac{J_2^4 J_6}{\Delta}, \frac{J_7^2}{\Delta}, \frac{J_2^3 J_8}{\Delta}, \frac{J_2^5 J_9^2}{\Delta^2}, \frac{J_2^2 J_{10}}{\Delta} \right), \tag{8.5.1}$$

with Δ the discriminant of the binary octavic, which is an invariant of degree 14. They are optimal for computations in the sense that they involve invariants of small weight and the values of their denominators for a given curve are products of powers of the primes of bad reduction of the curve (see [33]). Note that a subset of this set was already used by Weng [79] for computing models of hyperelliptic curves with CM by a field which contains i.

Proposition 8.5.1. *The invariants in Equation* (8.5.1) *are modular, i.e. they can be written as quotients of Siegel modular forms of level 1.*

[1] An absolute invariant is a ratio of homogeneous invariants of the same degree.

Proof. The proof of this statement is straightforward, by using Igusa's map on the set of invariants described by Tsuyumine [75] and the relations between Tsuyumine's invariants and the Shioda projective invariants, computed by Lorenzo Garcia [48]. We have

$$\begin{aligned}
\frac{J_2^7}{\Delta} &= c_2^7\frac{I_2}{\Delta} = c_2^7\rho\left(\frac{\gamma_{20}^7}{\chi_{28}^5}\right),\\
\frac{J_2^4J_3^2}{\Delta} &= c_2^4c_3^2\frac{I_2^4I_3^2}{\Delta} = c_2^4c_3^2\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right),\\
\frac{J_2^5J_4}{\Delta} &= \frac{c_2^5I_2^5(c_{41}I_2^2+c_{42}I_4)}{\Delta} = d_1\rho\left(\frac{\gamma_{20}^7}{\chi_{28}^5}\right)+d_2\rho\left(\frac{\gamma_{20}^5\alpha_{12}}{\chi_{28}^4}\right),\\
\frac{J_5J_9}{\Delta} &= \frac{(c_{51}I_2I_3+c_{52}I_5)\left(c_{91}I_2^3I_3+c_{92}I_2^5I_5+c_{93}I_2I_3I_4+c_{94}I_2I_7+c_{95}I_3^3+c_{96}I_3I_6+c_{97}I_4I_5+c_{98}I_9\right)}{\Delta}\\
&= e_1\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right)+e_2\rho\left(\frac{\gamma_{20}^3\gamma_{30}\beta_{22}}{\chi_{28}^4}\right)+e_3\rho\left(\frac{\gamma_{20}^2\gamma_{30}^2\alpha_{12}}{\chi_{28}^4}\right)+e_4\rho\left(\frac{\gamma_{20}^2\gamma_{30}\beta_{14}}{\chi_{28}^3}\right)+e_5\rho\left(\frac{\gamma_{20}\gamma_{30}^4}{\chi_{28}^5}\right)\\
&+ e_6\rho\left(\frac{\gamma_{20}\gamma_{30}^2\alpha_4}{\chi_{28}^3}\right)+e_7\rho\left(\frac{\gamma_{20}\gamma_{30}\alpha_{12}\beta_{22}}{\chi_{28}^3}\right)+e_8\rho\left(\frac{\gamma_{20}\gamma_{30}\alpha_6}{\chi_{28}^2}\right)+e_9\rho\left(\frac{\gamma_{20}^3\gamma_{30}\beta_{22}}{\chi_{28}^4}\right)+e_{10}\rho\left(\frac{\gamma_{20}^2\beta_{22}^2}{\chi_{28}^3}\right)\\
&+ e_{11}\rho\left(\frac{\gamma_{20}\beta_{22}\beta_{14}}{\chi_{28}^2}\right)+e_{12}\rho\left(\frac{\gamma_{30}^3\beta_{22}}{\chi_{28}^4}\right)+e_{13}\rho\left(\frac{\gamma_{30}\beta_{22}\alpha_4}{\chi_{28}^2}\right)+e_{14}\rho\left(\frac{\alpha_{12}\beta_{22}^2}{\chi_{28}^2}\right)+e_{15}\rho\left(\frac{\beta_{22}\alpha_6}{\chi_{28}}\right),\\
\frac{J_2^4J_6}{\Delta} &= \frac{c_2^4I_2^4\left(c_{61}I_2^3+c_{62}I_2I_4+c_{63}I_3^2+c_{64}I_6\right)}{\Delta}\\
&= f_1\rho\left(\frac{\gamma_{20}^7}{\chi_{28}^5}\right)+f_2\rho\left(\frac{\gamma_{20}^5\alpha_{12}}{\chi_{28}^4}\right)+f_3\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right)+f_4\rho\left(\frac{\gamma_{20}^4\alpha_4}{\chi_{28}^3}\right),\\
\frac{J_7^2}{\Delta} &= \frac{\left(c_{71}I_2^2I_3+c_{72}I_2I_5+c_{73}I_3I_4+c_{74}I_7\right)^2}{\Delta}\\
&= g_1\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right)+g_2\rho\left(\frac{\gamma_{20}^3\gamma_{30}\beta_{22}}{\chi_{28}^4}\right)+g_3\rho\left(\frac{\gamma_{20}^2\gamma_{30}^2\alpha_{12}}{\chi_{28}^4}\right)+g_4\rho\left(\frac{\gamma_{20}^2\gamma_{30}\beta_{14}}{\chi_{28}^3}\right)+g_5\rho\left(\frac{\gamma_{20}^2\beta_{22}^2}{\chi_{28}^3}\right)\\
&+ g_6\rho\left(\frac{\gamma_{20}\gamma_{30}\alpha_{12}\beta_{22}}{\chi_{28}^3}\right)+g_7\rho\left(\frac{\gamma_{20}\beta_{22}\beta_{14}}{\chi_{28}^2}\right)+g_8\rho\left(\frac{\gamma_{30}^2\alpha_{12}^2}{\chi_{28}^3}\right)+g_9\rho\left(\frac{\gamma_{30}\alpha_{12}\beta_{14}}{\chi_{28}^2}\right)+g_{10}\rho\left(\frac{\beta_{14}}{\chi_{28}}\right),
\end{aligned}$$

$$\frac{J_2^3 J_8}{\Delta} = \frac{c_2^3 I_2^3\left(c_{81}I_2^4 + c_{82}I_2^2 I_4 + c_{83}I_2 I_3^2 + c_{84}I_2 I_6 + c_{85}I_3 I_5 + c_{86}I_4^2 + c_{87}I_8\right)}{\Delta}$$
$$= h_1\rho\left(\frac{\gamma_{20}^7}{\chi_{28}^5}\right) + h_2\rho\left(\frac{\gamma_{20}^5\alpha_{12}}{\chi_{28}^4}\right) + h_3\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right) + h_4\rho\left(\frac{\gamma_{20}^4\alpha_4}{\chi_{28}^3}\right)$$
$$+ h_5\rho\left(\frac{\gamma_{20}^3\gamma_{30}\beta_{22}}{\chi_{28}^4}\right) + h_6\rho\left(\frac{\gamma_{20}^3\alpha_{12}^2}{\chi_{28}^3}\right) + h_7\rho\left(\frac{\gamma_{20}^3\gamma_{24}}{\chi_{28}^3}\right),$$
$$\frac{J_2^5 J_9^2}{\Delta^2} = \frac{c_2^5 I_2^5\left(c_{91}I_2^3 I_3 + c_{92}I_2^2 I_5 + c_{93}I_2 I_3 I_4 + c_{94}I_2 I_7 + c_{95}I_3^3 + c_{96}I_3 I_6 + c_{97}I_4 I_5 + c_{98}I_9\right)^2}{\Delta^2}$$
$$= i_1\rho\left(\frac{\gamma_{20}^{11}\gamma_{30}^2}{\chi_{28}^{10}}\right) + i_2\rho\left(\frac{\gamma_{20}^{10}\gamma_{30}\beta_{22}}{\chi_{28}^9}\right) + i_3\rho\left(\frac{\gamma_{20}^9\gamma_{30}^2\alpha_{12}}{\chi_{28}^9}\right) + i_4\rho\left(\frac{\gamma_{20}^9\gamma_{30}\beta_{14}}{\chi_{28}^8}\right) + i_5\rho\left(\frac{\gamma_{20}^8\gamma_{30}^4}{\chi_{28}^{10}}\right)$$
$$+ i_6\rho\left(\frac{\gamma_{20}^8\gamma_{30}^2\alpha_4}{\chi_{28}^8}\right) + i_7\rho\left(\frac{\gamma_{20}^8\gamma_{30}\alpha_{12}\beta_{22}}{\chi_{28}^8}\right) + i_8\rho\left(\frac{\gamma_{20}^8\gamma_{30}\alpha_6}{\chi_{28}^7}\right) + i_9\rho\left(\frac{\gamma_{20}^9\beta_{22}^2}{\chi_{28}^8}\right) + i_{10}\rho\left(\frac{\gamma_{20}^7\gamma_{30}^2\alpha_{12}^2}{\chi_{28}^8}\right)$$
$$+ i_{11}\rho\left(\frac{\gamma_{20}^7\beta_{14}^2}{\chi_{28}^6}\right) + i_{12}\rho\left(\frac{\gamma_{20}^5\gamma_{30}^6}{\chi_{28}^{10}}\right) + i_{13}\rho\left(\frac{\gamma_{20}^5\gamma_{30}^2\alpha_4^2}{\chi_{28}^6}\right) + i_{14}\rho\left(\frac{\gamma_{20}^5\alpha_{12}^2\beta_{22}^2}{\chi_{28}^6}\right) + i_{15}\rho\left(\frac{\gamma_{20}^5\alpha_6^2}{\chi_{28}^4}\right),$$
$$\frac{J_2^2 J_{10}}{\Delta} = \frac{c_2^2 I_2^2\left(c_{101}I_2^5 + c_{102}I_2^3 I_4 + c_{103}I_2^2 I_3^2 + c_{104}I_2^2 I_6 + c_{105}I_2 I_3 I_5 + c_{106}I_2 I_4^2\right)}{\Delta}$$
$$+ \frac{c_2^2 I_2^2\left(c_{107}I_2 I_8 + c_{108}I_3^2 I_4 + c_{109}I_3 I_7 + c_{110}I_4 I_6 + c_{111}I_5^2 + c_{112}I_{10}\right)}{\Delta}$$
$$= j_1\rho\left(\frac{\gamma_{20}^7}{\chi_{28}^5}\right) + j_2\rho\left(\frac{\gamma_{20}^5\alpha_{12}}{\chi_{28}^4}\right) + j_3\rho\left(\frac{\gamma_{20}^4\gamma_{30}^2}{\chi_{28}^5}\right) + j_4\rho\left(\frac{\gamma_{20}^4\alpha_4}{\chi_{28}^3}\right)$$
$$+ j_5\rho\left(\frac{\gamma_{20}^3\gamma_{30}\beta_{22}}{\chi_{28}^4}\right) + j_6\rho\left(\frac{\gamma_{20}^3\alpha_{12}}{\chi_{28}^3}\right) + j_7\rho\left(\frac{\gamma_{20}^3\gamma_{24}}{\chi_{28}^3}\right) + j_8\rho\left(\frac{\gamma_{20}^2\gamma_{30}^2\alpha_{12}}{\chi_{28}^4}\right)$$
$$+ j_9\rho\left(\frac{\gamma_{20}^2\gamma_{30}\beta_{14}}{\chi_{28}^3}\right) + j_{10}\rho\left(\frac{\gamma_{20}^2\alpha_{12}\alpha_4}{\chi_{28}^2}\right) + j_{11}\rho\left(\frac{\gamma_{20}^2\beta_{22}^2}{\chi_{28}^3}\right) + j_{12}\rho\left(\frac{\gamma_{20}^2\beta_{16}}{\chi_{28}^2}\right)$$

where the constants $c_k, d_k, e_k, f_k, g_k, h_k, i_k, j_k$ are computed in [48]. □

For the rest of this chapter we fix the following notation.

Notation 8.5.2. Let $(A,E) \cong A(\mathfrak{a},\xi,t)$ in $\mathrm{Princ}(K,\Phi,\mathfrak{m})$, and let $\sigma \in G_{\mathfrak{m}}^r$ (see Equation 8.3.5). Suppose that under the Artin map, the element σ correspond to the class of the ideal $\mathfrak{c}$. For the rest of this chapter we restrict, for our explicit computations, to $\mathfrak{m} = m\mathcal{O}_K$ where $m = 1, 2$. Let

$$B = (B_1, B_2)$$

be a (3×6) complex-valued matrix containing a symplectic basis for the lattice $\Phi(\mathfrak{a})$ with respect to the Riemann form $E_{\Phi,\xi}$. Let $Z = B_2^{-1}B_1 \in \mathcal{H}_3$ be the small period matrix. By Definition 8.3.11, the action of σ on $A(\mathfrak{a},\xi,t)$ yields a principally polarized abelian variety in $\mathrm{Princ}(K,\Phi,\mathfrak{m})$ given by

$$\sigma(A(\Phi,\mathfrak{a},\xi,t)) \cong A(\mathcal{N}_{\Phi^r,\mathfrak{m}}(\mathfrak{b})(\mathfrak{a},\xi,t)),$$

where

$$A(\mathcal{N}_{\Phi^r,\mathfrak{m}}(\mathfrak{b})(\mathfrak{a},\xi,t)) = A(N_{\Phi^r,\mathfrak{m}}(\mathfrak{c})^{-1}\mathfrak{a},\ N(\mathfrak{c})\xi,\ t \pmod{N_{\Phi^r,\mathfrak{m}}(\mathfrak{c})^{-1}\mathfrak{a}}).$$

In a similar manner let

$$C = (C_1, C_2)$$

be the matrix containing a symplectic basis for the lattice $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a})$ with respect to the conjugate Riemann form $E_{\xi'}$ where $\xi' = \Phi, N(\mathfrak{c})\xi$. Let

$$Z' = C_2^{-1}C_1 \in \mathcal{H}_3.$$

We express C in terms of B by taking a matrix M, such that $C = BM^T$. The matrix M has the following properties: It is in $\mathrm{GSp}_6(\mathbb{Q})$, m-integral and invertible $\pmod m$ with inverse $U \in \mathrm{GSp}_6(\mathbb{Z}/m\mathbb{Z})$. We also denote by $\widetilde{U} \in \mathrm{Sp}_6(\mathbb{Z})$ any lift of U. Such a lift can be computed for instance thanks to [56, Theorem VII.21].

Remark 8.5.3. We can deduce the same construction as in Notation 8.5.2 when considering $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$.

To illustrate the construction in Notation 8.5.2, we look at the following example.

Example 8.5.4. Let K be the CM field defined by the polynomial $x^6 + 43x^4 + 451x^2 + 729$ and denote by a a generator for this field. We choose the first CM type given by the implementation [2] and we get that the tuple

$$(\mathfrak{a}, \xi) = \left(\mathcal{O}_K,\ \frac{16}{114939}a^5 + \frac{1313}{229878}a^3 + \frac{5857}{114939}a\right)$$

yields a CM point. We compute the action on this CM point by the ideal

$$\mathfrak{c} = \left(9,\ \frac{1}{48}a^5 + \frac{11}{24}a^3 + \frac{1}{2}a^2 - \frac{155}{48}a + \frac{15}{2}\right)$$

and get a second CM point given by

$$(\mathfrak{a}', \xi') = \left(\left(9,\ \frac{1}{48}a^5 + \frac{11}{24}a^3 + \frac{1}{2}a^2 - \frac{155}{48}a + \frac{15}{2}\right),\ \frac{16}{114939}a^5 + \frac{1313}{229878}a^3 + \frac{5857}{114939}a\right).$$

The code in [2] gives symplectic bases for $(\mathfrak{a}, \xi)$ and $(\mathfrak{a}', \xi')$ and we compute

$$M = \begin{pmatrix} -1 & 1 & -1 & 0 & 1 & 3 \\ 2 & -1 & 0 & -2 & 1 & 4 \\ 2 & 0 & 1 & 2 & 4 & -1 \\ 0 & -1 & -1 & -1 & 3 & -1 \\ 1 & 0 & -1 & 1 & -1 & 1 \\ -1 & -1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

In order to compute class polynomials, we need an explicit description of the computation of Galois conjugate modular invariants. M. Streng gives in [71, Thm. 2.4] an explicit version of Shimura's reciprocity law.

Theorem 8.5.5. *Let $\sigma \in G_{\mathfrak{m}}^r$. Suppose that under the Artin map, the element σ correspond to the class of the ideal $\mathfrak{c}$. Let $Z, Z' \in \mathcal{H}_3$ and the matrix M as in Notation 8.5.2. For any Siegel modular function f of level m with Fourier expansion coefficients in $\mathbb{Q}(\xi_m)$, we have*

$$\sigma(f(Z)) \cong f(Z)^{\mathfrak{c}} = f^U(Z'),$$

where we denote by $f^U(Z') = f(\widetilde{U}.Z')$, for any lift $\widetilde{U} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ of U.

Proof. See [71, Thm. 2.4]. □

Remark 8.5.6. We will use Theorem 8.5.5 to compute the Galois conjugates of the Shioda invariants of a hyperelliptic curve whose period matrix is obtained via the complex multiplication construction.

Corollary 8.5.7. *Let $A(\mathfrak{a},\xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ be isomorphic to a hyperelliptic Jacobian* $\mathrm{Jac}(X)$. *Let $Z \in \mathcal{H}_3$ be its period matrix. Let $\sigma \in G^r_{\mathfrak{m}}$ for $\mathfrak{m} = \mathcal{O}_K$, and suppose that under the Artin map the element σ correspond to the class of the ideal $\mathfrak{c}$. Denote by S_j for $1 \leq j \leq 9$ the Siegel modular function giving the jth absolute Shioda invariant of X in Equation* (8.5.1). *Then*

$$\sigma(S_j) \cong S_j(Z)^{\mathfrak{c}} = S_j(Z'), \tag{8.5.2}$$

where Z' is given by the construction in Notation 8.5.2

Proof. Follows from Theorem 8.5.5. □

We now restrict to the case of the modulus $\mathfrak{m} = 2\mathcal{O}_K$. The following result allows us to compute Galois conjugates Rosenhain invariants of a hyperelliptic curve whose period matrix is obtained via the complex multiplication construction.

Remark 8.5.8. In the paper [17] we chose another normalization (see [17, Equation 2.11]) for a Rosenhain model of a hyperelliptic curve X. It is different from the one in Definition 4.3.4. This is caused by the code in [2]. In the remaining part of this chapter we chose the same normalization (and the index notation, respectively) as in [17, Equation 2.11] give by

$$X : y^2 = x(x-1)\prod_{\ell=1}^{5}(x-\lambda_\ell)$$

and where $\lambda_6 = 0, \lambda_7 = 1$.

Theorem 8.5.9. *Let* $\mathrm{Jac}(X) = \mathbb{C}^3/(Z\mathbb{Z}^3 + \mathbb{Z}^3)$ *be the Jacobian of a marked genus* 3 *hyperelliptic curve X, and let $Z \in \Gamma_6(2)\backslash\mathcal{H}_3$ be its period matrix. Let $\sigma \in G^r_{\mathfrak{m}}$, and suppose that under the Artin map the element σ correspond to the class of the ideal $\mathfrak{c}$. Let $Z' \in \mathcal{H}_3$ obtained as in Notation 8.5.2. We consider η the azygetic system associated to Z and let λ_ℓ for $1 \leq \ell \leq 5$ be the Rosenhain invariants of X in Equation* (4.3.2). *Then for any lift $\widetilde{U} = \begin{pmatrix} \widetilde{A} & \widetilde{B} \\ \widetilde{C} & \widetilde{D} \end{pmatrix} \in \mathrm{Sp}_6(\mathbb{Z})$ of the matrix U with $\delta_0 = \begin{pmatrix} (\widetilde{C}^T\widetilde{D})_0 \\ (\widetilde{A}^T\widetilde{B})_0 \end{pmatrix}$ we have that*

$$\sigma(\lambda_\ell) \cong \lambda_\ell^{\mathfrak{c}} = \exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2) \cdot \zeta_4(\widetilde{U},\eta) \cdot \lambda'_\ell,$$

where

$$\begin{aligned}\zeta_4(\widetilde{U},\eta) = \exp\Big(2\Big(&k(\widetilde{\mathrm{U}},\widetilde{\mathrm{U}}^T(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,\ell\})} - \frac{1}{2}\delta_0)) + k(\widetilde{\mathrm{U}},\widetilde{\mathrm{U}}^T(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,\ell\})} - \frac{1}{2}\delta_0)) \\ &- k(\widetilde{\mathrm{U}},\widetilde{\mathrm{U}}^T(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})} - \frac{1}{2}\delta_0)) - k(\widetilde{\mathrm{U}},\widetilde{\mathrm{U}}^T(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})} - \frac{1}{2}\delta_0))\Big)\Big)\end{aligned}$$

and

$$\lambda'_\ell = \left(\frac{\vartheta[\widetilde{\mathrm{U}}^t\left(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,\ell\})} - \frac{1}{2}\delta_0\right)] \cdot \vartheta[\widetilde{\mathrm{U}}^t\left(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,\ell\})} - \frac{1}{2}\delta_0\right)]}{\vartheta[\widetilde{\mathrm{U}}^t\left(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})} - \frac{1}{2}\delta_0\right)] \cdot \vartheta[\widetilde{\mathrm{U}}^t\left(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})} - \frac{1}{2}\delta_0\right)]}\right)^2 (Z').$$

Proof. Using Theorem 5.5.2 for $\lambda_6 = 0, \lambda_7 = 1$, the coefficients λ_ℓ with $\ell = 1, \dots 5$ can be computed as

$$\lambda_\ell = \exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6,\ell\})] \cdot \vartheta[\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6,\ell\})]}{\vartheta[\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6,7\})] \cdot \vartheta[\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6,7\})]}\right)^2 (Z).$$

For the sake of simplicity let

$$c_1 = \eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6,\ell\})}, \quad c_2 = \eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6,\ell\})}, \quad c_3 = \eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6,7\})}, \quad c_4 = \eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6,7\})}.$$

By using Theorem 8.5.5 we have that

$$\lambda_\ell^{\mathfrak{c}} = \left(\exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[c_1] \cdot \vartheta[c_2]}{\vartheta[c_3] \cdot \vartheta[c_4]}\right)^2 (Z)\right)^{\mathfrak{c}} \tag{8.5.3}$$

$$= \exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2)\left(\left(\frac{\vartheta[c_1] \cdot \vartheta[c_2]}{\vartheta[c_3] \cdot \vartheta[c_4]}\right)^2\right)^U (Z'). \tag{8.5.4}$$

We denote by $c_j' = \widetilde{\mathrm{U}}^T\left(c_j - \frac{1}{2}\delta_0\right)$. By applying the theta transformation formula we get that

$$\vartheta\left[c_j\right]^U (Z') = \vartheta\left[\widetilde{\mathrm{U}}.c_j'\right]\left(\widetilde{\mathrm{U}}.Z'\right) = \zeta\left(\widetilde{\mathrm{U}}\right)\exp\left(k(\widetilde{\mathrm{U}}, c_j')\right)\sqrt{\det(\widetilde{\mathrm{C}}Z' + \widetilde{\mathrm{D}})}\ \vartheta\left[c_j'\right](Z').$$

Hence Equation (8.5.3) becomes to

$$\lambda_l^{\mathfrak{c}} = \exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2)\exp\left(2(k(\widetilde{\mathrm{U}}, c_1') + k(\widetilde{\mathrm{U}}, c_2') - k(\widetilde{\mathrm{U}}, c_3') - k(\widetilde{\mathrm{U}}, c_4'))\right) \cdot \left(\frac{\vartheta[c_1'] \cdot \vartheta[c_2']}{\vartheta[c_3'] \cdot \vartheta[c_4']}\right)^2 (Z').$$

After a straightforward computation we get that

$$\zeta_4(\widetilde{\mathrm{U}}, \eta) = \exp(2(k(\widetilde{\mathrm{U}}, c_1') + k(\widetilde{\mathrm{U}}, c_2') - k(\widetilde{\mathrm{U}}, c_3') - k(\widetilde{\mathrm{U}}, c_4')))^2$$

is a fourth root of unity. □

Corollary 8.5.10. *Let $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathcal{O}_K}(\Phi)$ be isomorphic to the Jacobian of a marked hyperelliptic curve X. Let $Z \in \Gamma_6(2)\backslash\mathcal{H}_3$ be the small period matrix for $A(\mathfrak{a}, \xi)$ and η be an azygetic system associated to Z. Let $\sigma \in G_{\mathfrak{m}}^r$ and suppose that under the Artin map, the element σ correspond to the class of the ideal $\mathfrak{c}$. There exist matrices Z', M and $\widetilde{\mathrm{U}}$ as in Notation 8.5.2, such that*

$$\eta' = \widetilde{\mathrm{U}}^T \eta$$

is an azygetic system associated to the small period matrix Z' of the marked hyperelliptic curve with Rosenhain invariants $\lambda_\ell^{\mathfrak{c}}$ for $l = 3, \dots, 7$.

Proof. We first note that we can choose C and the period matrix Z' in Notation 8.5.2 such that $\widetilde{\mathrm{U}} \in \Gamma_6(2)$. Indeed, if this is not the case then define

$$C' = BM^T\widetilde{\mathrm{U}}^T = BM'^T$$

with $M' = \widetilde{\mathrm{U}}M \in \mathrm{GSp}_6(\mathbb{Q})$. Then C' is still a symplectic basis for of $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a})$ with respect to E_ξ' where $\xi' = N(\mathfrak{c})\xi$. Let $\overline{M} \in \mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ the reduction of $M \pmod 2$. We get that

$$\overline{M'} = \overline{\widetilde{\mathrm{U}}M} = U\overline{M} = I_6.$$

Then $(\overline{M'})^{-1} = I_6$ in $\mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$. Therefore, by letting $C = C'$ and Z' the period matrix obtained from this new symplectic basis, we ensure that $\widetilde{\mathrm{U}} \in \Gamma_6(2)$.

Recall that the action described in Definition (8.3.11) yields an isogeny between $A(\Phi, \mathfrak{a}, \xi)$ and its Galois conjugate $\sigma(A(\Phi, \mathfrak{a}, \xi))$ which is given by

$$\begin{aligned} I_{\mathfrak{c}} : \mathbb{C}^3/\Phi(\mathfrak{a}) &\longrightarrow \mathbb{C}^3/\Phi(N_{\Phi^r,\mathfrak{m}}(\mathfrak{c})^{-1}\mathfrak{a}) \\ x &\mapsto x. \end{aligned}$$

For simplicity, we will work $I_{\mathfrak{c}}$ as an isogeny between the non-normalized tori, i.e.

$$I_{\mathfrak{c}} : \mathbb{C}^3/(B_1\mathbb{Z}^3 + B_2\mathbb{Z}^3) \to \mathbb{C}^3/(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3).$$

We consider the image of the fixed points $B_1(\eta_i)_1 + B_2(\eta_i)_2 \pmod{(B_1\mathbb{Z}^3 + B_2\mathbb{Z}^3)}$ via $I_{\mathfrak{c}}$. We compute η_i' such that

$$B_1(\eta_i)_1 + B_2(\eta_i)_2 = C_1(\eta_i')_1 + C_2(\eta_i')_2 \pmod{(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3)}. \tag{8.5.5}$$

By writing $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and using that $C = BM^T$, the 2-torsion point in Equation 8.5.5 writes as

$$(B_1a^t + B_2b^t)(\eta_i')_1 + (B_1c^t + B_2d^t)(\eta_i')_2 \equiv B_1(a^t(\eta_i')_1 + c^t(\eta_i')_2) + B_2(b^t(\eta_i')_1 + d^t(\eta_i')_2) \pmod{(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3)}.$$

Hence $\bar{\eta}_i = \bar{M}^T\bar{\eta}_i'$. Then $\eta_i' = \widetilde{\mathrm{U}}^T\,\eta_i$ is in fact an azygetic basis associated to Z' (see [61, Definition 1.4.12]). The first two properties in [61, Definition 1.4.12] are clear. The third property in [61, Definition 1.4.12] follows by applying [49, Prop. 13.2(b)] for the isogeny $I_{\mathfrak{c}}$, which has degree prime to 2.

To show that η' is associated to Z', we will use the Vanishing Criterion. We choose an even theta characteristic $u \in (1/2)\mathbb{Z}^6$ such that $\vartheta[u](Z) \neq 0$ and $\vartheta[u](Z') \neq 0$ and apply once more Shimura's reciprocity law [71] on the quotients of the type $\left(\frac{\vartheta[v](Z)}{\vartheta[u](Z)}\right)^2$ with $v \in (1/2)\mathbb{Z}^6$ even. We deduce that the unique even theta constant vanishing Z' is $\vartheta[\eta_{\mathcal{U}_{\eta'}}]$ (since $\eta_{\mathcal{U}_{\eta'}} = \eta_{\mathcal{U}_\eta}$).

Finally, by applying Theorem 8.5.9, we get that

$$\lambda_\ell^{\mathfrak{c}} = \exp(4\pi i(\eta_\ell + \eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[c_1]\cdot\vartheta[c_2]}{\vartheta[c_3]\cdot\vartheta[c_4]}\right)^2(M'.Z), \tag{8.5.6}$$

for $\ell = 1, \ldots, 5$. Hence the right-hand side expressions in Equation (8.5.6) are the Rosenhain invariants of a marked genus 3 hyperelliptic curve. □

Remark 8.5.11. From a computational point view, if we simply aim at computing the Galois conjugates of the Rosenhain invariants and deriving class field equations, one can choose between the approach in Theorem 8.5.9 or the one in Corollary 8.5.10. One can pick any period matrix for the Galois conjugate $\sigma(A(\Phi, \mathfrak{a}, \xi, t))$ and use the formula in Theorem 8.5.9, or construct the period matrix Z' and its associated azygetic system as explained in the proof of the Corollary 8.5.10 and compute the resulting Rosenhain invariants via Formula (5.5.1).

Definition 8.5.12. We define the *Shioda* and the *Rosenhain class polynomials* to be monic polynomials given by

$$H^R_{K^r,i}(t) = \prod_{\sigma\in G^r_{\mathfrak{m}}}(t - \lambda_i^\sigma), \qquad H^S_{K^r,j}(t) = \prod_{\sigma\in G^r_{\mathfrak{m}}}(t - \mathrm{Shi}_j^\sigma), \tag{8.5.7}$$

where $\mathfrak{m} = 2\mathcal{O}_K$ in the first case, and $\mathfrak{m} = \mathcal{O}_K$ in the second.

Remark 8.5.13. Algorithm 3 in my paper [17] gives all the steps of our computation of a list of approximations for the Galois conjugates of the Rosenhain invariants, that we used to get the polynomials $H^R_{K^r,i}$ in Equation (8.5.7). The algorithm for computing the Shioda class polynomial $H^S_{K^r,j}$ is similar and relies on the computation of the Siegel modular functions S_j in Theorem 8.5.2. In applications, for $i, j \geq 2$, it is easier to use the *Hecke representation* as introduced by Gaudry *et al* [24], given by

$$\hat{H}^R_{K^r,i}(t) = \sum_{\sigma} \lambda_i^{\sigma} \prod_{\sigma' \neq \sigma} (t - \lambda_1^{\sigma'}), \quad \hat{H}^S_{K^r,j}(t) = \sum_{\sigma} \mathrm{Shi}_j^{\sigma} \prod_{\sigma' \neq \sigma} (t - \mathrm{Shi}_1^{\sigma'}), \tag{8.5.8}$$

where $\sigma, \sigma' \in \sigma \in G^r_{\mathfrak{m}}$.

We end this chapter by presinting the following practical experiments: Let K be the CM field defined by the polynomial $x^6 + 43x^4 + 451x^2 + 729$. Since the field contains i, all principally polarized abelian variety with CM by K are hyperelliptic. For one of its primitive CM types, our implementation yields the reflex field as the field of equation $x^6 + 1012x^4 + 262048x^2 + 3968064$. The subgroup $\mathcal{N}_{\Phi^r,\mathfrak{m}}(Cl_m(K^r))$, for $\mathfrak{m} = (1), (2)$, has three elements, which means that the class polynomials $H^R_{K^r,i}$, $H^S_{K^r,j}$ in Definition 8.5.12 have degree 3.

For most computations on the Rosenhains 500 bits of precision were enough, whereas for the Shiodas we used 5000 bits of precision. Indeed, the Siegel modular forms appearing in the expressions of the Shiodas have much larger weight, which results into much more precision needed when computing with the Shiodas. To compute the Shiodas, we first computed the Rosenhain coefficients and got an approximation of the equation of the curve, and afterwards computed the Shiodas from this equation. All computations were performed on a single core of a Intel Core *i7-4790 CPU 3.60GHz* and took approximatively 5 minutes at 500 bits of precision and less than 2 hours for 5000 bits. Most time is spent on the theta constants computation, which is performed using the naive implementation in [2]. To compute the coefficients of the class polynomials $H^R_{K^r,i}$ and $H^S_{K^r,i}$ as algebraic integers, we use the algebraic dependence testing algorithm [13], implemented in *PARI/GP* by the function *algdep*. This algorithm gives us a conjectured minimal polynomial for each coefficient of the class polynomials.

Since $\mathrm{Princ}(K, \Phi)$ is stable under complex conjugation, it can be shown by using similar arguments as in [69, Section III.2] that the coefficients of the Shioda class polynomials are in fact in the field K^r_0, which the real multiplication subfield of K^r. We conjecture that a similar result holds for the Rosenhain class polynomials. For the chosen example, K and K^r are equal, so we take K^r_0 to be the field given by the equation $x^3 - 43x^2 + 451x^2 - 729$ and we denote by α a generator for this field. Tables 8.1 and 8.2 give the coefficients of Rosenhain and Shioda class polynomials, respectively. Table 8.2 gives the Shioda class polynomials for the first Shioda invariant, and the full example is given in [17]. As expected, the polynomials for the Shiodas have larger coefficients, which is due again to the shape of the modular forms in their expression.

In order to heuristically check the correctness of these computations, we use a well known approach in the literature which consists in choosing a prime number p such that the abelian varieties with CM by $\mathcal{O}_K$ have good reduction, compute the roots of class polynomials $\pmod p$ and check that the Jacobians of the curves obtained in this way have the right number of points (see for instance [1] for details).

Table 8.1: Coefficients of polynomials $H^R_{K^r,i}$ for the field of equation $x^6 + 43x^4 + 451x^2 + 729$.

pol.	t^3	t^2	t	1
$H_{K^r,1}$	1	$1/16\alpha^2 - 19/8\alpha + 181/16$	$1/48\alpha^2 - 49/24\alpha + 875/16$	$1/6\alpha^2 - 16/3\alpha + 19/2$
$\hat{H}_{K^r,2}$	1	$-7/144\alpha^2 + 149/72\alpha - 3331/144$	$3/16\alpha^2 - 65/8\alpha + 1295/16$	$-11/48\alpha^2 + 239/24\alpha - 1521/16$
$\hat{H}_{K^r,3}$	1	$-1/16\alpha^2 + 19/8\alpha - 277/16$	$13/48\alpha^2 - 277/24\alpha + 1791/16$	$-11/24\alpha^2 + 227/12\alpha - 1377/8$
$\hat{H}_{K^r,4}$	1	$7/144\alpha^2 - 149/72\alpha + 2467/144$	$-1/144\alpha^2 + 11/72\alpha + 59/144$	$7/144\alpha^2 - 143/72\alpha + 2551/144$
$\hat{H}_{K^r,5}$	1	-6	12	-8

Table 8.2: Coefficients of the polynomial $H^S_{K^r,1}$ for the field of equation $x^6 + 43x^4 + 451x^2 + 729$.

	coeff.
t^3	1
t^2	$\frac{-150499810389818442869289571906287699141437 5}{1106030051237012236054152188167439553303783103}\alpha^2 + \frac{576021917913534128335758291802230916493406 30}{1106030051237012236054152188167439553303783103}\alpha - \frac{182610135152410817952949427128063513960980968701}{247750731477090740876130090149506459940047415072}$
t	$\frac{271537582048409045934259507591982005281201875}{867127560169817593066455315523272609790165952752}\alpha^2 - \frac{171559472382027900944379509650789590018494955 35}{1300691340254726389599682973284908914685248929128}\alpha + \frac{189221715181445169536136728129202262948355551 1744769}{116541944086823484508131594406327838755798304049 8688}$
1	$\frac{-4970183343949242284467452261947818401413441768 75}{244738082582329317467076348253288461387176438504724 48}\alpha^2 + \frac{114442556401918903153013990970527856060706070221 15}{122369041291164658733538174126644230693588219252362 24}\alpha - \frac{191953650625925394207069308222518633622840220848155861}{164463991495325301337875306026209846052182566675174850 56}$

9 Linear Algebra Data of Supersingular Abelian Varieties

Previously in this thesis we considered polarized abelian varieties of dimension 3 over $\mathbb{C}$ with CM. In this chapter we choose another setup. We consider principally polarized abelian varieties of dimension g over algebraically closed fields k of $\mathrm{char}(k) = p > 0$, given by pairs

$$(A, \eta).$$

More precisely, we consider so-called *polarized flag type quotients (pftq's)* of dimension g over k. These are given by a sequence (Y_i, η_i) of polarized abelian varieties over k together with isogenies $\rho_i : Y_i \to Y_{i-1}$ for $1 \leq i \leq g-1$, where $Y_{g-1} = E^g$ for a supersingular elliptic curve E over $k \supset \mathbb{F}_p$, ending on a principally polarized abelian variety (Y_0, η_0) such that

$$(Y_0 = Y, \eta_0) \cong (A, \eta).$$

For a given pair

$$(g, p),$$

with positive integers $g \geq 2$, prime numbers $p \geq 2$, *and* for any pair $(Y_{g-1} = E^g, \eta_{g-1})$, where E is supersingular elliptic curve over $k \supset \mathbb{F}_p$ *and* where η_{g-1} "runs" over all equivalence classes of polarizations on Y_{g-1}, the moduli problem is that of parametrizing pairs (A, η), where

$$(A, \eta) \cong (Y_0 = Y, \eta_0).$$

The goal of this chapter is to give an explicit description of the pftq's of abelian varieties of dimension 2 and 3 over k with respect to polarizations, in terms of the linear-algebraic data. This data is given by the so-called *Dieudonné modules*.

To solve problems involving lifts from characteristic $p > 0$ to characteristic 0, there are techniques for handling p-torsion points phenomena in characteristic p. The main tools for this purpose are the so-called *Dieudonné* theory and the theory of *p-divisible groups*. We consider in this chapter the *contravariant* version of Dieudonné theory. There is an anti-equivalence between p-divisible groups of height h over k and Dieudnné modules of finite length over the ring of Witt vectors $W(k)$. The construction of pftq's is given by projections $\rho_i : Y_i \to Y_{i-1}$ where $Y_{i-1} \cong \ker(\rho_i)$ where $\ker(\rho_i)$ is a finite commutative group scheme over k of local-local type (see Definition 9.2.1). In this chapter we follow the discussion in [46] and [11, Chapter 3 and Appendix B.3].

9.1 Definitions

For the rest of this chapter we denote by k an arbitrary field of $\mathrm{char}(k) = p > 0$, that we assume to be algebraically closed. We fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ such that the relative Frobenius F satisfies the equation

$$F^2 = -p. \tag{9.1.1}$$

Remark 9.1.1. It is known that the condition in Equation (9.1.1) is part of a formula for elliptic curves given by

$$F^2 - aF + q = 0 \quad \text{in } \mathrm{End}(E),$$

where $a = q + 1 - \#E(\mathbb{F}_q)$ for $q = p^n$ and positive integers n. In the case where $n = 1$ and E supersingular, then $a = 0$. In other words, any supersingular curve E over $\mathbb{F}_p$ where $p \geq 5$ has $(p+1)$ $\mathbb{F}_p$-rational points on $E(\mathbb{F}_p)$ (see [65, Exercise 5.15]). For the existence of E over $\mathbb{F}_p$, see [46, page 11].

We begin this chapter by recalling basic definitions and properties of supersingular elliptic curves. It is well known that the number of isomorphism classes of supersingular elliptic curves over k is roughly $p/12$, and that any two supersingular elliptic curves over $k \supset \mathbb{F}_p$ are isogenous, see [46, page 11].

Definition 9.1.2. An elliptic curve E over k is called *supersingular* if its endomorphism ring

$$\mathcal{O} = \mathrm{End}(E) \tag{9.1.2}$$

is a maximal order in a *quaternion* $\mathbb{Q}$*-algebra*

$$\mathcal{B} = \mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}_{p,\infty}, \tag{9.1.3}$$

ramified only at (p, ∞). See [46, Chapter 1].

Definition 9.1.3. An abelian variety A of dimension g over k is called *supersingular* or *superspecial* respectively, if

$$A \sim E^g, \text{ or } A \cong E^g$$

respectively, where E is a supersingular elliptic curve over k and where $\sim$ denotes isogeny equivalence.

Remark 9.1.4. There is an equivalent characterization of superspecial abelian varieties by their a-numbers (for the definition, see B.1.3), related to their p-divisible groups. See [46, Page 14].

Definition 9.1.5. An abelian variety A of dimension g over k is called *superspecial* if $a(A) = \dim(A)$. A is called *supergeneral* if A is supersingular and $a(A) = 1$. See [46, page 13-14].

As a generalization for the genus-1 case, we have the following classification of supersingular abelian varieties by their endomorphism rings.[1]

Theorem 9.1.6. *An abelian variety A of dimension g is supersingular if and only if its endomorphism ring is of rank-$(4g^2)$ over $\mathbb{Z}$.*

Proof. See [46]. □

[1] As mentioned in the introduction of this chapter, we consider algebraically closed fields k of $\mathrm{char}(k) = p > 0$. We consider their morphisms to be defined over k.

9.2 Polarized flaq type quotients

In order to understand the linear-algebraic data to supersingular polarized abelian varieties of dimension g over algebraically closed fields k of $\mathrm{char}(k) = p > 0$, we introduce in this section the concept of the so-called *polarized flag type quotients*. We follow the discussion in [46, Chapter 3]. The authors in [46] described a method to construct a sequence of inseparable isogenies with properties described by the following definition. By their construction they ensure, that the polarization of the final abelian variety in this chain is principal, and that the a-number of the target abelian variety has a value between 1 and g.

Definition 9.2.1. A *polarized flag type quotient (pftq)* with respect to a polarization

$$\eta : E^g = Y_{g-1} \to Y_{g-1}^t$$

is a sequence of isogenies ρ_i of abelian varieties Y_i of dimension g over k given by

$$E^g = Y_{g-1} \xrightarrow{\rho_{g-1}} Y_{g-2} \xrightarrow{\rho_{g-2}} \ldots \longrightarrow Y_1 \xrightarrow{\rho_1} Y_0 = Y, \tag{9.2.1}$$

satisfying the following conditions:

(i) $\ker(\rho_i) \cong (\alpha_p)^i$ for $1 \leq i \leq g-1$,

(ii) $\ker(\eta) = E^g[F^{g-1}]$. Here F is the relative Frobenius.

(iii) There are polarizations η_i on Y_i for $0 \leq i \leq g-1$ that make the following diagram commute:

$$\begin{array}{ccccccccc} Y_{g-1} & \xrightarrow{\rho_{g-1}} & Y_{g-2} & \xrightarrow{\rho_{g-2}} & \cdots & \longrightarrow & Y_1 & \xrightarrow{\rho_1} & Y_0 \\ \downarrow{\scriptstyle \eta_{g-1}} & & \downarrow{\scriptstyle \eta_{g-2}} & & & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_0} \\ Y_{g-1}^t & \xleftarrow[\rho_{g-1}^t]{} & Y_{g-2}^t & \xleftarrow[\rho_{g-2}^t]{} & \cdots & \longleftarrow & Y_1^t & \xleftarrow[\rho_0^t]{} & Y_0^t \end{array} \tag{9.2.2}$$

(iv) $\ker(\eta_i) \subset Y_i[F^i]$, for $0 \leq i \leq g-1$.

(v) The polarization $\eta_{g-1} = \eta$, and η_0 is an isomorphism.

See [46, Chapter 3].

Remark 9.2.2. In this thesis we do *not* consider the property of pftq's to be *rigid* (see [46, Definition 3.2]). In dimension 2 this is automatically true, see [46, 9.2]. In a more general context, the authors in [46] define isomorphism classes of pftq's over schemes S, and isomorphism classes of *rigid* pftq's over S as sub-schemes of the former. The former are for $g \leq 3$ as quasi-projective schemes *non-singular*, and where the latter are *non-singular* for arbitrary g. Since in this thesis we restrict to the cases where $g = 2, 3$ and since in this case the corresponding schemes are non-singular, we will not consider the rigidity condition of pftq's.

9.3 The Dieudonné-Cartier-Oda-classification

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. One of the main structures in the deformation theory of abelian varieties in characteristic $p > 0$ is the ring of p-adic Witt vectors $W(k)$ over k. As a truncated (additive) group it contains

elements of finite length. It is a finite commutative group scheme over k, and every finite commutative group scheme over k of local-local type can be embedded into some quotient group schemes of it (see Remark 9.3.1). Given an abelian variety in characteristic $p > 0$, one way to handle its p-torsion phenomena is to consider the relationship between the p-divisible group of A and modules over the so-called *Dieudonné* ring. It is defined over the ring $W(k)$ (see Definition 9.3.4). The main purpose of this section is to describe anti-equivalence of categories between the p-divisible groups of height h over k (or finite commutative group schemes over k of local-local type, respectively) of A and Dieudonné modules which are free over $W(k)$ of rank h (or Dieudonné modules of finite $W(k)$-length, with nilpotent (semi-)linear operators) (see Theorems 9.3.6 and 9.3.7).

We begin this section by considering the ring of of infinite p-adic *Witt vectors*

$$W(k) := \prod_{n\geq 0} \mathbb{A}^1_k$$

with entries in k, and with addition and multiplication given by

$$\underline{a} + \underline{b} = (\varphi_0, \varphi_1, \ldots), \qquad \underline{ab} = (\psi_0, \psi_1, \ldots)$$

for $\underline{a} = (a_0, a_1, \ldots)$, $\underline{b} = (b_0, b_1, \ldots,) \in W(k)$ and where φ_i, ψ_i are polynomials in $\mathbb{Z}[x_0, \ldots, x_i, y_0, \ldots, y_i]$ for all i. There are two operators on $W(k)$ called *Frobenius* and *Verschiebung*, given by

$$\begin{aligned} \sigma : W(k) &\to W(k) \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_0^p, a_1^p, a_2^p, \ldots), \end{aligned}$$

and

$$\begin{aligned} \mu : W(k) &\to W(k) \\ (a_0, a_1, a_2, \ldots) &\mapsto (0, a_0, a_1, \ldots), \end{aligned}$$

satisfying the relations $\mu \circ \sigma = \sigma \circ \mu = p$. In positive characteristic $W(k)$ is a complete discrete valuation ring with uniformizer p and residue field $W(k)/(p) \cong k$, see [60, Theorem 21.2].

Remark 9.3.1. For any integer $n \geq 1$, we consider *truncated* Witt vectors over k of length n together with operation given by addition. It is given by

$$W_n(k) = \prod_{m=0}^{n-1} \mathbb{A}^1_k.$$

It is an (additive) group scheme over k, and as a finite commutative group scheme over k isomorphic to $W(k)/V^n W(k)$. See [60, Lecture 9]

Remark 9.3.2. For any integer $m \geq 1$ the kernel of the m-iterated Frobenius F^m in $W_n(k)$ is given by

$$W_n^m(k) = \ker\Big(F^m : W_n(k) \to W_n(k);\ (a_0, \ldots, a_{n-1}) \mapsto \Big(a_o^{p^m}, \ldots, a_{n-1}^{p^m}\Big) = (0, \ldots, 0)\Big). \tag{9.3.1}$$

One can show that every finite commutative group scheme over k of *local-local type* can be embedded into some $(W_n^m(k))^{\oplus_s}$ for some positive numbers n, m, s see [60, Proposition 22.5].

Example 9.3.3. By construction $W_1^m(k) \cong \alpha_{p^m}$ for all $m \geq 1$.

We can define the main structure in this chapter.

Definition 9.3.4. The *Dieudonné ring* $\mathcal{D}_k = W(k)[F, V]$ is a non commutative ring over $W(k)$ where F and V are two indeterminates subject to the relations

$$F \cdot w = \sigma(w) \cdot F, \qquad V \cdot \sigma(w) = w \cdot V, \qquad F \circ V = V \circ F = p$$

for $w \in W(k)$ and where $w \mapsto \sigma(w)$ is the Frobenius automorphism of $W(k)$ given by

$$w = (w_0, w_1, w_2, \ldots) \mapsto \sigma(w) = (w_0^p, w_1^p, w_2^p, \ldots).$$

See [46, Chapter 5].

Definition 9.3.5. A *Dieudonné module* over $W(k)$ is a left $\mathcal{D}_k$-module which is finitely generated as a $W(k)$-module.

We can state the two main theorems of this chapter.

Theorem 9.3.6 (Dieudonné-Cartier-Oda)**.** *The functor*

$$\begin{aligned} M : \mathbb{G} &\xrightarrow{\sim} \mathscr{M} \\ G &\longmapsto M(G) = \varinjlim_{m,n} \mathrm{Hom}(G, W_n^m(k)) \end{aligned}$$

defines an anti-equivalence between the category $\mathbb{G}$ *of finite commutative group schemes over* k *of local-local type, to the category* $\mathscr{M}$ *of semisimple left* $\mathcal{D}_k$*-modules of finite* $W(k)$*-length, with nilpotent* F *and* V*, taking a group scheme* G *of order* p^n *to a module* $M(G)$ *of* $W(k)$*-length* n*.*

Proof. See [60, Theorem 23.2]. □

Theorem 9.3.7. *If* $G = (G_n)_{n \in \mathbb{N}}$ *is a* p*-divisible group of height* h*, then*

$$M(G) = \varprojlim M(G_n)$$

is a left $\mathcal{D}_k$*-module which is* $W(k)$*-free of rank-*h*. This gives an anti-equivalence of categories between* p*-divisible groups of height* h *over* k *and left* $\mathcal{D}_k$*-module which are* $W(k)$*-free of rank-*h*.*

Proof. See [46, page 41]. □

Proposition 9.3.8. *If* E *is a supersingular elliptic curve over* $k \supset \mathbb{F}_p$*, then its Dieudonné module* M_E *is as a left* $\mathcal{D}_k$*-module isomorphic to*

$$M_E \cong \mathcal{D}_k/(F + V)\mathcal{D}_k. \tag{9.3.2}$$

*It is free and or rank-*2 *over* $W(k)$*. See [46, Chapter 5.6].*

Remark 9.3.9. There are *two* different ways to describe Dieudonné modules over $W(k)$. First, as left $\mathcal{D}_k$-modules as in Definition 9.3.5, and second as $W(k)$-modules M, equipped with a σ-linear map $F : M \to M$ and a σ^{-1}-linear map $V : M \to M$, where σ is the Frobenius automorphism of $W(k)$.

Remark 9.3.10. If E is a supersingular elliptic curve over $k \supset \mathbb{F}_p$, then as a finite commutative group scheme over k,

$$M(E[p]) \cong \frac{\mathcal{D}_k}{(F+V)\mathcal{D}_k} \cong \frac{M(W_2^2(k))}{(F+V)M(W_2^2(k))},$$

whereby the first consideration is as a left $\mathcal{D}_k$-module, the second as a $W(k)$-module. See Proposition 9.5.1.

Definition 9.3.11. For any integer n, we define the *Frobenius twist* for modules M over $W(k)$ by

$$M^{(n)} := W(k) \otimes_{(W(k),\sigma^n)} M,$$

where the $W(k)$-module structure on $M^{(n)}$ is given by $w \cdot m = w^{\sigma^{-n}} \cdot m$ for all $w \in W(k)$ and $m \in M$.

Proposition 9.3.12. *As abelian groups $M^{(n)} \xrightarrow{\sim} M$ via the map*

$$1 \otimes m \mapsto m.$$

for $m \in M$.

Proof. See [11, B.3.2.1]. □

Proposition 9.3.13. *For any p-divisible group or any finite commutative group scheme over k of local-local type with associated relative Frobenius-and Verschiebung morphisms, the functor M in Theorem 9.3.6 gives rise to a datum*

$$(M, F : M^{(1)} \to M,\ V : M \to M^{(1)})$$

which satisfies the relations $V \circ F = p \cdot \mathrm{id}_{M^{(1)}}$, $F \circ V = p \cdot \mathrm{id}_M$. For any $w \in W(k)$ and $m \in M$ we have $w^\sigma \otimes m = 1 \otimes wm$ in $M^{(1)}$.

Proof. See [11, B.3]. □

9.4 Polarized flag type quotients of supersingular Dieudonné modules

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. Let (A, η) be a polarized supersingular abelian variety of dimension g over k. By the discussion above, there exists a triple (g, p, E), where $g \geq 2$ is a positive integer, where $p \geq 2$ is a prime number and where E is a supersingular elliptic curve over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$, and an pftq of dimension g over k to (g, p, E) ending on a principally polarized abelian variety (Y_0, η_0), such that $(Y_0, \eta_0) \cong (E, \eta)$. Then, for any p-divisible group $A[p^\infty]$ over k to A, there exists free left $\mathcal{D}_k$-modules

$$M \cong M(A[p^\infty]) \tag{9.4.1}$$

of rank $2g$ over $W(k)$ representing these groups up to isomorphism. (The same is true after replacing p-divisible groups by finite commutative group scheme over k of local-local type, and left $\mathcal{D}_k$-modules of rank $2g$ over $W(k)$ by finitely generated Dieudonné modules with

nilpotent F and V). In this chapter we introduce the theory of the so-called *polarized flag type quotients (pftq's)* of Dieudonné modules over the ring $W(k)$. There is an anti-equivalence between the category of pftq's over k (see Definition 9.2.1), which is uniquely determined up to isomorphism by the polarization η_{g-1} on $Y_{g-1} = E^g$, to the category of pftq's of Dieudonné modules of genus g over $W(k)$ (see Proposition 9.4.9). In this section we describe the following: We define supersingular, superspecial or supergeneral Dieudonné modules, depending on their underlying abelian varieties. Then, we introduce the quasi-polarization on the dual Dieudonné modules.[2] Based on their anti-equivalence between the categories in Proposition 9.4.9, the authors in [46] defined *polarized flag type quotient* of Dieudonné modules of genus g over $W(k)$. By their construction, the authors in [46] force an isomorphism between Dieudonné modules representing the principal polarization on the abelian variety Y_0. In other words if we denote by $(M_0, M_{\eta_0}) = (M(Y_0), M(\eta_0))$ the Dieudonné modules to the pair (Y_0, η_0), then $M_{\eta_0} : M_0^t \to M_0$ is an isomorphism. We follow in this section [46, Chapter 6].

We begin this section with the following definition.

Definition 9.4.1. A Dieudonné module M of genus g over $W(k)$ is called *supersingular*, *superspecial* or *supergeneral*, if M is of the form as in Equation (9.4.1) for some supersingular, superspecial or supergeneral abelian varieties A of dimension g over k (see Definition 9.1.3).

Remark 9.4.2. By the Dieudonné-Manin classification in Theorem 9.3.6, the category $\mathscr{M}$ is semisimple. In other words, any supersingular Dieudonné module M of genus $g \geq 1$ has a decomposition as a direct sum given by

$$M \cong M_{E^g} \cong (M_E)^{\otimes g} \tag{9.4.2}$$

with M_E as in Equation (9.3.2).

Definition 9.4.3. Let A be an abelian variety of dimension g over k. Let $M = M(A[p^\infty])$ be the Dieudonné module to A of rank $2g$ over $W(k)$. The *dual Dieudonné module* of M is given by

$$M^t = \mathrm{Hom}_{W(k)}(M, W(k)).$$

It is free of rank-$2g$ over $W(k)$, and $M^t \cong M(A^t[p^\infty])$. As a Dieudonné module, M^t has a structure given by

$$(Fn)(m) = n(Vm)^\sigma, \qquad (Vn)(m) = n(Fm)^{\sigma^{-1}} \tag{9.4.3}$$

for $n \in M^t$ and $m \in M$. See [46, Chapter 5.9].

Any polarization $\eta : A \to A^t$ induces an homomorphism between the associated p-divisible groups of A and the its dual abelian variety A^t. By contravariant Dieudonné Theory, η induces a so-called quasi-polarization on the corresponding Dieudonné module which we define below.

Definition 9.4.4. Let M be a supersingular Dieudonné module of genus g over $W(k)$. A *quasi-polarization on M* is a non-degenerate alternating bilinear-form

$$\langle , \rangle : M^t \times M^t \to W(k)$$

such that $\langle F(x), y\rangle = \langle x, V(y)\rangle^\sigma$ for all $x, y \in M^t$. A quasi-polarization is called *principal* if it is a perfect pairing.

[2] The concept of attaching a quasi-polarization on the dual Dieudonné module is based on the contravariant version of Dieudonné theory.

Definition 9.4.5. A *polarized flag type quotient (pftq)* of Dieudonné modules of genus g over $W(k)$ corresponds to a filtration of quasi-polarized Dieudonné modules

$$M_{g-1} \supset \ldots \supset M_0$$

with the following properties:

(i) $M_{g-1} \cong \left(\frac{\mathcal{D}_k}{(F+V)\mathcal{D}_k}\right)^{\oplus_g}$ and $M_{g-1}^t = F^{g-1}M_{g-1}$.

(ii) $(F,V)M_i \subset M_{i-1}$ and $\dim_k\left(\frac{M_i}{M_{i-1}}\right) = \text{i}$ for all $i = 1,\ldots,g-1$.

(iii) $F^{i-j}V^j M_i \subset M_i^t$ for all $i = 1,\ldots,g-1$ and $j = 0,\ldots,\lfloor i/2 \rfloor$.

(iv) $M_i = M_0 + F^{g-1-i}M_{g-1}$ for all $i = 1,\ldots,g-1$.

Remark 9.4.6. As a Dieudonné module, M_{g-1} is either *decomposable* or *indecomposable*. This condition is related to conditions on the quasi-polarization on M_{g-1}. We will consider this separately for the cases $g = 2,3$ in the next sections. See [46, Chapter 6].

Lemma 9.4.7. *For any Dieudonné modules M_i in Definition 9.4.5, the quotients*

$$\frac{M_i}{M_{i-1}}$$

are k-vector spaces.

Proof. By part (ii) of the Definition 9.4.5 , the quotients $\frac{M_i}{M_{i-1}}$ have a W(k)-module structure where $p = F \circ V$ acts as 0 on $\frac{M_i}{M_{i-1}}$. Since $k = W(k)/(p)$, there is an action of k on the quotients $\frac{M_i}{M_{i-1}}$, from which we conclude that the latter are k-vector spaces. □

Proposition 9.4.8. *Let A be a supersingular abelian variety of dimension g over k and let $M_{g-1} = M(A)$ be its Dieudonné module. For any submodule M_i in the filtration from Defintion 9.4.5, we have*

$$\dim_k\left(\frac{M_i}{FM_i}\right) = g$$

for $0 \leq i \leq g-1$.

Proof. Follows from [23, Proposition 4.4]. □

We can state the Main Result of this section.

Proposition 9.4.9. *There is an anti-equivalence between the category of polarized flag type quotients over k (see Definition 9.2.1), to the category of polarized flag type quotients of Dieudonné modules of genus g over $W(k)$ (see Definition 9.4.5).*

Proof. See [46, Chapter 7.4]. □

Definition 9.4.10. We define the *a-number* of a Dieudonné module M of genus g over $W(k)$ as the dimension of the k-vector space

$$a(M) = \dim_k\left(\frac{M}{(F,V)M}\right).$$

See [46, page 30].

Remark 9.4.11. Since M is the Dieudonné module of the p-divisible group of an abelian variety A of dimension g, it is known that $a(M) \leq g$.

We will identify in the next two paragraphs pftq's of Dieudonné modules of genus 2 and 3 over k. For these identifications we have the following correspondence theorem for PID's. A proof of this can be found in most linear algebra books, e.g. [62, Theorem 4.7].

Lemma 9.4.12. *Let M be an R-module, and let S be a submodule of M. Then there is a bijection between submodules T of M that contains S and quotient modules $T/S \subseteq M/S$.*

9.5 Linear algebra data of supersingular elliptic curves

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. For the rest of this section we fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$. In order to understand the linear-algebraic data to polarized abelian varieties of dimension 2 and 3 over k, we describe in this section these data for the curve E. By Proposition 9.3.8, as a Dieudonné module

$$M := M_E \cong \mathcal{D}_k/(F+V)\mathcal{D}_k$$

is free of rank 2 over $W(k)$.

Proposition 9.5.1. *As a finite commutative group scheme over k, we have*

$$M(E[p]) \cong \frac{M(W_2^2(k))}{(F+V)M(W_2^2(k))}.$$

Proof. Following [11, B.3] the module $M(E[p])$ is isomorphic to

$$M(E[p]) \cong \frac{M}{pM} \cong \frac{\mathcal{D}_k}{(p, F+V)\mathcal{D}_k} \cong \frac{\mathcal{D}_k}{(F+V)\mathcal{D}_k}$$

By [60, Proposition 22.2, Lemma 22.3] there exists an embedding $E[p] \hookrightarrow W_2^2(k)$. Applying the Dieudonné-Cartier-Oda functor M on the truncated Witt group scheme $W_2^2(k)$ yields a left $\mathcal{D}_k$-module $M(W_2^2(k))$ together with a left-exact sequence

$$0 \leftarrow \frac{M(W_2^2(k))}{(F+V)M(W_2^2(k))} \leftarrow M(W_2^2(k)) \xleftarrow{M(F+V)} M(W_2^2(k))$$

from which we conclude the statement. □

There is a basis f_1, f_2 for M as a $W(k)$-module such that

$$Ff_1 = f_2, \qquad Ff_2 = p \cdot f_1, \qquad Vf_2 = p \cdot f_1, \qquad Vf_1 = f_2. \tag{9.5.1}$$

See [46, Chapter 6.1]. Then, the representation matrix for the pairing $\langle , \rangle$ in Definition 9.4.4 with respect to the dual basis of M^t is given by

$$A = \begin{bmatrix} 0 & \beta \\ -\beta & 0 \end{bmatrix} \tag{9.5.2}$$

where $\beta \in W(k)$, $\beta = p^r \cdot \varepsilon$ for some $r \in \mathbb{Z}$ and some units $\varepsilon \in W(\mathbb{F}_{p^2}) \backslash pW(\mathbb{F}_{p^2})$ and with $\beta^\sigma = -\beta$. See [46, Proposition 6.1].

Lemma 9.5.2. *For any genus one quasi-polarized Dieudonné module M there is a $W(k)$-basis for the dual Dieudonné module M^t such that the representation matrix for the pairing $\langle , \rangle$ corresponding to this basis is given by the matrix A in Equation* (9.5.2).

Proof. If $\widetilde{f_1}, \widetilde{f_2}$ is a basis for M_E^t and if $\widetilde{A}$ is the representation matrix for the pairing $\langle , \rangle$ with respect to this basis, then there is a matrix $S \in \mathrm{GL}(2, W(k))$ such that $A = S^t \widetilde{A} S$. □

Remark 9.5.3. For the rest of our discussion, we assume always to choose a basis for M as in Equation (9.5.1), such that the representation matrix for the pairing with respect to the dual basis is given by the matrix A in Equation (9.5.2). See [46, Chapter 6.1].

9.6 The genus-2 case

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. For the rest of this section we fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$. In this, and in the next section we give an explicit description of the linear-algebraic data of polarized flag type quotients over k (see Definition 9.2.1), in terms of flag type quotients of Dieudonné modules of genus $g = 2, 3$ over the ring of Witt vectors $W(k)$. In this section we restrict to the genus-2 case.

As stated in Section 9.2, the authors in [46] describe a way to construct a sequence of inseparable isogenies

$$(Y_1 = E^2, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0) \tag{9.6.1}$$

such that η_0 is a principal polarization and where $a(Y_0) = 1, 2$. By Proposition 9.4.9, the pftq in Equation 9.6.1 induces an pftq of genus-2 Dieudonné modules over $W(k)$ that makes the following diagram commute

$$\begin{array}{ccc} M_1 = M(Y_1) & \xleftarrow{M(\rho_1)} & M_0 = M(Y_0) \\ {\scriptstyle M(\eta_1)}\uparrow & & \uparrow{\scriptstyle M(\eta_0')} \\ M_1^t = M(Y_1^t) & \xrightarrow{M(\rho_1^t)} & M_0^t = M(Y_0^t). \end{array} \tag{9.6.2}$$

In this section we describe the linear-algebraic data that goes with the diagram in Equation (9.6.2). As stated in Remark 9.4.6, as a Dieudonné module, M_1 is either *decomposable* or *indecomposable* as a $W(k)$-module. In the former case, M_1 decomposes as a direct sum of two Dieudonné modules of the form

$$M_1^1 \oplus M_1^2, \tag{9.6.3}$$

where M_1^i are indecomposable $W(k)$-modules of rank 2. As genus-1 quasi-polarized Dieudonné modules,

$$M_1^1 = M(E \times \{0\}), \text{ and } M_1^2 = M(\{0\} \times E).$$

We will show that in this case the quasi-polarization on M_1 is induced *only* from *one* of the two copies of the elliptic curve E in Equation (9.6.1). As we have seen in Definition 9.2.1, there is a condition on the kernel of the polarization η_1, namely that $\ker(\eta_1) = Y_1[F]$. We prove in Theorem 9.6.1, respectively in Proposition 9.6.3, together with the Remark 9.6.4 that in the genus-2 case this condition is equivalent for M_1 beeing indecomposable as a $W(k)$-module. In other words, M_1 is *not* a direct sum of two genus-1 quasi-polarized Dieudonné modules as in Equation (9.6.3).

The Dieudonné module $M_1 = M(Y_1)$

Theorem 9.6.1. *Let $(Y_1 = E^2, \eta_1)$ be a polarized abelian surface over k with the restriction on the polarization as in Definition 9.2.1, and satisfying the condition $\ker(\eta_1) = Y_1[F]$. There is a $W(k)$-basis f_1, f_2, f_3, f_4 for M_1 such that*

$$\begin{aligned} Ff_1 &= f_2, \quad Ff_2 = pf_1, \quad Ff_3 = f_4, \quad Ff_4 = pf_3, \\ Vf_1 &= f_2, \quad Vf_2 = pf_1, \quad Vf_3 = f_4, \quad Vf_4 = pf_3, \end{aligned} \tag{9.6.4}$$

and such that the representation matrix for the pairing $\langle , \rangle$ in Definition 9.4.4 with respect to the dual basis f_i^* for M_1^t is given by

$$A = \begin{bmatrix} 0 & 0 & -p & 0 \\ 0 & 0 & 0 & -1 \\ p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Proof. The basis f_i for M_1 with the properties in Equation (9.6.4) is given by [46, Proposition 6.1.ii].

On Dieudonné side the condition $\ker(\eta_1) = Y_1[F]$ is equivalent to

$$\operatorname{im}(M(\eta_1) : M_1^t \to M_1) = \operatorname{im}(F : M_1^{(p)} \to M_1). \tag{9.6.5}$$

Let e_1, e_3, e_3, e_4 be the basis for $M_1^{(p)}$ corresponding to the basis f_i of M_1 as in the statement of Proposition 9.3.12. From the bijection in Proposition 9.3.12, we get that

$$Fe_i = F(1 \otimes f_i) = Ff_i \tag{9.6.6}$$

for all $i = 1, \ldots, 4$. Then $\operatorname{im}(F : M_1^{(p)} \to M_1) = \langle pf_1, f_2, pf_3, f_4 \rangle$.

Let A be the representation matrix for $\langle , \rangle$ with respect to the dual basis f_i^* of M_1^t. By the relations in Equation (9.4.3), for the induced linear map $M(\eta_1)$, we get the following relations

$$(M(\eta_1))(f_1^*) = pf_3, \quad (M(\eta_1))(f_2^*) = f_4, \quad (M(\eta_1))(f_3^*) = -pf_1, \quad (M(\eta_1))(f_4^*) = -f_2,$$

from which we conclude the equality in Equation (9.6.5). This shows our claim. □

Remark 9.6.2. We stated in Equation (9.6.6) an equality, which we should explain. In the first interpretation $F : M_1^{(p)} \to M_1$ is a linear map, where in the last interpretation, $F : M_i^t \to M_1$ is a p-linear map. The condition on the kernel of the polarization η_1 induces an equality on the images of the maps in Equation (9.6.5). Since their images is uniquely determined by the images of their generators, we will do this identification in the further course of this chapter, without mentioning it explicitly.

Proposition 9.6.3. *We have $M(\ker(\eta_1)) \cong k^2$ and $\ker(\eta_1) \cong \alpha_p^2$.*

Proof. By Theorem 9.6.1, the image of $M(\eta_1)$ is generated by $-pf_1, -f_2, pf_3, f_4$. It follows that

$$M(\ker(\eta_1)) \cong \frac{M}{\operatorname{im}(M(\eta_1))} = \frac{\langle f_1, f_2, f_3, f_4 \rangle}{\langle -pf_1, -f_2, pf_3, f_4 \rangle} \cong \langle [f_1], [f_3] \rangle,$$

and $\langle [f_1], [f_3] \rangle \subset M_1/pM_1$. The first claim follows from the identification $k \cong \frac{W(k)}{(p)}$. The second claim follows immediately from the fact that F, V act trivially on both equivalence classes. □

Remark 9.6.4. With the setup as in Theorem 9.6.1 we get that: If M_1 is decomposable as a $W(k)$-module, then $M_1 \cong M_1^1 \oplus M_1^2$ (see Equation 9.6.3) where the M_1^i are simple rank-2 $W(k)$-modules. As in the proof of Theorem 9.6.1, the representation matrix for the pairing $\langle , \rangle$ with respect to the dual basis f_i^* of M_1^t, is in this case given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & p \\ 0 & 0 & -p & 0 \end{bmatrix}.$$

(See also [46, Proposition 6.1.i].) Then, in this case we can see that $\mathrm{im}(M(\eta_1)) = \langle f_1, -f_2, pf_3, -pf_4 \rangle$. It follows that

$$M(\ker(\eta_1)) \cong \frac{M_1}{\langle f_1, -f_2, pf_3, -pf_4 \rangle} \cong \langle [f_3], [f_4] \rangle,$$

and $\langle [f_3], [f_4] \rangle \subset M_1/pM_1$. The action of F, V on $M(\ker(\eta_1))$ is *non-trivial* in this case since

$$F[f_3] = [f_4], \quad F[f_4] = [pf_3] \equiv 0 \pmod{p}, \quad V[f_3] = [f_4], \quad V[f_4] = [pf_3] \equiv 0 \pmod{p}.$$

This shows that in the decomposable genus 2-case, $\ker(\eta_1) \ncong \alpha_p^2$. In other words we can see that in this case $\ker(\eta_1) \neq Y_1[F]$. In this case we have

$$\ker(\eta_1) \simeq (\{0\} \times E)[p],$$

where E is the second copy of Y_1.

Lemma 9.6.5. *For any pftq of Dieudonné modules of genus 2 over $W(k)$ there is an equivalent condition between $\ker(\eta_1) = Y_1[F]$ and the indecomposability condition of the Dieudonné module $M_1 = M(Y_1)$.*

Proof. Follows from Theorem 9.6.1, respectively from Remark 9.6.4. □

Remark 9.6.6. For the rest of this chapter we assume that M_1 is indecomposable as a Dieudonné module, which after Theorem 9.6.1 is equivalent to the condition $\ker(\eta_1) = Y_1[F]$. Following [46, Corollary on page 36], the latter condition is equivalent to the existence of an isomorphism $\varphi : M_1 \xrightarrow{\sim} FM_1^t$ induced by "the" quasi-polarization η_1 on M_1. We will not prove the last equivalence here.

Lemma 9.6.7. *If M_1 is indecomposable then $(F, V)M_1$ is as a $W(k)$-module generated by pf_1, f_2, pf_3, f_4.*

Proof. Clear from the relations in the Equation (9.6.4). □

The a-number $a(M_1)$

We can explicitly compute the a-number $a(M_1)$. By Remark 9.4.11, we know that $a(M_i) \leq g$ for all $0 \leq i \leq g-1$.

Proposition 9.6.8. *Let $M_1 \supset M_0$ be a genus 2 pftq. Then we have $\dfrac{M_1}{(F,V)M_1} \cong k^2$.*

Proof. Using the above identifications, we get that

$$\frac{M_1}{(F,V)M_1} \cong \left(\frac{\mathcal{D}_k/\mathcal{D}_k(F+V)}{(F,V)(\mathcal{D}_k/\mathcal{D}_k(F+V))}\right)^{\oplus_2} \cong \left(\frac{\mathcal{D}_k}{\mathcal{D}_k(F,V)}\right)^{\oplus_2} \cong M(\alpha_p)^{\oplus_2}.$$

Since $M_1/(F,V)M_1$ is a torsion $\mathcal{D}_k$-module of length 2, with the classification of modules over PID, we get that $M(\alpha_p)^{\oplus_2} \cong (W(k)/(p))^{\oplus_2} \cong k^2$ which proves the statement. □

Corollary 9.6.9. *We get that $a(M_1) = 2$.*

Proof. Clear from Proposition 9.6.8 and from Definition 9.4.10. □

Corollary 9.6.10. *There is an isomorphism of k-vector spaces $\frac{M_1}{(F,V)M_1} \xrightarrow{\sim} k^2$, given by*

$$[f_1] \mapsto \begin{bmatrix}1\\0\end{bmatrix}, \quad [f_3] \mapsto \begin{bmatrix}0\\1\end{bmatrix}.$$

Proof. Follows from Proposition 9.6.8. □

In order to determine dimensions of the relevant k-spaces corresponding to quotients of Dieudonné modules we prove the following lemma.

Lemma 9.6.11. *The map $\tau : \frac{M_0}{(F,V)M_1} \to \frac{M_1}{M_0}$, given by*

$$[m] \mapsto [M(\rho_1)(m)] \tag{9.6.7}$$

is the zero map on M_1/M_0, where $M(\rho_1) : M_0 \to M_1$ is the embedding in Diagram (9.6.2).

Proof. We note first that τ is well-defined. Take any $[m] \in \dfrac{M_0}{(F,V)M_1}$ and take representatives $s,t \in [m]$ of the form $s = u + (F,V)v$ and $t = u + (F,V)w$ for $u \in M_0$ and $v,w \in M_1$. Then $\tau(s) = \tau(t) = u$ since $(F,V)M_1 \subset M_0$. But

$$\tau([m]) = [M(\rho_1)(m)] = [m] = 0$$

for all $[m] \in \dfrac{M_0}{(F,V)M_1}$ since $M(\rho_1)$ is an embedding and since we are quotiening out by all of M_0. With other words $\operatorname{im}\tau = \dfrac{M_0}{M_0} \subset \dfrac{M_1}{M_0}$. □

Proposition 9.6.12. *There is a short exact sequence of k-vector spaces*

$$0 \to \frac{M_0}{(F,V)M_1} \xrightarrow{\iota} \frac{M_1}{(F,V)M_1} \xrightarrow{\pi} \frac{M_1}{M_0} \to 0$$

with $\tau = \pi \circ \iota$ as in Lemma 9.6.11.

Proof. The injection ι follows from chain of inclusions $(F,V)M_1 \subset M_0 \subset M_1$. The surjection π and that $\ker\pi = \operatorname{im}\iota = \dfrac{M_0}{(F,V)M_1}$ follow from Equation (9.6.7). Then by construction $\tau = \pi \circ \iota$. □

Corollary 9.6.13. *We get that $\dfrac{M_1}{M_0} \cong \dfrac{M_1/(F,V)M_1}{M_0/(F,V)M_1}$ and*

$$\dim_k\left(\frac{M_0}{(F,V)M_1}\right) = \dim_k\left(\frac{M_1}{M_0}\right) = 1, \quad \dim_k\left(\frac{M_1}{(F,V)M_1}\right) = 2.$$

Proof. The first statement follows from the third isomorphism theorem for modules, whereas the second statement follows from Lemma 9.6.11, respectively from Proposition 9.6.12. □

The Dieudonné module $M_0 = M(Y_0)$

In this section we fix an pftq of dimension 2 over k as in Equation (9.6.1), given by

$$(Y_1 = E^2, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0).$$

One of the main results in this chapter is given by the following theorem. The theory so far describes the isogeny

$$\rho_1 : Y_1 \to Y_0$$

in terms of Dieudonné modules M_0, which we can describe more precisely as follows:

Theorem 9.6.14. *Let k be a algebraically closed field of $char(k) = p > 0$. Let E be a supersingular elliptic curve over $k \supset \mathbb{F}_p$. Then, for any pftq of Dieudonné modules of genus 2 over $W(k)$ there is an equivalence between left $\mathcal{D}_k$-modules M_0 such that $M_1 \supset M_0$ is a pftq, and points in $\mathbb{P}^1_k$.*

Proof. After Corollary 9.6.10, as a k-vector space $\dfrac{M_1}{(F,V)M_1} \cong \langle [f_1], [f_3] \rangle$. By Corollary 9.6.13, as a one-dimensional k-vector space

$$\frac{M_0}{(F,V)M_1} \cong \langle \alpha[f_1] + \beta[f_3] \rangle,$$

where $\alpha, \beta \in k$ both non-zero. In other words, the point $[\alpha, \beta] \in \mathbb{P}^1_k$ uniquely determines the k-vector space. Then, by Theorem 9.4.12 as a rank-4 $W(k)$-module

$$M_0 = \langle \underline{\alpha} f_1 + \underline{\beta} f_3, pf_1, f_2, pf_3, f_4 \rangle,$$

where $\underline{\alpha}, \underline{\beta} \in W(k)$ of the form $\underline{\alpha} = (\alpha, 0, \ldots), \underline{\beta} = (\beta, 0, \ldots)$, and where pf_1, f_2, pf_3, f_4 is a basis for $(F,V)M_1 \subset M_0$ as in Proposition 9.6.7.

In order to prove the opposite direction of the statement, we need to describe explicitly the matrix representation of the pairing $\langle , \rangle$ on M_0 induced by the pairing $\langle , \rangle$ on M_1. □

Some explicit bases for $M_0 = M(Y_0)$

In order to finish the proof of Theorem 9.6.14, we give an explicit description of the relevant linear-algebraic data on M_0, depending on some explicit bases.

Proposition 9.6.15. *Let $[\alpha : \beta] \in \mathbb{P}^1_k$, such that M_0 is generated as a $W(k)$-module of rank 4 by*

$$\langle \underline{\alpha} f_1 + \underline{\beta} f_3, pf_1, f_2, pf_3, f_4 \rangle \tag{9.6.8}$$

and where pf_1, f_2, pf_3, f_4 is a $W(k)$-basis of $(F,V)M_1$. Depending on $\alpha \neq 0$ ($\beta \neq 0$, respectively) there are $W(k)$-bases for M_0 given by:

$$\begin{aligned} &\text{if } \alpha \neq 0: \quad \underline{\alpha} f_1 + \underline{\beta} f_3, f_2, pf_3, f_4, \\ &\text{if } \beta \neq 0: \quad \underline{\alpha} f_1 + \underline{\beta} f_3, pf_1, f_2, f_4. \end{aligned} \tag{9.6.9}$$

Proof. We have seen that the statement holds modulo $(F,V)M_1$. Since M_0 is a $W(k)$-module of rank 4, it is enough to show that in the first case pf_1, and in the second case pf_3 are representable by a linear combination in the set of elements in Equation (9.6.9) with coefficients in $W(k)$. We have $pf_1 = \underline{\alpha}^{-1}(p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3) - \underline{\beta} \cdot pf_3)$, $pf_3 = \underline{\beta}^{-1}(p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3) - \underline{\alpha} \cdot pf_1)$ which shows the claim. □

Remark 9.6.16. The element $\underline{\alpha} \in W(k)$ is the so-called *Teichmüller lift* of $k \to W(k)$, given by

$$x \mapsto \underline{x} := (x, 0, 0, ...).$$

Notation 9.6.17. For the rest of this section, we denote by $\mathcal{B}_\alpha = (\underline{\alpha} f_1 + \underline{\beta} f_3, f_2, pf_3, f_4)$, for $\alpha \neq 0$ and by $\mathcal{B}_\beta = (\underline{\alpha} f_1 + \underline{\beta} f_3, pf_1, f_2, f_4)$, for $\beta \neq 0$, the $W(k)$-bases of M_0 in Proposition 9.6.15.

Corollary 9.6.18. *For the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ in Notation 9.6.17, the matrix representations for $F = F|_{M_1}$ and $V = V|_{M_1}$ with respect to these bases are given by*

$$F = \begin{bmatrix} 0 & p\underline{\alpha}^{-1} & 0 & 0 \\ \underline{\alpha}^\sigma & 0 & 0 & 0 \\ 0 & -\underline{\beta}\underline{\alpha}^{-1} & 0 & 1 \\ \underline{\beta}^\sigma & 0 & p & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & p(\underline{\alpha}^{-1})^\sigma & 0 & 0 \\ \underline{\alpha} & 0 & 0 & 0 \\ 0 & -(\underline{\beta}/\underline{\alpha})^\sigma & 0 & 1 \\ \underline{\beta} & 0 & p & 0 \end{bmatrix},$$

respectively

$$F = \begin{bmatrix} 0 & 0 & 0 & p\underline{\beta}^{-1} \\ 0 & 0 & 1 & \underline{\alpha}\underline{\beta}^{-1} \\ \underline{\alpha}^\sigma & p & 0 & 0 \\ \underline{\beta}^\sigma & 0 & 0 & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 0 & 0 & p(\underline{\beta}^{-1})^\sigma \\ 0 & 0 & 1 & -(\underline{\alpha}/\underline{\beta})^\sigma \\ -\underline{\alpha} & p & 0 & 0 \\ \underline{\beta} & 0 & 0 & 0 \end{bmatrix}.$$

Proof. We prove this only for the basis $\mathcal{B}_\alpha$ i.e. for the case where $\alpha \neq 0$. The second case is similar. Let e_1, e_2, e_3, e_4 be the basis of $M_0^{(p)}$ corresponding to the chosen basis, via the correspondence in Proposition 9.3.12. Then, by the bijection in the same Proposition, the relations in Theorem 9.6.1 and in Proposition 9.6.15, we get that

$$\begin{aligned} Fe_1 &= F(1 \otimes (\underline{\alpha} f_1 + \underline{\beta} f_3)) = \underline{\alpha}^\sigma f_2 + \underline{\beta}^\sigma f_4, \\ Fe_2 &= F(1 \otimes f_2) = pf_1 = \underline{\alpha}^{-1} p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3) - \underline{\alpha}^{-1}\underline{\beta} \cdot pf_3, \\ Fe_3 &= F(1 \otimes pf_3) = p \cdot f_4, \\ Fe_4 &= F(1 \otimes f_4) = 1 \cdot pf_3. \end{aligned}$$

which shows the matrix representation for F. In order to prove the matrix representation for V with respect to this basis, we notice the following: After identifying $M_0 \hookrightarrow M_1$ by the linear map $M(\rho_1)$ in the Diagram 9.6.2 which is induced by the identity, F and V are restrictions of linear maps $F|_{M_0} : M_1^{(p)} \to M_1$ and $V|_{M_0} : M_1 \to M_1^{(p)}$. Therefore to check the matrix for V we just need to use relation $[p] = FV = VF$, which shows the claim. □

Proposition 9.6.19. *We have that $M(\ker(F|_{M_0})) \cong k^2$ and $\ker(F|_{M_0}) \cong \alpha_p^2$.*

Proof. By contravariant Dieudonné theory, the module $M(\ker(F|_{M_0}))$ is determined by the following exact sequence:

$$0 \leftarrow M(\ker(F|_{M_0})) \leftarrow M_0 \xleftarrow{M(F|_{M_0})} M_0^{(p)} \leftarrow 0.$$

It is enough to prove the claim for a single basis of M_0 in Equation (9.6.9) and we choose the first. In this case, we get that

$$M(\ker(F|_{M_0})) \cong \frac{M_0}{\operatorname{im}(M(F|_{M_0}))} = \frac{\langle \underline{\alpha} f_1 + \underline{\beta} f_3, f_2, pf_3, f_4 \rangle}{\langle \underline{\alpha}^\sigma f_2 + \underline{\beta}^\sigma f_4, pf_1, pf_4, pf_3 \rangle}.$$

Since k is of characteristic $p > 0$ and $\alpha \neq 0$ in k, then $\underline{\alpha} = (\alpha, 0, \ldots)$ is a unit in $W(k)$ and we may assume that $\underline{\alpha} = (1, 0, \ldots)$. Then we get

$$M(\ker(F|_{M_0})) \cong \frac{\langle f_1 + \underline{\beta} f_3, f_2, pf_3, f_4 \rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4, pf_1, pf_4, pf_3 \rangle} \cong \frac{\langle f_1 + \underline{\beta} f_3, f_4 \rangle}{\langle pf_1, pf_3, pf_4 \rangle} \cong \langle [f_1 + \underline{\beta} f_3], [f_4] \rangle \cong (W(k)/(p))^{\oplus_2} \cong k^2.$$

An explicit isomorphism $M(\ker(F|_{M_0})) \xrightarrow{\sim} k^2$ is given by

$$\begin{bmatrix} 1 \\ 0 \\ \beta \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} x \\ 0 \\ \beta \\ y \end{bmatrix} \mapsfrom \begin{bmatrix} x \\ y \end{bmatrix}.$$

Since F, V are acting trivial on $M(\ker(F|_{M_0}))$, this shows the second claim. □

The a-numbers $a(M_0)$

We have seen in Theorem 9.6.14 that, in the "language" of Dieudonné modules, any choice of isogeny $\rho_1 : Y_1 \to Y_0$ with $\ker(\rho_1) \cong \alpha_p$ is equivalent to the choice of a point in $[\alpha : \beta] \in \mathbb{P}^1_k$. It describes uniquely the Dieudonné module M_0. Theorem 9.6.20 (Corollary 9.6.21, more precisely) describe, depending on the coordinates of the point $[\alpha : \beta]$ the a-number $a(M_0) = a(M(Y_0))$, which by contravariant Dieudonné theory is identical with the a-number of the supersingular abelian variety Y_0 of dimension 2 over k.

Theorem 9.6.20. *For any of the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ in Notation 9.6.17, we get that*

$$\frac{M_0}{(F,V)M_0} \cong k^{\varepsilon},$$

and where, up to permutation of α and β

$$\varepsilon = \begin{cases} 2, & \text{if and only if } \alpha \in \mathbb{F}_p^{\times},\ \beta \in \mathbb{F}_{p^2}, \\ 1, & \text{if and only if } \alpha \in \mathbb{F}_p^{\times},\ \beta \notin \mathbb{F}_{p^2}. \end{cases}$$

Proof. By a similar computation as in Proposition 9.6.19, we get that

$$\frac{M_0}{(F,V)M_0} = \frac{\langle \underline{\alpha} f_1 + \underline{\beta} f_3, f_2, pf_3, f_4 \rangle}{\langle \underline{\alpha}^{\sigma} f_2 + \underline{\beta}^{\sigma} f_4, \underline{\alpha}^{\sigma^{-1}} f_2 + \underline{\beta}^{\sigma^{-1}} f_4, pf_1, pf_4, pf_3 \rangle}.$$

Since the dimension of any k-vector space is independent of the chosen basis, we prove this for the basis $\mathcal{B}_\alpha$. In comparison to Proposition 9.6.19, we get the extra condition $\underline{\alpha}^{\sigma^{-1}} f_2 + \underline{\beta}^{\sigma^{-1}} f_4 = 0$ from the Verschiebungsoperator V. Since $\alpha \neq 0$ we set w.l.o.g. $\underline{\alpha} = (1, 0, \ldots)$. Simplifying the first two conditions in the denominator and writing them down in a matrix form yields a system of linear equations

$$\left[\begin{array}{cc|c} 1 & \underline{\beta}^{\sigma} & 0 \\ 0 & (\underline{\beta}^{\sigma} - \underline{\beta}^{\sigma^{-1}}) & 0 \end{array}\right]$$

with rank equal to 1, if and only if $\underline{\beta}^{\sigma^2} = \underline{\beta}$, and where the latter condition is equivalent to $\beta^{p^2} \equiv \beta \pmod{p}$. In other words, the latter congruence is true if and only if $\beta \in \mathbb{F}_{p^2}$. In this case we get that

$$\begin{aligned}
\frac{M_0}{(F,V)M_0} &= \frac{\langle f_1 + \underline{\beta} f_3, f_2, pf_3, f_4\rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4, f_2 + \underline{\beta}^{\sigma^{-1}} f_4, pf_1, pf_4, pf_3\rangle} \\
&\cong \frac{\langle f_1 + \underline{\beta} f_3, f_2, pf_3, f_4\rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4, pf_1, pf_4, pf_3\rangle} \\
&\cong \frac{\langle f_1 + \underline{\beta} f_3, f_2 + \underline{\beta}^{\sigma} f_4, pf_3, f_4\rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4, pf_1, pf_4, pf_3\rangle} \\
&\cong \frac{\langle f_1 + \underline{\beta} f_3, f_4\rangle}{\langle pf_1, pf_3, pf_4\rangle} \\
&\cong \langle [f_1 + \underline{\beta} f_3], [f_4]\rangle \\
&\cong k^2,
\end{aligned}$$

and where $\langle [f_1 + \underline{\beta} f_3], [f_4]\rangle \cong M(\ker(F|_{M_0}))$, as we proved in Proposition 9.6.19.

In the case where the rank of the matrix above is 2, in other words when $\beta \in k \backslash \mathbb{F}_{p^2}$ we get that

$$\frac{M_0}{(F,V)M_0} \cong \langle [f_1 + \underline{\beta} f_3]\rangle \cong k,$$

which shows the claim. □

Corollary 9.6.21. *With the same notation as at the beginning of this section we get that, up to permutation of α and β,*

$$a(M_0) = \begin{cases} 1, & \text{if and only if } \beta/\alpha \in \mathbb{F}_{p^2}, \\ 2, & \text{if and only if } \beta/\alpha \notin \mathbb{F}_{p^2}. \end{cases}$$

Proof. Follows from Theorem 9.6.20 and from Definition 9.4.10, respectively. □

Lemma 9.6.22. *For any of the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ in Notation 9.6.17, the matrix representation for $M(\rho_1) : M_0 \to M_1$ with respect to these bases are given by*

$$\begin{bmatrix} \underline{\alpha} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \underline{\beta} & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} \underline{\alpha} & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \underline{\beta} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively.

Proof. Follows immediately from the exact sequence $0 \leftarrow M(\ker(\rho_1)) \leftarrow M_1 \xleftarrow{M(\rho_1)} M_0 \leftarrow 0$. □

Corollary 9.6.23. *The inverse of $A_{M(\rho_1)} \in \mathrm{Mat}_4(W(k)[1/p])$ are given by*

$$\begin{bmatrix} \underline{\alpha}^{-1} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -\underline{\beta}(\underline{\alpha}p)^{-1} & 0 & p^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & \underline{\beta}^{-1} & 0 \\ p^{-1} & 0 & -\underline{\alpha}(p\underline{\beta})^{-1} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively.

Proof. A straightforward computation. □

Lemma 9.6.24. *With the notation as in Lemma 9.6.22, we have that* $M(\ker(\rho_1)) \cong k$ *and* $\ker(\rho_1) \cong \alpha_p$.

Proof. By the exact sequence in Lemma 9.6.22 and the matrix representations for $A_{M(\rho_1)}$ with respect to the basis $\mathcal{B}_\alpha$, we get that

$$M(\ker(\rho_1)) \cong \frac{M_1}{\mathrm{im}(M(\rho_1))} = \frac{\langle f_1, f_2, f_3, f_4\rangle}{\langle \underline{\alpha} f_1 + \underline{\beta} f_3,\ f_2, pf_3, f_4\rangle}.$$

Since k is a field of characteristic $p > 0$ and $\alpha \neq 0$ in k, $\underline{\alpha} = (\alpha, 0, \ldots)$ is a unit in $W(k)$ and we may assume that $\underline{\alpha} = (1, 0, \ldots)$. Then we have

$$M(\ker(\rho_1)) \cong \frac{\langle f_1, f_2, f_3, f_4\rangle}{\langle f_1 + \underline{\beta} f_3,\ f_2, pf_3, f_4\rangle} \cong \frac{\langle f_1 + \underline{\beta} f_3, f_2, f_3, f_4\rangle}{\langle f_1 + \underline{\beta} f_3,\ f_2, pf_3, f_4\rangle} \cong \langle [f_3]\rangle \cong W(k)/(p) \cong k.$$

Once can see that F and V are acting trivial on $M(\ker(\rho_1))$ since f_4 is already in $\mathrm{im}(M(\rho_1))$. This proves the claim. □

Proposition 9.6.25. *For any of the bases* $\mathcal{B}_\alpha, \mathcal{B}_\beta$ *in Notation 9.6.17, the matrix representation* $A_{M(\eta_0)} \in \mathrm{Mat}_4(W(k))$ *for the pairing on* M_0*, induced by the pairing on* M_1 *and with respect to the dual bases for* M_0^t*, these are given by*

$$\begin{bmatrix} 0 & 0 & -\underline{\alpha}^{-1} & 0 \\ 0 & 0 & 0 & -1 \\ \underline{\alpha}^{-1} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \underline{\beta}^{-1} & 0 & 0 \\ -\underline{\beta}^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

respectively.

Proof. A straightforward computation using $A_{M(\rho_1)} = A$ in Theorem 9.6.1 and the matrices $A_{M(\rho_1)}$ in Lemma 9.6.22, and Corollary 9.6.23, and the relation

$$A_{M(\eta_0)} = A_{M(\rho_1)}^{-1} A_{M(\eta_1)} (A_{M(\rho_1)}^{-1})^t.$$

□

After the identification of the for us relevant linear-algebraic data for the pftq of Dieudonné modules of genus 2 over $W(k)$, we can *finish* the proof of *Theorem 9.6.14*.

Proof. [Proof of Theorem 9.6.14.]
Let $f_1, \ldots, f_4$ be a $W(k)$-basis for M_1 as in Theorem 9.6.1 and let $[x : y] \in \mathbb{P}^1_k$. By following the proof of Theorem 9.6.14 we construct a $W(k)$-module of rank 4, $\widetilde{M}_0$ generated by

$$\underline{x} f_1 + \underline{y} f_2, pf_1, f_2, pf_3, f_4$$

such that $(F, V)M_1 \subset \widetilde{M}_0 \subset M_1$. Then by the discussion above, and since M_1 is a polarized Dieudonné module, the pairing $\langle\rangle$ on M_1^t induced by M_1 induces a perfect pairing $\langle\rangle_{\widetilde{M}_0^t} := \langle\rangle|_{\widetilde{M}_0^t}$ on $\widetilde{M}_0^t$. Depending on the values $x \neq 0$ or $y \neq 0$, the matrix representations of the pairing $\langle\rangle_{\widetilde{M}_0^t}$ with respect to some bases of $\widetilde{M}_0^t$ is similar to the one in Proposition 9.6.25. This shows the claim. □

As stated at the beginning of this section, any choice of an isogeny $\rho_1 : Y_1 \to Y_0$ with $\ker(\rho_1) \cong \alpha_p$ is equivalent to the choice of a point in $\mathbb{P}^1_k$ uniquely identifying the Dieudonné module M_0.

Proposition 9.6.26. *There is a bijection between the set of isogenies* $\{\rho_1 : Y_1 \to Y_0\}$ *in Equation* (9.6.1) *modulo equivalence and points in* $\mathbb{P}^1_k$.

Proof. By construction, Y_0 is given by the projection $Y_1/\ker(\rho_1)$ for an isogeny ρ_1 modulo equivalence (see Definition 9.1.3). If M_0 is the Dieudonné module to $Y_0 \cong Y_1/\ker\rho_1$, then by Theorem 9.6.14 the module M_0 is as a $W(k)$-module uniquely identified by a point $[\alpha : \beta]$ in $\mathbb{P}^1_k$.

On the other hand any submodule $\widetilde{M}$ with the property that $(F, V)M_1 \subset \widetilde{M} \subset M_1$ corresponds to an isogeny class $[\widetilde{\rho}]$, depending on a point $[x : y] \in \mathbb{P}^1_k$, which uniquely identifies $\widetilde{M}$ and where $\widetilde{M}_0 = M(Y_1/\ker(\widetilde{\rho}))$. □

Lemma 9.6.27. *Let* $(Y_1 = E^2, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0)$ *be a pftq of dimension* 2 *over* k *with respect to the polarization* η_1, *and where* $\ker(\eta_1) = Y_1[F]$. *Then* $\eta_0 : Y_0 \to Y_0^t$ *is a principal polarization.*

Proof. By Definition 9.2.1 we have $\deg(\eta_1) = \deg(\rho_1)^2 \deg(\eta_0)$. The claim follows from Proposition 9.6.3 and Lemma 9.6.24. □

The supersingular locus $\mathcal{S}_{2,1}$

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. For the rest of this section we fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$. In the previous sections we investigate the linear-algebraic data of tftq's of dimension 2 over k in terms of Dieudonné modules. In this section we briefly consider the so-called *supersingular locus*. We give some relations between our explicit calculations in the previous sections the latter space.

Let $Y_1 = E^2$ be a supersingular abelian surface over k. By following [46], we denote by Λ the set of equivalence classes of polarizations

$$\Lambda = \left\{[\eta] : \eta : Y_1 \to Y_1^t,\ \ker(\eta) = Y_1[F]\right\}/\sim$$

where $[\eta] \sim [\eta']$ if there is an $\varphi \in \mathrm{Aut}_k(Y_1)$ such that $\eta' = \varphi^t \circ \eta \circ \varphi$.

Remark 9.6.28. By the discussions above, the conditions on the $\ker(\eta)$ in the definition of Λ correspond to: By Lemma 9.6.4, this condition is equivalent to

$$\ker(\eta) \ncong (\{0\} \times E)[p] \text{ or } \ker(\eta) \ncong (E \times \{0\})[p].$$

As we noticed in Lemma 9.6.5, the condition on $\ker(\eta)$ is on the Dieudonné "site" equivalent to $M_1 = M(Y_1) \neq M_1^1 \oplus M_1^2$ as a $W(k)$-module and where the M_1^i are simple rank-2 $W(k)$-modules.

There is a deep relationship between the endomorphism algebra of the supersingular elliptic curve E and the cardinality of the set Λ. We briefly describe it. Let $\mathcal{B} = \mathbb{Q}_{p,\infty}$ be the definite quaternion $\mathbb{Q}$-algebra in Definition 9.1.2, ramified only at (p, ∞). By [46, Chapters 4 and 9], the set of equivalence classes of polarizations Λ is finite. Its cardinality is given by

$$\#\Lambda = H_2(1, p),$$

where $H_2(1, p)$ corresponds to the *class number of the non-principal genus* of positive definite quaternion hermitian space of dimension 2 over $\mathcal{B}$ (for the definition, see [35, 30]).

Using the formula in [46, page 56], we get for primes up to 60 the values of the class number $H_2(1,p)$ which are given by the following table [3]:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
$H_2(1,p)$	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4	6	5

Table 9.1: $H_2(1,p)$-values for primes $p < 60$.

Definition 9.6.29. For any equivalence class of polarizations $[\eta] \in \Lambda$, we define by $\mathcal{P}'_{2,\eta}$ the *rigid moduli space of principally polarized flag type quotients of dimension 2 over $\mathbb{F}_{p^2}$ with respect to η*. We define by $S_{2,1}$ the *moduli space of supersingular principally polarized abelian surfaces* over k. It is the supersingular locus in the coarse moduli $\mathcal{A}_2$ of principally polarized abelian surfaces (see [46, Page 15]).

Remark 9.6.30. For general g, the authors in [46, Chapter 3] introduce $\mathcal{P}_{g,\eta}$ as the moduli space of principally polarized flag type quotients of dimension g over $\mathbb{F}_{p^2}$, with the property that $\mathcal{P}'_{g,\eta} \subseteq \mathcal{P}_{g,\eta}$ for any g. In the genus 2, the spaces $\mathcal{P}'_{g,\eta} = \mathcal{P}_{g,\eta}$, and we will consider for the rest of this chapter only the first space. See also Remark 9.2.2.

There is a quasi-finite and surjective morphism defined over $\mathbb{F}_{p^2}$, given by

$$\Psi : \coprod_{[\eta]\in\Lambda} \mathcal{P}'_{2,\eta} \to \mathcal{S}_{2,1}$$
$$(Y_1 \xrightarrow{\rho_1} Y_0) \mapsto (Y_0, \eta_0).$$

See [46, page 24]. By following [46, Corollary 4.4,] we get the following properties for $\mathcal{P}'_{2,\eta}$:

(i) It is non-singular, geometrically integral of dimension 1.

(ii) The generic fibre of Y_0 over $\mathcal{P}'_{2,\eta}$ is supergeneral.

By contravariant Dieudonné theory, and the explicit computations in the previous sections of this chapter, we could *convince* ourselves that $\mathcal{P}'_{2,\eta} \cong \mathbb{P}^1_k$ by proving Theorem 9.6.14 (see also here [46, Chapter 9.2]). Further we could explicitly determine in Corollary 9.6.21 the points in $\mathbb{P}^1_k$ such that $M_0 = M(Y_0)$ is supergeneral.

Remark 9.6.31. Recently *Andreas Pieper* described an algorithmic construction of the image of $\mathcal{P}'_{2,\eta}$ in $\mathcal{S}_{2,1}$ under Ψ. See [58].

[3] The random prime numbers $p < 60$ is due to the available space.

9.7 The genus-3 case

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. For the rest of this section we fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$. As stated in Section 9.2, the authors in [46] describe a way to construct a sequence of inseparable isogenies

$$(Y_2 = E^3, \eta_2) \xrightarrow{\rho_2} (Y_1, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0) \tag{9.7.1}$$

such that η_0 is a principal polarization and where $a(Y_0) = 1, 2, 3$. The sequence in Equation 9.7.1 is equivalent to the following commutative diagram

$$\begin{array}{ccccc} Y_2 & \xrightarrow{\rho_2} & Y_1 & \xrightarrow{\rho_1} & Y_0 \\ {\scriptstyle \eta_2}\downarrow & & {\scriptstyle \eta_1}\downarrow & & {\scriptstyle \eta_0'}\downarrow \\ Y_2^t & \xleftarrow{\rho_2^t} & Y_1^t & \xleftarrow{\rho_1^t} & Y_0^t \end{array} \tag{9.7.2}$$

By Proposition 9.4.9 it induces an pftq of Dieudonné modules genus 3 over $W(k)$, given by

$$\begin{array}{ccccc} M_2 & \xleftarrow{M(\rho_2)} & M_1 & \xleftarrow{M(\rho_1)} & M_0 \\ {\scriptstyle M(\eta_2)}\uparrow & & {\scriptstyle M(\eta_1)}\uparrow & & \uparrow{\scriptstyle M(\eta_0')} \\ M_2^t & \xrightarrow{M(\rho_2^t)} & M_1^t & \xrightarrow{M(\rho_1^t)} & M_0^t. \end{array} \tag{9.7.3}$$

In this chapter we describe the linear-algebraic data according to the Diagram in Equation (9.7.3).

Remark 9.7.1. By [46, Chapter 6.1], the module M_2 is as a module over $W(k)$ of rank 6 *decomposable*, as

$$M_2^1 \oplus M_2^2 \oplus M_2^3, \tag{9.7.4}$$

and where M_2^i are indecomposable $W(k)$-modules of rank 2. One may prove rigorous, that in genus 3 the decomposable condition of M_2 is equivalent to the condition that $\ker(\eta_2) = Y_2[F^2]$. We will not prove this at this point.

By the construction of the pftq of Dieudonné modules in Equation (9.7.3), and by Definition 9.4.5, there are module chains

$$M_0 \subset M_1 \subset M_2, \quad (F,V)M_2 \subset M_1 \subset M_2, \quad (F,V)M_1 \subset M_0 \subset M_1. \tag{9.7.5}$$

In the following we use the diagram construction in Equation (9.7.3), as well as the informations encoded in the module chains in Equation (9.7.5), to identify the whole linear-algebraic data to the pftq in Equation (9.7.1).

The Dieudonné module $M_2 = M(Y_2)$

We begin our identification with the left square in diagram (9.7.3).

Theorem 9.7.2. *Let $(Y_2 = E^3, \eta_2)$ be a polarized abelian threefold over k with the restriction on the polarization (see Definition 9.2.1), given by* $\ker(\eta_2) = Y_2[F^2]$. *There is a $W(k)$-basis $f_1, \dots, f_6$ for M_2 such that*

$$\begin{aligned} Ff_1 &= f_2, \quad Ff_2 = pf_1, \quad Ff_3 = f_4, \quad Ff_4 = pf_3, \quad Ff_5 = f_6, \quad Ff_6 = pf_5, \\ Vf_1 &= f_2, \quad Vf_2 = pf_1, \quad Vf_3 = f_4, \quad Vf_4 = pf_3, \quad Vf_5 = f_6, \quad Vf_6 = pf_5. \end{aligned} \tag{9.7.6}$$

The representation matrix for the pairing $\langle , \rangle$ in Definition 9.4.4 with respect to the dual basis f_i^* for M_2^t is given by

$$A = \begin{bmatrix} 0 & p & 0 & 0 & 0 & 0 \\ -p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & -p & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & p \\ 0 & 0 & 0 & 0 & -p & 0 \end{bmatrix}. \tag{9.7.7}$$

Proof. The condition $\ker(\eta_2) = Y_2[F^2]$ is on Dieudonné side equivalent to [4]

$$\operatorname{im}(M(\eta_2) : M_2^t \to M_2) = \operatorname{im}(F^2 : M_2^{(p^2)} \to M_2). \tag{9.7.8}$$

Let $e_1, \dots, e_6$ be the basis for $M^{(p^2)}$ corresponding to the basis f_i of M_2 as in the statement of Proposition 9.3.12. Then we get

$$\begin{aligned} F^2e_1 &= F(F(1 \otimes f_1)) = F(f_2) = pf_1, \quad & F^2e_2 &= F(F(1 \otimes f_2)) = pF(f_1) = pf_2, \\ F^2e_3 &= F(F(1 \otimes f_3)) = F(f_4) = pf_3, \quad & F^2e_4 &= F(F(1 \otimes f_4)) = pF(f_3) = pf_4, \\ F^2e_5 &= F(F(1 \otimes f_5)) = F(f_6) = pf_5, \quad & F^2e_6 &= F(F(1 \otimes f_6)) = pF(f_5) = pf_6. \end{aligned}$$

Then $\operatorname{im}(F^2 : M^{(p^2)} \to M)$ is generated by $pf_1, \dots, pf_6$.

If A is the representation matrix for $\langle , \rangle$ with respect to the dual basis f_i^*, then for the induced linear p-map $M(\eta_2)$, we get

$$\begin{aligned} (M(\eta_2))(f_1^*) &= -pf_2, \quad & (M(\eta_2))(f_2^*) &= pf_1, \quad & (M(\eta_2))(f_3^*) &= -pf_4, \\ (M(\eta_2))(f_4^*) &= pf_3, \quad & (M(\eta_2))(f_5^*) &= -pf_6, \quad & (M(\eta_2))(f_6^*) &= pf_5 \end{aligned}$$

from which we conclude the equality in Equation (9.7.8). This shows our claim. □

Proposition 9.7.3. *We have $M(\ker(\eta_2)) \cong k^6$, and $\ker(\eta_2) \cong Y_2[p]$.*

Proof. By Theorem 9.7.2 the image of $M(\eta_2)$ is generated by $pf_1, -pf_2, pf_3, -pf_4, pf_5, -pf_6$. Then

$$M(\ker(\eta_2)) \cong \frac{M_2}{\operatorname{im}(M(\eta_2))} = \frac{\langle f_1, f_2, f_3, f_4, f_5, f_6 \rangle}{\langle pf_1, -pf_2, pf_3, -pf_4, pf_5, -pf_6 \rangle} \cong \langle [f_1], \dots, [f_6] \rangle.$$

Since p acts as zero on the quotient space and by the isomorphism $k \cong W(k)/(p)$ this shows the first claim.

In order to prove the second claim, we observe that the action of F and V on $M(\ker(\eta_2))$ is non-trivial and induced by Equation (9.7.6). Since $\operatorname{im}(M(\eta_2))$ corresponds to the multiplication by p together with a flipping of the generators of any of the indecomposable modules of M_2 in Equation 9.7.4, this shows the second claim. □

[4] In the following, we use the same arguments related to the next equality and its interpretation as in Remark 9.6.2.

Proposition 9.7.4. *The module $(F,V)M_2$ is as a $W(k)$-module rank 6 generated by*

$$pf_1, f_2, pf_3, f_4, pf_5, f_6.$$

Proof. Follows from the relations in Equation 9.7.6. □

The a-number, $a(M_2)$

Proposition 9.7.5. *Let $M_2 \supset M_1 \supset M_0$ be a genus 3 pftq. Then we have $\dfrac{M_2}{(F,V)M_2} \cong k^3$.*

Proof. By using the same arguments as in the proof of Proposition 9.6.8, we get that

$$\frac{M_2}{(F,V)M_2} \cong \left(\frac{\mathcal{D}_k/\mathcal{D}_k(F+V)}{(F,V)(\mathcal{D}_k/\mathcal{D}_k(F+V))}\right)^{\oplus_3} \cong \left(\frac{\mathcal{D}_k}{\mathcal{D}_k(F,V)}\right)^{\oplus_3} \cong M(\alpha_p)^{\oplus_3}.$$

Using the fact that $\dfrac{M_2}{(F,V)M_2}$ is a torsion $\mathcal{D}_k$-module of length 3 together with the classification of modules over PID's, we get $M(\alpha_p)^{\oplus_3} \cong \left(\dfrac{W(k)}{(p)}\right)^{\oplus_3} \cong k^3$ which proves the statement. □

Corollary 9.7.6. *As a k-vector space*

$$\frac{M_2}{(F,V)M_2} \cong \langle [f_1], [f_3], [f_5] \rangle,$$

and there is an isomorphism of k-vector spaces $\frac{M_2}{(F,V)M_2} \xrightarrow{\sim} k^3$, given by

$$[f_1] \mapsto \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad [f_3] \mapsto \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad [f_5] \mapsto \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Proof. The proof of the first statement is a straightforward calculation given by

$$\frac{M_2}{(F,V)M_2} = \frac{\langle f_1, f_2, f_3, f_4, f_5, f_6 \rangle}{\langle f_2, pf_1, f_3, pf_4, f_5, pf_6 \rangle} \cong \langle [f_1], [f_3], [f_5] \rangle.$$

The second statement follows immediately. □

Corollary 9.7.7. *We have $a(M_2) = 3$.*

Proof. Clear from Definition 9.4.10 and Corollary 9.7.6. □

Our next step is the explicit description of the Dieudonné module $M_1 = M(Y_1)$, where by the construction (see Equation 9.7.1), $Y_1 \cong Y_2/\ker(\rho_2)$ and $\ker(\rho_2) \cong \alpha_p^2$. Let $(F,V)M_2 \subset M_1 \subset M_2$ be the second Dieudonné module chain in Equation (9.7.5) (see Definition 9.4.5). This induces quotient modules of the form

$$0 \subset \frac{M_1}{(F,V)M_2} \subset \frac{M_2}{(F,V)M_2}.$$

In order to determine dimensions of the k-spaces corresponding to these quotients, we prove the following lemma and proposition.

Lemma 9.7.8. *The map* $\tau : \dfrac{M_1}{(F,V)M_2} \to \dfrac{M_2}{M_1}$, *given by*

$$[m] \mapsto [M(\rho_2)(m)]$$

is the zero map on the quotient $\dfrac{M_2}{M_1}$.

Proof. Use the same arguments as in Lemma 9.6.11 after replacing by the corresponding quotients. □

Proposition 9.7.9. *There is a short exact sequence of* k*-vector spaces*

$$0 \to \frac{M_1}{(F,V)M_2} \xrightarrow{\iota} \frac{M_2}{(F,V)M_2} \xrightarrow{\pi} \frac{M_2}{M_1} \to 0$$

with $\tau = \pi \circ \iota$ *in Lemma 9.7.8.*

Proof. Use the same arguments as in Proposition 9.6.12 after replacing by the corresponding quotients. □

Corollary 9.7.10. *We get that* $\dfrac{M_2}{M_1} \cong \dfrac{M_2/(F,V)M_2}{M_1/(F,V)M_2}$ *and*

$$\dim_k\left(\frac{M_1}{(F,V)M_2}\right) = 1, \quad \dim_k\left(\frac{M_2}{M_1}\right) = 2.$$

Proof. The first statement follows from the third Isomorphism theorem of modules, whereas the second statement follows from Proposition 9.7.9 and Lemma 9.7.25. □

The Dieudonné module $M_1 = M(Y_1)$

Proposition 9.7.11. *As a* $W(k)$*-module of rank* 6, M_1 *is generated by*

$$\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, pf_5, f_6. \tag{9.7.9}$$

Proof. As a k-vector space $\dfrac{M_2}{(F,V)M_2} \cong \langle [f_1], [f_3], [f_5] \rangle$ (see Corollary 9.7.6). As a one-dimensional k-vector space (see Corollary 9.7.31)

$$\frac{M_1}{(F,V)M_2} \cong \langle \alpha[f_1] + \beta[f_3] + \gamma[f_5] \rangle$$

where $\alpha, \beta, \gamma \in k$ all three nonzero. In other words $[\alpha : \beta : \gamma] \in \mathbb{P}^2_k$. Then $\underline{\alpha} = (\alpha, 0, \ldots), \underline{\beta} = (\beta, 0, \ldots), \underline{\gamma} = (\gamma, 0, \ldots)$ are elements in $W(k)$.

In order to compute generators for M_1 we use the fact that $(F,V)M_2 \subset M_1$ (see Equation (9.7.5)). This guarantees that the basis $pf_1, f_2, pf_3, f_4, pf_5, f_6$ of $(F,V)M_2$ can be extended to a generating system of M_1. Together with these generators and the pull-back of the generator of $\dfrac{M_1}{(F,V)M_2}$ (see Lemma 9.4.12) shows the claim. □

The descending condition on η_1 and points on the Fermat curve $\mathcal{V}$

Let

$$(Y_2 = E^3, \eta_2) \xrightarrow{\rho_2} (Y_1, \eta_1)$$

be the first part of the 3-dimensional pftq over k from the sequence in Equation (9.7.1). By Definition 9.2.1, in order to guarantee a descending of the polarizations η_i, such that η_0 is a principal polarization, there is a condition on η_1 given by $\ker(\eta_1) \subset Y_1[F]$. In this section, we show in Theorem 9.7.13 that the latter condition on η_1 is equivalent to a point $P = [\alpha : \beta : \gamma] \in \mathbb{P}^2_k$, such that P is a point on the *Fermat curve*

$$\mathcal{V} := \mathcal{Z}(X^{p+1} + Y^{p+1} + Z^{p+1}) \subset \mathbb{P}^2_k. \tag{9.7.10}$$

Further we show in Corollary 9.7.14 and Proposition 9.7.15, that any $P \in \mathcal{V}$ uniquely identifies a Dieudonné module $\widetilde{M}$ up to isomorphism, such that

$$(F, V)M_2 \subset \widetilde{M} \subset M_2$$

and such that $\widetilde{M} = M(Y_2/\ker(\widetilde{\rho}))$, where $\ker(\widetilde{\rho})$ is an α-group scheme (see Definition B.1.1) of order p^2.

The dual Dieudonné module $M_1^t = M(Y_1^t)$

In order to prove the statements above, we need an explicit description of the dual Dieudonné module M_1^t.

Proposition 9.7.12. *Let $f_1^*, \dots, f_6^*$ be a basis of M_2^t dual to the basis $f_1, \dots, f_6$ of M_2 in Equation (9.7.6). Let*

$$\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, pf_5, f_6$$

be generators of M_1 as in Proposition 9.7.11. Then, as a $W(k)$-module of rank 6,

$$M_1^t = \left\{ m \in M_2^t \otimes_{W(k)} K : \begin{array}{l} m = \omega_1 f_1^* \otimes p^{-1} + \omega_2 f_2^* \otimes 1 + \omega_3 f_3^* \otimes p^{-1} + \omega_4 f_4^* \otimes 1 + \omega_5 f_5^* \otimes p^{-1} + \omega_6 f_6^* \otimes 1, \\ \underline{\alpha}\omega_1 + \underline{\beta}\omega_3 + \underline{\gamma}\omega_5 \equiv 0 \pmod{p}, \omega_i \in W(k). \end{array} \right\}$$

where $K = W(k)[1/p]$ is the fraction field of $W(k)$.

Proof. Let $M_2^t = \mathrm{Hom}_{W(k)}(M_2, W(k))$. By definition, the dual of M_1 is given by

$$M_1^t = \{m \in M_2^t \otimes_{W(k)} K : m(M_1) \subset W(k)\}. \tag{9.7.11}$$

Since $M_2^t \subset M_1^t$ (one can see this i.e. from Diagram 9.7.3), in order to construct M_1^t we need to allow scalar extensions to M_2^t.

Let $m \in M_2^t \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $m = \sum_{i=1}^6 \lambda_i f_i^*$ with $\lambda_i \in W(k)$. Computing generators for M_1^t is equivalent to solving a linear system given by linear forms m respecting the condition in Equation (9.7.11). Concretely, we have given the following linear system of equations:

$$m(pf_1) = \lambda_1 \otimes \frac{1}{p} = \omega_1, \qquad m(f_2) = \lambda_2 \otimes 1 = \omega_2, \qquad m(pf_3) = \lambda_3 \otimes \frac{1}{p} = \omega_3,$$

$$m(f_4) = \lambda_4 \otimes 1 = \omega_4, \qquad m(pf_5) = \lambda_5 \otimes \frac{1}{p} = \omega_5, \qquad m(f_6) = \lambda_6 \otimes 1 = \omega_6,$$

$$m(\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) = \underline{\alpha}\lambda_1 \otimes \frac{1}{p} + \underline{\beta}\lambda_3 \otimes \frac{1}{p} + \underline{\gamma}\lambda_5 \otimes \frac{1}{p} = \omega_7.$$

The last equation is equivalent to $p^{-1}\underline{\alpha}\omega_1 + p^{-1}\underline{\beta}\omega_3 + p^{-1}\underline{\gamma}\omega_5 = \omega_7$ and this is solvable in $W(k)$ if and only if $p\omega_7$ is an element in $W(k)$. With other words, we have a congruence relation given by

$$\underline{\alpha}\omega_1 + \underline{\beta}\omega_3 + \underline{\gamma}\omega_5 \equiv 0 \pmod{p}.$$

Together with the equations above this shows our claim. □

Theorem 9.7.13. *Let $P = [\alpha : \beta : \gamma]$ be a point in $\mathbb{P}^2_k$ uniquely identifying M_1 as a $W(k)$-module of rank 6 as in Proposition 9.7.11. Then* $\ker(\eta_1) \subset Y_1[F]$ *is equivalent to the point P to be on the* Fermat curve

$$\mathcal{V} = \mathcal{Z}(X^{p+1} + Y^{p+1} + Z^{p+1}) \subset \mathbb{P}^2_k. \tag{9.7.12}$$

Proof. In order to prove our statement we use properties of the left square of the Diagram 9.7.2, which is given by

$$\begin{array}{ccc} M_2 & \xleftarrow{M(\rho_2)} & M_1 \\ {\scriptstyle M(\eta_2)}\uparrow & & \uparrow{\scriptstyle M(\eta_1)} \\ M_2^t & \xrightarrow{M(\rho_2^t)} & M_1^t \end{array} \tag{9.7.13}$$

By Equation (9.7.15), the image of $M(\eta_2)$ is the multiplication by $[p]$-map, together with a flipping of the generators of any of the indecomposable $W(k)$-modules of M_2 in Equation 9.7.4.

We notice that the matrix representation of $M(\eta_2)$ in Equation (9.7.15) has its inverse in the quotient field $K = W(k)[\frac{1}{p}]$. This has the following consequence: For any element $n \in M_2$ where $n \in \mathrm{im}(M(\eta_2))$, there are unique elements $\widetilde{m}_2 \in M_2^t \otimes_{W(k)} K$ and $\widetilde{m} \in M_1^t$ respect the following commutative diagram

$$\begin{array}{ccc} n & \xleftarrow{M(\rho_2)} & n \\ {\scriptstyle M(\eta_2)}\uparrow & & \uparrow{\scriptstyle M(\eta_1)} \\ \widetilde{m}_2 & \xmapsto{M(\rho_2^t)} & \widetilde{m} \end{array} \tag{9.7.14}$$

and where $M(\rho_2) : M_1 \to M_2$ corresponds to the natural embedding induced by the identity-map. Therefore we can compute $\widetilde{m}_2$ for any $n \in M_2$ with this property by computing the inverse of A in Equation (9.7.7). Then $\widetilde{m}_2 = A^{-1}n$, where

$$A^{-1} = \begin{bmatrix} 0 & -p^{-1} & 0 & 0 & 0 & 0 \\ p^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -p^{-1} & 0 & 0 \\ 0 & 0 & p^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -p^{-1} \\ 0 & 0 & 0 & 0 & p^{-1} & 0 \end{bmatrix}. \tag{9.7.15}$$

By contravariant Dieudonné theory, the condition $\ker(\eta_1) \subset Y_1[F]$ is equivalent to

$$\mathrm{im}(M(F|_{M_1})) \subset \mathrm{im}(M(\eta_1)).$$

Consider the particular element

$$n = F(\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) = \underline{\alpha}^{\sigma} f_2 + \underline{\beta}^{\sigma} f_4 + \underline{\gamma}^{\sigma} f_6 \in \mathrm{im}(M(F|_{M_1})).$$

Then $n \in \mathrm{im}(M(\eta_1))$, and by the discussion above and after writing n as a vector we have

$$A^{-1}n = \begin{bmatrix} 0 & -p^{-1} & 0 & 0 & 0 & 0 \\ p^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -p^{-1} & 0 & 0 \\ 0 & 0 & p^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -p^{-1} \\ 0 & 0 & 0 & 0 & p^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \underline{\alpha}^{\sigma} \\ 0 \\ \beta^{\sigma} \\ 0 \\ \gamma^{\sigma} \end{bmatrix} = \begin{bmatrix} -p^{-1}\underline{\alpha}^{\sigma} \\ 0 \\ -p^{-1}\underline{\beta}^{\sigma} \\ 0 \\ -p^{-1}\underline{\gamma}^{\sigma} \\ 0 \end{bmatrix}$$

where

$$\widetilde{m}_2 = -\underline{\alpha}^{\sigma} f_1^* \otimes p^{-1} - \underline{\beta}^{\sigma} f_3^* \otimes p^{-1} - \underline{\gamma}^{\sigma} f_5^* \otimes p^{-1} \in M_2^t \otimes_{W(k)} K. \tag{9.7.16}$$

Then by the discussion above $\widetilde{m} = M(\rho_2^t)(\widetilde{m}_2)$ is an element in M_1^t and therefore fulfills the congruence relation

$$\underline{\alpha}^{\sigma+1} + \underline{\beta}^{\sigma+1} + \underline{\gamma}^{\sigma+1} \equiv 0 \pmod{p}. \tag{9.7.17}$$

With other words $P = [\alpha : \beta : \gamma]$ is a point on the Fermat curve $\mathcal{V}$ in Equation (9.7.12).

Conversely, assume that we are given a pftq of dimension 3 with respect to the polarization $\underline{\eta} = \eta_2$ and $\ker(\eta_2) = Y[F^2]$ (see Theorem 9.7.2). Further let $P' = [\alpha' : \beta' : \gamma'] \in \mathcal{V} \subset \mathbb{P}_k^2$ such that $\widetilde{M}$ is as a rank-6 $W(k)$-module generated by

$$\widetilde{M} = \langle \underline{\alpha}' f_1 + \underline{\beta}' f_3 + \underline{\gamma}' f_5, p f_1, f_2, p f_3, f_4, p f_5, f_6 \rangle.$$

Then by construction $(F, V)M_2 \subset \widetilde{M} \subset M_2$. Since M_2 is quasi polarized it induces a quasi polarization on $\widetilde{M}$ respecting the diagram in Equation (9.7.13).

To show is that $\mathrm{im}(M(F|_{\widetilde{M}})) \subset \mathrm{im}(M(\widetilde{\eta}) : \widetilde{M}^t \to \widetilde{M})$. Let $u = (\underline{\alpha}'^{\sigma} f_2 + \underline{\beta}'^{\sigma} f_4 + \underline{\gamma}'^{\sigma} f_6) \in \mathrm{im}(F|_{\widetilde{M}})$ and assume that $u \notin \mathrm{im}(M(\widetilde{\eta}))$. Then by the commutative diagram in Equation (9.7.14) $u \notin \mathrm{im}(M(\eta_2))$. Then there is no $\widetilde{m}_2 \in M_2^t \otimes_{W(k)} K$ as in Equation (9.7.16) such that $\widetilde{m}_2 = A^{-1}u$ and where $\widetilde{m}_2$ fulfills the congruence relation in Equation (9.7.17). But then $P' \notin \mathcal{V}$. This shows the claim. □

Corollary 9.7.14. *Let k be a algebraically closed field of $\mathrm{char}(k) = p > 0$. Let E be a supersingular elliptic curve over $k \supset \mathbb{F}_p$. Then, for any pftq of Dieudonné modules of genus 3 over $W(k)$ there is an equivalence between left $\mathcal{D}_k$-modules M_1 with $(F, V)M_2 \subset M_1 \subset M_2$ and points $P = [\alpha : \beta : \gamma]$ on the Fermat curve $\mathcal{V} \subset \mathbb{P}_k^2$.*

Proof. Follows from Proposition 9.7.11, Theorem 9.7.13, and similar arguments as in the proof of Theorem 9.6.14. □

Proposition 9.7.15. *There is a bijection between the set of isogenies $\{\rho_2 : Y_2 \to Y_1\}$ modulo equivalence and points on the Fermat curve $\mathcal{V} \subset \mathbb{P}_k^2$.*

Proof. By construction Y_1 is given by the projection $Y_1/\ker \rho_2$ for an isogeny ρ_2 with $\ker(\rho_2) \cong \alpha_p^2$ modulo equivalence. If M_1 is the Dieudonné module to Y_1 then by the discussion above M_1 is uniquely identified by a point $P \in \mathcal{V}$. Conversely any point on $\widetilde{P} \in \mathcal{V}$ corresponds to a submodule $\widetilde{M}$ with the property that $(F, V)M_2 \subset \widetilde{M} \subset M_2$. Then by contravariant Dieudonné theory $\widetilde{M}$ corresponds (up to isomorphism) to the Dieudonné module of a quotient $Y_2/\ker(\widetilde{\rho}_2)$. □

Some explicit bases for $M_1 = M(Y_1)$.

As we noticed in Proposition 9.7.11 as a $W(k)$-module of rank 6,

$$M_1 = \langle \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, pf_5, f_6 \rangle, \tag{9.7.18}$$

where $[\alpha : \beta : \gamma] \in \mathbb{P}^2_k$ is a point on the Fermat curve $\mathcal{V}$ in Equation (9.7.10) and where the latter uniquely identifies M_1. In order to identify the right square in Diagram 9.7.3, we choose in this section some explicit bases depending of the values of α, β and γ. More precisely, using the fact that $\mathcal{V} \subset \mathbb{P}^2_k$ together with an affine covering of $\mathbb{P}^2_k$ given by

$$U_x \cup U_y \cup U_z, \tag{9.7.19}$$

where U_x, U_y, U_z are the affine pieces of $\mathbb{P}^2_k$ with coordinates $x \neq 0$, $y \neq 0$ and $z \neq 0$ respectively, we consider affine pieces of $\mathcal{V}$ depending on the coordinate of their points.

Remark 9.7.16. In the following section, most of the proofs we will only treat for the case where $\alpha \neq 0$. The other cases are similar and we will skip them. We will no longer mention this explicitly.

Proposition 9.7.17. *Depending on which of the values of α, β, γ is nonzero, a $W(k)$-basis of M_1 is given by:*

$$\begin{aligned} &\text{if } \alpha \neq 0: && \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6. \\ &\text{if } \beta \neq 0: && \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, f_4, pf_5, f_6. \\ &\text{if } \gamma \neq 0: && \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, f_6. \end{aligned} \tag{9.7.20}$$

Proof. Since M_1 is a $W(k)$-module of rank 6, it is enough to show that in the first case pf_1, in the second case pf_3, and in the third case pf_5 are representable by a linear combinations in the generators with coefficients in $W(k)$. We have

$$\begin{aligned} pf_1 &= \underline{\alpha}^{-1}(p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) - \underline{\beta} \cdot pf_3 - \underline{\gamma} \cdot pf_5) \\ pf_3 &= \underline{\beta}^{-1}(p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) - \underline{\alpha} \cdot pf_1 - \underline{\gamma} \cdot pf_5) \\ pf_5 &= \underline{\gamma}^{-1}(p \cdot (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) - \underline{\alpha} \cdot pf_1 - \underline{\beta} \cdot pf_3). \end{aligned}$$

This shows the claim. □

Notation 9.7.18. For the rest of this section, we denote by

$$\begin{aligned} \mathcal{B}_\alpha &= (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6), && \text{if} \alpha \neq 0, \\ \mathcal{B}_\beta &= (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, f_4, pf_5, f_6), && \text{if} \beta \neq 0, \\ \mathcal{B}_\gamma &= (\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, f_6), && \text{if} \gamma \neq 0 \end{aligned}$$

the $W(k)$-bases of M_1 in Proposition 9.7.17.

Corollary 9.7.19. *For any of the $W(k)$-bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ and $\mathcal{B}_\gamma$ of M_1 in Notation 9.7.18, the matrix representations for $F = F|_{M_1}$ and $V = V|_{M_1}$ with respect to these bases is given by*

$$F = \begin{bmatrix} 0 & p\underline{\alpha}^{-1} & 0 & 0 & 0 & 0 \\ \underline{\alpha}^{\sigma} & 0 & 0 & 0 & 0 & 0 \\ 0 & -\underline{\beta}\underline{\alpha}^{-1} & 0 & 1 & 0 & 0 \\ \underline{\beta}^{\sigma} & 0 & p & 0 & 0 & 0 \\ 0 & -\underline{\gamma}\underline{\alpha}^{-1} & 0 & 0 & 0 & 1 \\ \underline{\gamma}^{\sigma} & 0 & 0 & 0 & p & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & p(\underline{\alpha}^{-1})^{\sigma} & 0 & 0 & 0 & 0 \\ \underline{\alpha} & 0 & 0 & 0 & 0 & 0 \\ 0 & -(\underline{\beta}/\underline{\alpha})^{\sigma} & 0 & 1 & 0 & 0 \\ \underline{\beta} & 0 & p & 0 & 0 & 0 \\ 0 & -(\underline{\gamma}/\underline{\alpha})^{\sigma} & 0 & 0 & 0 & 1 \\ \underline{\gamma}^{\sigma} & 0 & 0 & 0 & p & 0 \end{bmatrix}$$

$$F = \begin{bmatrix} 0 & 0 & 0 & p\underline{\beta}^{-1} & 0 & 0 \\ 0 & 0 & 1 & -\underline{\alpha}\underline{\beta}^{-1} & 0 & 0 \\ \underline{\alpha}^{\sigma} & p & 0 & 0 & 0 & 0 \\ \underline{\beta}^{\sigma} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\underline{\gamma}\underline{\beta}^{-1} & 0 & 1 \\ \underline{\gamma}^{\sigma} & 0 & 0 & 0 & p & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 0 & 0 & p(\underline{\beta}^{-1})^{\sigma} & 0 & 0 \\ 0 & 0 & 1 & -(\underline{\alpha}/\underline{\beta})^{\sigma} & 0 & 0 \\ \underline{\alpha} & p & 0 & 0 & 0 & 0 \\ \underline{\beta} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -(\underline{\gamma}/\underline{\beta})^{\sigma} & 0 & 1 \\ \underline{\gamma} & 0 & 0 & 0 & p & 0 \end{bmatrix}$$

$$F = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & p\underline{\gamma}^{-1} \\ 0 & 0 & 1 & 0 & 0 & -\underline{\alpha}\underline{\gamma}^{-1} \\ \underline{\alpha}^{\sigma} & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -\underline{\beta}\underline{\gamma}^{-1} \\ -\underline{\beta}^{\sigma} & 0 & 0 & p & 0 & 0 \\ \underline{\gamma}^{\sigma} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & p(\underline{\gamma}^{-1})^{\sigma} \\ 0 & 0 & 1 & 0 & 0 & -(\underline{\alpha}/\underline{\gamma})^{\sigma} \\ \underline{\alpha} & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & (\underline{\beta}/\underline{\gamma})^{\sigma} \\ \underline{\beta} & 0 & 0 & p & 0 & 0 \\ \underline{\gamma} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proof. Similar to the proof of Corollary 9.6.18. □

Proposition 9.7.20. *We have $M(\ker(F|_{M_1})) \cong k^3$ and $\ker(F|_{M_1}) \cong \alpha_p^3$.*

Proof. By contravariant Dieudonné theory $M(\ker(F|_{M_1}))$ is given by the exact sequence

$$0 \leftarrow M(\ker(F|_{M_1})) \leftarrow M_1 \xleftarrow{M(F|_{M_1})} M_1^{(p)} \leftarrow 0.$$

Since $\alpha \neq 0$, this implies that $\underline{\alpha} \in W(k)^\times$ and we may assume that $\underline{\alpha} = (1, 0, \ldots)$. Then we have

$$\begin{aligned} M(\ker(F|_{M_1})) &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle \mathrm{im}(M(F|_{M_1})) \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4 + \underline{\gamma}^{\sigma} f_6, pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2 + \underline{\beta}^{\sigma} f_4 + \underline{\gamma}^{\sigma} f_6, pf_3, f_4, pf_5, f_6 \rangle}{\langle f_2 + \underline{\beta}^{\sigma} f_4 + \underline{\gamma}^{\sigma} f_6, pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_4, f_6 \rangle}{\langle pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \langle [f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5], [f_4], [f_6] \rangle \\ &\cong (W(k)/(p))^{\oplus 3} \\ &\cong k^3. \end{aligned}$$

To prove the second claim we use the relations in Equation (9.7.20), in order to recognize that F and V are acting trivial on $M(\ker(F|_{M_1}))$. □

Remark 9.7.21. By the result above we can see that the dimensions of the k-vector space corresponds to the dimension of the abelian variety in Proposition 9.4.8.

The a-numbers, $a(M_1)$

We noticed in Corollary 9.7.14 and in Proposition 9.7.15, that *any* choice of an isogeny $(Y_2 = E^3, \eta_2) \xrightarrow{\rho_2} (Y_1, \eta_1)$ with $\alpha_p^2 \cong \ker(\rho_2) \subset Y_2[F]$ is equivalent to the choice of a point $P = [\alpha : \beta : \gamma]$ in $\mathbb{P}_k^2$ on the Fermat curve $\mathcal{V}$ in Equation (9.7.10). Theorem 9.7.22 and Corollary 9.7.42 describe the a-number $a(M_1)$ depending on the coordinates of P .

Theorem 9.7.22. *For any of the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ and $\mathcal{B}_\gamma$ of M_1 in Notation 9.7.18, we get that*

$$\frac{M_1}{(F,V)M_1} \cong k^\varepsilon$$

and where, up to permuting α, β and γ

$$\varepsilon = \begin{cases} 3, & \text{if and only if } \alpha \in \mathbb{F}_p^\times \text{ and } \beta, \gamma \in \mathbb{F}_{p^2}, \\ 2, & \text{if and only if } \alpha \in \mathbb{F}_p^\times \text{ and } \beta \notin \mathbb{F}_{p^2} \text{ or } \gamma \notin \mathbb{F}_{p^2}. \end{cases}$$

Proof. After a similar computation as in Proposition 9.7.20, we get that

$$\frac{M_1}{(F,V)M_1} = \frac{\langle \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle \underline{\alpha}^\sigma f_2 + \underline{\beta}^\sigma f_4 + \underline{\gamma}^\sigma f_6, \underline{\alpha}^{\sigma^{-1}} f_2 + \underline{\beta}^{\sigma^{-1}} f_4 + \underline{\gamma}^{\sigma^{-1}} f_6, pf_1, pf_4, pf_3, pf_6, pf_5 \rangle}.$$

Since the dimension of the k-vector space is independent of the chosen basis, we give a proof for the basis $\mathcal{B}_\alpha$ of M_1.

In comparison to Proposition 9.7.20, we get the extra condition $\underline{\alpha}^{\sigma^{-1}} f_2 + \underline{\beta}^{\sigma^{-1}} f_4 + \underline{\gamma}^{\sigma^{-1}} f_6 = 0$ coming from the Verschiebungsoperator V.

Since $\alpha \neq 0$ we may assume once again that $\underline{\alpha} = (1, 0, \ldots)$. Simplifying the first 2 conditions in the denominator gets a system of linear equation in matrix form given by

$$\left[\begin{array}{ccc|c} 1 & \underline{\beta}^\sigma & \underline{\gamma}^\sigma & 0 \\ 0 & (\underline{\beta}^\sigma - \underline{\beta}^{\sigma^{-1}}) & (\underline{\gamma}^\sigma - \underline{\gamma}^{\sigma^{-1}}) & 0 \end{array}\right].$$

The rank of the matrix above is equal to 1 if and only if $\underline{\beta}^{\sigma^2} = \underline{\beta}$ and $\underline{\gamma}^{\sigma^2} = \underline{\gamma}$. This is equivalent to the condition that $\beta, \gamma \in \mathbb{F}_{p^2}$. In this case

$$\begin{aligned} \frac{M_1}{(F,V)M_1} &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle f_2 + \underline{\beta}^\sigma f_4 + \underline{\gamma}^\sigma f_6, pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2 + \underline{\beta}^\sigma f_4 + \underline{\gamma}^\sigma f_6, pf_3, f_4, pf_5, f_6 \rangle}{\langle f_2 + \underline{\beta}^\sigma f_4 + \underline{\gamma}^\sigma f_6, pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_4, f_6 \rangle}{\langle pf_1, pf_4, pf_3, pf_6, pf_5 \rangle} \\ &\cong \langle [f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5], [f_4], [f_6] \rangle \\ &\cong k^3, \end{aligned}$$

where $\langle [f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5], [f_4], [f_6] \rangle \cong M(\ker(F|_{M_1}))$ as we showed in Proposition 9.7.20.

In the case where the rank of the matrix is 2, i.e. where up to permutation $\beta \in \mathbb{F}_{p^2}$, $\gamma \in k \setminus \mathbb{F}_{p^2}$, we get that

$$\frac{M_1}{(F,V)M_1} \cong \langle [f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5], [f_4] \rangle \cong k^2.$$

This shows the claim. □

Corollary 9.7.23. *With the same notation as in Theorem 9.7.22, we get that up to permuting α, β and γ,*

$$a(M_1) = \begin{cases} 2, & \text{if and only if } \beta/\alpha \notin \mathbb{F}_{p^2} \text{ or } \gamma/\alpha \notin \mathbb{F}_{p^2}, \\ 3, & \text{if and only if } \beta/\alpha, \gamma/\alpha \in \mathbb{F}_{p^2}. \end{cases}$$

Proof. Follows from Theorem 9.7.22 and from Definition 9.4.10, respectively. □

Lemma 9.7.24. *For any of the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ of M_1 in Notation 9.7.18, the matrix representation for $M(\rho_2) : M_1 \to M_2$ with respect to this bases is given by*

$$\begin{bmatrix} \underline{\alpha} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \underline{\beta} & 0 & p & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \underline{\gamma} & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \underline{\alpha} & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \underline{\beta} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \underline{\gamma} & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \underline{\alpha} & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \underline{\beta} & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ \underline{\gamma} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively.

Proof. Follows from the exact sequence

$$0 \leftarrow M(\ker(\rho_2)) \leftarrow M_2 \xleftarrow{M(\rho_2)} M_1 \leftarrow 0. \tag{9.7.21}$$

□

Lemma 9.7.25. *With the notation as in Lemma 9.7.24, we get that $M(\ker(\rho_2)) \cong k^2$ and $\ker(\rho_2) \cong \alpha_p^2$.*

Proof. By the exact sequence in Lemma 9.7.21 and the matrix representations for $A_{M(\rho_2)} = A_{M(\rho_2)}(\mathcal{B}_\alpha)$, we get that

$$M(\ker(\rho_2)) \cong \frac{M_2}{\operatorname{im}(M(\rho_2))} = \frac{\langle f_1, f_2, f_3, f_4, f_5, f_6 \rangle}{\langle \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, p f_3, f_4, p f_5, f_6 \rangle}.$$

Since $\alpha \neq 0$ this implies that $\underline{\alpha} \in W(k)^\times$ and we may assume that $\underline{\alpha} = (1, 0, \ldots)$. Then we have

$$M(\ker(\rho_2)) \cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, f_3, f_4, f_5, f_6 \rangle}{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, p f_3, f_4, p f_5, f_6 \rangle} \cong \langle [f_3], [f_5] \rangle \cong (W(k)/(p))^{\oplus_2} \cong k^2.$$

This shows the first claim.

Since F and V act trivially on $M(\ker(\rho_2))$ this shows our second claim. □

Remark 9.7.26. From Lemma 9.7.25, we can see that $\ker(\rho_2) \cong \alpha_p^2$ has the expected properties as in Definition 9.2.1.

We finish this section with the investigation of the affine group scheme $\ker(\eta_1 : Y_1 \to Y_1^t)$. See here also [46, Page 58].

Proposition 9.7.27. *With the notation as in Proposition 9.7.24, the matrix representations for $M(\eta_1) : M_1^t \to M_1$ with respect to the dual bases of M_1 are given by*

$$\begin{bmatrix} 0 & p\underline{\alpha}^{-1} & 0 & 0 & 0 & 0 \\ -p\underline{\alpha}^{-1} & 0 & \underline{\beta}\underline{\alpha}^{-1} & 0 & \underline{\gamma}\underline{\alpha}^{-1} & 0 \\ 0 & -\underline{\beta}\underline{\alpha}^{-1} & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -\underline{\gamma}\underline{\alpha}^{-1} & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & p\underline{\beta}^{-1} & 0 & 0 & 0 \\ 0 & 0 & 1 & -\underline{\alpha}\underline{\beta}^{-1} & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ -p\underline{\beta}^{-1} & \underline{\alpha}\underline{\beta}^{-1} & 0 & 0 & \underline{\gamma}\underline{\beta}^{-1} & 0 \\ 0 & 0 & 0 & -\underline{\gamma}\underline{\beta}^{-1} & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & p\underline{\gamma}^{-1} \\ 0 & 0 & 1 & 0 & 0 & -\underline{\alpha}\underline{\gamma}^{-1} \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -\underline{\beta}\underline{\gamma}^{-1} \\ 0 & 0 & 0 & -1 & 0 & 0 \\ -p\underline{\gamma}^{-1} & \underline{\alpha}\underline{\gamma}^{-1} & 0 & \underline{\beta}\underline{\gamma}^{-1} & 0 & 0 \end{bmatrix},$$

respectively.

Proof. Follows from the identification $A_{M(\eta_1)} = A_{M(\rho_2)}^{-1} A_{M(\eta_2)} (A_{M(\rho_2)}^t)^{-1}$, where $A_{M(\eta_2)} = A$ is the matrix representation for the pairing in Theorem 9.7.2, induced by the polarization η_2 on Y_2. □

Proposition 9.7.28. *We get that $M(\ker(\eta_1)) \cong k^2$ and $\ker(\eta_1) \cong \alpha_p^2$.*

Proof. In order to prove the statement we compute the so-called *Smith normal form* of $A_{M(\eta_1)}(\mathcal{B}_\alpha)$ (the dimension does not depend of the chosen basis). This provides matrices S, U and V such that $S = UFV$. Then, the columns of U^{-1} correspond to a new basis for M_1 in the image of $A_{M(\eta_1)}(\mathcal{B}_\alpha)$, where

$$U^{-1} = \begin{pmatrix} 0 & p\underline{\alpha}^{-1} & 0 & 0 & 0 & 0 \\ -p\underline{\alpha}^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \underline{\beta}\underline{\alpha}^{-1} & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -\underline{\gamma}\underline{\alpha}^{-1} & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

Then we get

$$M(\ker(\eta_1)) \cong \frac{\langle \underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle \mathrm{im}(M(\eta_1)) \rangle} \cong \langle [\underline{\alpha} f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5], [f_2] \rangle \cong (W(k)/(p))^{\oplus_2} \cong k^2.$$

Once again we can see that F, V are acting trivial on $M(\ker(\eta_1))$ which shows the second claim. □

The Dieudonné module $M_0 = M(Y_0)$.

For any of the bases $\mathcal{B}_\alpha, \mathcal{B}_\beta$ and $\mathcal{B}_\gamma$ of M_1 in Notation 9.7.18, we compute in this section the Dieudonné module M_0 as well as its a-numbers. We follow here [46, Chapter 9.3]. Let

$$(F,V)M_1 \subset M_0 \subset M_1 \tag{9.7.22}$$

be the right module chain in Equation (9.7.5), and let

$$\begin{array}{ccc} M_1 & \xleftarrow{M(\rho_1)} & M_0 \\ {\scriptstyle M(\eta_1)}\uparrow & & \uparrow{\scriptstyle M(\eta_0')} \\ M_1^t & \xrightarrow{M(\rho_1^t)} & M_0^t \end{array} \tag{9.7.23}$$

be the right square in Diagram 9.7.3. As in the previous sections, the module chain in Equation (9.7.22) induces the k-vector spaces

$$\frac{M_0}{(F,V)M_1} \subset \frac{M_1}{(F,V)M_1}.$$

In order to determine their dimension as k-vector spaces, we prove Lemma 9.7.29 and Proposition 9.7.30.

Lemma 9.7.29. *The map* $\tau : \dfrac{M_0}{(F,V)M_1} \to \dfrac{M_1}{M_0}$, *given by*

$$[m] \mapsto [M(\rho_1)(m)]$$

is the zero map on $\dfrac{M_1}{M_0}$.

Proof. Use the same arguments as in Lemma 9.7.8, after replacing by the corresponding quotients. □

Proposition 9.7.30. *There is a short exact sequence of k-vector spaces*

$$0 \to \frac{M_0}{(F,V)M_1} \xrightarrow{\iota} \frac{M_1}{(F,V)M_1} \xrightarrow{\pi} \frac{M_1}{M_0} \to 0$$

with $\tau = \pi \circ \iota$ in Lemma 9.7.29.

Proof. Use the same arguments as in Proposition 9.7.9, after replacing by the corresponding quotients. □

Depending on the exact sequence in Proposition 9.7.30 and the value

$$n := \dim_k\left(\frac{M_1}{(F,V)M_1}\right)$$

in Theorem 9.7.22, we prove the following.

Corollary 9.7.31. *We get that* $\dfrac{M_1}{M_0} \cong \dfrac{M_1/(F,V)M_1}{M_0/(F,V)M_1}$ *and* $\dim_k\left(\dfrac{M_1}{M_0}\right) = 1$, *and*

$$\dim_k\left(\frac{M_0}{(F,V)M_1}\right) = \begin{cases} 1, & \text{if } n = 2, \\ 2, & \text{if } n = 3. \end{cases}$$

Proof. The first statement follows from the third Isomorphism Theorem of modules.

The second statement follows from the isomorphism $\frac{M_1}{M_0} \cong M(\ker(\rho_1)) \cong k$. The latter isomorphism follows from the following arguments: By construction the polarization η_0 descends to a principal polarization. It induces an isomorphism $M(\eta_0) : M_0^t \to M_0$. Since by construction $M(\rho_1) : M_0 \to M_1$ is an embedding induced by the identity-map, the $\ker(\rho_1)$ is trivial, and as a k-vector space, the quotient is isomorphic to k. The dimension of the vector space $\frac{M_0}{(F,V)M_1}$ follows from the exact sequence in Proposition 9.7.30. □

Remark 9.7.32. In order to identify the Dieudonné module M_0 and its a-numbers, we do the following observation: We noticed in Proposition 9.7.30 and Corollary 9.7.31, that the dimension of the k-vector space $\frac{M_0}{(F,V)M_1}$ depends on the dimension of the k-vector space $\frac{M_1}{(F,V)M_1}$. By [46, Section 9.4], we know that for any $P \in \mathcal{V}$ which uniquely identifies M_1, the module M_0 corresponds to a unique point $[u : v] \in \mathbb{P}^1_k$ above P. In order to get this correspondence, we need another description of an exact sequence as in Proposition 9.7.30. This "new" description is independent of the latter dimension as a k-vector space. Together with this new exact sequence in Equation (9.7.25) and with Theorem 9.4.12, we will get a description of the Dieudonné module M_0.

Lemma 9.7.33. *We have*

$$\operatorname{im}(M(\eta_1)) = \left\{ \sum_{i=1}^{6} \omega_i f_i : \ \underline{\alpha}\omega_2 + \underline{\beta}\omega_4 + \underline{\gamma}\omega_6 \equiv 0 \pmod{p},\ \omega_1, \omega_3, \omega_5 \equiv 0 \pmod{p},\ \omega_i \in W(k) \right\}. \tag{9.7.24}$$

Proof. Follows from Theorem 9.7.13, the commutative diagrams in Equation 9.7.13 respectively 9.7.14, and the matrix representation of $M(\eta_2)$ in Equation 9.7.7. □

Corollary 9.7.34. *Depending of the values $\alpha, \beta, \gamma \neq 0$, $\operatorname{im}(M(\eta_1))$ is generated by:*

(i) If $\alpha \neq 0$: $pf_1, pf_2, pf_3, pf_4, pf_5, pf_6, -(\underline{\beta}/\underline{\alpha})f_2 + f_4, -(\underline{\gamma}/\underline{\alpha})f_2 + f_6$.

(ii) If $\beta \neq 0$: $pf_1, pf_2, pf_3, pf_4, pf_5, pf_6, f_2 - (\underline{\alpha}/\underline{\beta})f_4, -(\underline{\gamma}/\underline{\beta})f_4 + f_6$.

(iii) If $\gamma \neq 0$: $pf_1, pf_2, pf_3, pf_4, pf_5, pf_6, f_2 - (\underline{\alpha}/\underline{\gamma})f_6, f_4 - (\underline{\beta}/\underline{\gamma})f_6$.

Proof. Follows from Lemma 9.7.33. □

Proposition 9.7.35. *We have $(F,V)M_1 \subseteq \operatorname{im}(M(\eta_1))$, and with equality if for one (and therefore for any) basis $\mathcal{B}_\alpha, \mathcal{B}_\beta$ and $\mathcal{B}_\gamma$ of M_1, and up to permutation of the two other remaining variables after fixing a basis, one of them is in $\mathbb{F}_{p^2}$ and the other in $k \backslash \mathbb{F}_{p^2}$.*

Proof. Since $[\alpha : \beta : \gamma] \in \mathbb{P}^2_k$ is a point on the Fermat curve $\mathcal{V}$ identifying M_1, we have $FM_1 \subset \operatorname{im}(M(\eta_1))$ by Theorem 9.7.13.

In order to prove the first statement it remains to show that

$$V(\underline{\alpha}f_1 + \underline{\beta}f_3 + \underline{\gamma}f_5) = \underline{\alpha}^{\sigma^{-1}} f_2 + \underline{\beta}^{\sigma^{-1}} f_4 + \underline{\gamma}^{\sigma^{-1}} f_6 \in \operatorname{im}(M(\eta_1)).$$

Since $[\alpha : \beta : \gamma]$ is a point on $\mathcal{V}$, we get that $\alpha^{p+1} + \beta^{p+1} + \gamma^{p+1} \equiv 0 \pmod{p}$. But the latter congruence is equivalent to $\alpha^{1+\frac{1}{p}} + \beta^{1+\frac{1}{p}} + \gamma^{1+\frac{1}{p}} \equiv 0 \pmod{p}$ which proves the first stament.

In order to prove the second statement, we show that the dimensions of $\frac{M_1}{\mathrm{im}(M(\eta_1))}$ and $\frac{M_1}{(F,V)M_1}$ are equal as k-vector spaces. In Theorem 9.7.22 we noticed that the dimension of $\frac{M_1}{(F,V)M_1}$ is 2 if and only if up to permutation $\beta \in \mathbb{F}_{p^2}$ and $\gamma \in K \backslash \mathbb{F}_{p^2}$. Further, by the construction of pftq's (see Definition 9.2.1), the degrees of the morphisms respect the following commutative diagram

$$\begin{array}{ccccc} Y_2 & \xrightarrow{p^2} & Y_1 & \xrightarrow{p} & Y_0 \\ {\scriptstyle p^6}\downarrow & & {\scriptstyle p^2}\downarrow & & \downarrow{\scriptstyle 1} \\ Y_2^t & \xleftarrow[p^2]{} & Y_1^t & \xleftarrow[p]{} & Y_0^t \end{array}$$

where $p^6 = \deg(\eta_2)$, and $p^2 = \deg(\varrho_2), \deg(\varrho_2^t), \deg(\eta_1)$, and $p = \deg(\varrho_1), \deg(\varrho_1^t)$, and where $\deg(\eta_0) = 1$. By contravariant Dieudonné theory we get that

$$\dim_k\left(\frac{M_1}{\mathrm{im}(M(\eta_1))}\right) = \log(\deg(\eta_1)) = 2.$$

This shows the claim. □

Remark 9.7.36. By Proposition 9.7.35, there is a surjection $\pi : \frac{M_1}{(F,V)M_1} \to \frac{M_1}{\mathrm{im}(M(\eta_1))}$ induced by the identity-map. We identify $\frac{M_1}{(F,V)M_1}$ as a k-vector space in $\frac{M_1}{\mathrm{im}(M(\eta_1))}$ by π.

Lemma 9.7.37. *We chose the setup as in Corollary 9.7.34. For the case where $\alpha \neq 0$, we may assume that $\alpha = 1$. Then*

$$\frac{M_1}{\mathrm{im}(M(\eta_1))} \cong \langle [f_1 + \beta f_3 + \gamma f_5], [f_2] \rangle.$$

The same remain true after choosing $\beta, \gamma \neq 0$ in Corollary 9.7.34. In these cases the term $f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5$ will change to $\underline{\alpha} f_1 + f_3 + \underline{\gamma} f_5$, respectively to $\underline{\alpha} f_1 + \underline{\beta} f_3 + f_5$.

Proof. With Corollary 9.7.34, the generating system of M_1 in Equation (9.7.18), and the assumption on α, we get

$$\begin{aligned} \frac{M_1}{\mathrm{im}(M(\eta_1))} &= \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, pf_1, f_2, pf_3, f_4, pf_5, f_6 \rangle}{\langle pf_1, pf_2, pf_3, pf_4, pf_5, pf_6, -\underline{\beta} f_2 + f_4, -\underline{\gamma} f_2 + f_6 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2, f_4, f_6 \rangle}{\langle pf_1, pf_2, pf_3, pf_5, -\underline{\beta} f_2 + f_4, -\underline{\gamma} f_2 + f_6 \rangle} \\ &\cong \frac{\langle f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5, f_2 \rangle}{\langle pf_1, pf_2, pf_3, pf_5, \underline{\beta} f_2, \underline{\gamma\beta} f_2 \rangle} \\ &\cong \langle [f_1 + \beta f_3 + \gamma f_5], [f_2] \rangle \end{aligned}$$

which shows the claim. □

Remark 9.7.38. From Proposition 9.7.35 and Lemma 9.7.37, we get an exact sequence as in Proposition 9.7.30, given by

$$0 \to \frac{M_0}{\mathrm{im}(M(\eta_1))} \to \frac{M_1}{\mathrm{im}(M(\eta_1))} \to \frac{M_1}{M_0} \to 0. \tag{9.7.25}$$

Then

$$2 = \dim_k\left(\frac{M_1}{\mathrm{im}(M(\eta_1))}\right) = 1 + 1 = \dim_k\left(\frac{M_1}{M_0}\right) + \dim_k\left(\frac{M_0}{\mathrm{im}(M(\eta_1))}\right).$$

Proposition 9.7.39. *Let $M_2 \supset M_1 \supset M_0$ be a genus 3 pftq. For the point $P = [\alpha : \beta : \gamma] \in \mathcal{V}$ which uniquely identifies M_1, we get: If $\alpha \neq 0$ then as a $W(k)$-module of rank 6, M_0 is generated by*

$$\mathrm{im}(M(\eta_1)) + (\underline{u}(f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) + \underline{v} f_2) \tag{9.7.26}$$

where $[u : v] \in \mathbb{P}^1_k$, and where generators of $\mathrm{im}(M(\eta_1))$ are given in Corollary 9.7.34.

The same remain true after choosing $\beta, \gamma \neq 0$. In these cases the term $f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5$ in the representation of M_0 will change to $\underline{\alpha} f_1 + f_3 + \underline{\gamma} f_5$ respectively to $\underline{\alpha} f_1 + \underline{\beta} f_3 + f_5$.

Proof. Follows from Lemma 9.7.37, Theorem 9.4.12, and Lemma 9.7.37. □

Remark 9.7.40. In order to determine the a-numbers of M_0, we consider the pftq

$$(Y_2 = E^3, \eta_2) \xrightarrow{\rho_2} (Y_1, \eta_1) \xrightarrow{\rho_1} (Y_0, \eta_0) = (Y_2^{(p)}, \eta_0), \tag{9.7.27}$$

where $\ker(\rho_2) \cong \alpha_p^2$, $\ker(\rho_1) \cong \alpha_p$, and where $Y_0 = Y_2^{(p)}$ (see [46, Page 58]). There is an isogeny $\rho : Y_2 \to Y_0$ defined over $\mathbb{F}_{p^2}$ corresponding to the Frobenius F on Y_2, such that

$$F = \rho_2 \circ \rho_1,$$

and where $a(Y_2) = a(Y_0) = 3$. In other words, there are some points $[u : v] \in \mathbb{P}^1_k$, describing $M_0 = M(Y_0)$, and by following [46, Page 58] these points describe a section T of the map $\pi : \mathcal{P}_{3,\eta} \to \mathcal{V}$, given by

$$\mathcal{P}_{3,\eta} \supset T \xleftarrow[t]{\sim} \mathcal{V}, \tag{9.7.28}$$

where $\mathcal{P}_{3,\eta}$ is the moduli space of principally polarized flag type quotients of dimension 3 over k with respect to η, and where $t(\rho_2)$ correspond to pftq's as in Equation 9.7.27 for certain values of $[u : v] \in \mathbb{P}^1_k$ which we describe below. It should be clear from the discussion that under $t(\rho_2)$, we understand the point $[\alpha : \beta : \gamma] \in \mathcal{V}$ which uniquely identifies M_1, and $[u : v] \in \mathbb{P}^1_k$ which uniquely identifies M_0.

It remains to determine the a-numbers, $a(M_0)$ of

$$M_0 = \mathrm{im}(M(\eta_1)) + (\underline{u}(f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) + \underline{v} f_2).$$

In order to do this we need to prove Theorem 9.7.41. We will not do this in this thesis. I found out that some of my explicit calculations were incorrect. I will present this result elsewhere at a later date.

Theorem 9.7.41. *Let $M_0 = \mathrm{im}(M(\eta_1)) + (\underline{u}(f_1 + \underline{\beta} f_3 + \underline{\gamma} f_5) + \underline{v} f_2)$ be as in Proposition 9.7.39. Then:*

$$\dim_k\left(\frac{M_0}{(F,V)M_0}\right) = \begin{cases} 3, \text{ if } u = 0, \\ \geq 2, \text{ if } \beta, \gamma \in \mathbb{F}_{p^2}, \\ 1, \text{ if } u \neq 0 \text{ and } \beta \notin \mathbb{F}_{p^2} \text{ or } \gamma \notin \mathbb{F}_{p^2}. \end{cases}$$

Proof. See [46, Page 58]. □

The a-numbers $a(M_0)$

Corollary 9.7.42. *With the same notation as in Theorem 9.7.41, we get that up to permuting α, β and γ,*

$$a(M_0) = \begin{cases} 1, \text{ if and only if } u \neq 0 \text{ and } \beta/\alpha \notin \mathbb{F}_{p^2} \text{ or } \gamma/\alpha \notin \mathbb{F}_{p^2}, \\ \geq 2, \text{ if } \beta/\alpha, \gamma/\alpha \in \mathbb{F}_{p^2}, \\ 3, \text{ if } u = 0. \end{cases}$$

Proof. Follows from Theorem 9.7.41 and from Definition 9.4.10, respectively. □

The supersingular locus $\mathcal{S}_{3,1}$

As in the previous section, we denote by k an algebraically closed field of $\mathrm{char}(k) = p > 0$. For the rest of this section we fix a supersingular elliptic curve E over $k \supset \mathbb{F}_p$ with $F^2 + p = 0$ in $\mathrm{End}(E)$. In the previous sections we investigate the linear-algebraic data of pftq's of dimension 3 over k in terms of Dieudonné modules. In this section we briefly consider the *supersingular locus*. We give some relations between our explicit calculations in the previous sections the latter space.

Let $Y_1 = E^3$ be a supersingular abelian threefold over k. As in Section 9.6, we denote by Λ the set of equivalence classes of polarizations

$$\Lambda = \left\{ [\eta] : \eta : Y_1 \to Y_1^t,\ \ker(\eta) = Y_1[F] \right\} / \sim$$

where $[\eta] \sim [\eta']$ if there is an $\varphi \in \mathrm{Aut}_k(Y_1)$ such that $\eta' = \varphi^t \circ \eta \circ \varphi$.

As in Section 9.6, there is a relationship between the endomorphism algebra of the supersingular elliptic curve E and the cardinality of the set Λ. We briefly describe it. Let $\mathcal{B} = \mathbb{Q}_{p,\infty}$ be the definite quaternion $\mathbb{Q}$-algebra in Definition 9.1.2, ramified only at (p, ∞). By [46, Chapters 4 and 9], the set of equivalence classes of polarizations Λ is finite. Its cardinality is given by

$$\#\Lambda = H_3(p, 1),$$

where $H_3(p, 1)$ corresponds to the *class number of the principal genus* of positive definite quaternion hermitian space of dimension 3 over $\mathcal{B}$ (for the definition, see [35, 30]), and where $H_3(2, 1) = 1$ and $H_3(p, 1) > 1$ for all $p \geq 3$ (see [35, page 279]).

Definition 9.7.43. For any equivalence class of polarizations $[\eta] \in \Lambda$, we define by $\mathcal{P}'_{3,\eta}$ the *rigid moduli space of principally polarized flag type quotients of dimension* 3 *over* $\mathbb{F}_{p^2}$ *with respect to* η. We define by $S_{3,1}$ the *moduli space of supersingular principally polarized abelian threefolds* over k. It is the supersingular locus in the coarse moduli $\mathcal{A}_3$ of principally polarized abelian threefolds (see [46, Page 15]).

Remark 9.7.44. The authors in [46] define for general g, $\mathcal{P}_{g,\eta}$ as the moduli space of principally polarized flag type quotients of dimension g over $\mathbb{F}_{p^2}$, with the property that $\mathcal{P}'_{g,\eta} \subseteq \mathcal{P}_{g,\eta}$ for any g. In genus 3

$$\mathcal{P}'_{3,\eta} = \mathcal{P}_{3,\eta} \setminus T,$$

where T is the section of π in Equation (9.7.28).

There is a quasi-finite and surjective morphism defined over $\mathbb{F}_{p^2}$, given by

$$\Psi : \coprod_{[\eta]\in\Lambda} \mathcal{P}'_{3,\eta} \to \mathcal{S}_{3,1}$$
$$(Y_2 \xrightarrow{\rho_2} Y_1 \xrightarrow{\rho_1} Y_0) \mapsto (Y_0, \eta_0)$$

See [46, page 24]. By following [46, Corollary 4.4,] we get the following properties for $\mathcal{P}'_{3,\eta}$:

(i) It is non-singular, geometrically integral of dimension 2.

(ii) The generic fibre of Y_0 over $\mathcal{P}'_{3,\eta}$ is supergeneral.

Remark 9.7.45. In order to show that $\mathcal{P}_{3,\eta}$, is a *ruled surface* over the Fermat curve $\mathcal{V}$, we need to construct explicit transition functions for the restriction of the intersections of the affine pieces U_x, U_y, U_z to $\mathcal{V} \subset \mathbb{P}^2_k$ (see Equation 9.7.19). We skip this explicit computation and we refer to [46, Page 58].

Remark 9.7.46. By following [46, page 58] and the explicit computations in the previous sections of this chapter, we could convince ourselves (without an explicit computation of the transition functions (see Remark 9.7.45)), that $\mathcal{P}_{3,\eta}$ is a ruled surface over the Fermat curve $\mathcal{V}$, by the explicit computation of the modules M_0 (see Proposition 9.7.39), as well as their a-numbers (see Theorem 9.7.41). With these explicit computations we could convince ourselves that $\mathcal{P}_{3,\eta}$ is non-singular and irreducible as an abelian variety, as stated in [46, Chapter 4].

Remark 9.7.47. For $g \geq 4$, the space $\mathcal{P}_{g,\eta}$ is neither non-singular nor irreducible (see [46, Chapter 4]). As a future work in this area, I plan to study these spaces as well as the linear-algebraic data for these cases.

Appendices

A Group Schemes

This chapter is intended solely as a service for the reader. We discuss some basic properties of (affine) group schemes. For a detailed discussion about affine group schemes, we refer to [78], [27, Appendix A], respectively [76, Chapter 4.4]. For a detailed discussion about group schemes see e.g. [76, Chapter 3-4].

We denote by k an algebraically closed field of arbitrary characteristic. Let S be a scheme. A *group scheme* over S is an S-scheme $\pi : G \to S$ together with S-morphisms

$$\mathrm{inv} : G \to G, \qquad m : G \times_S G \to G, \qquad e : S \to G$$

respecting the following diagrams

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m\times\mathrm{id}} & G \times_S G \\ {\scriptstyle \mathrm{id}\times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(e\circ\pi,\mathrm{id})} & G \times_S G \\ {\scriptstyle (\mathrm{id},e\circ\pi)}\downarrow & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(\mathrm{inv},\mathrm{id})} & G \times_S G \\ {\scriptstyle (\mathrm{id},\mathrm{inv})}\downarrow & \searrow^{e\circ\pi} & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G. \end{array}$$

We call G a *commutative group scheme* over S if the following diagram commutes

$$\begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle s}\downarrow & \nearrow_{m} & \\ G \times_S G & & \end{array}$$

where the isomorphism s is switching the two factors. A group scheme G over S is called *finite* and *flat* if the morphism π is finite and flat. See [27, Appendix A].

A.1 p-Divisible Groups

In order to handle the p-torsion phenomena in characteristic $p > 0$, the main tools we consider in this thesis are p-divisible groups of abelian varieties and Dieudonné modules. For a definition of the latter and their relation to the former, see Chapter 9.

A *p-divisible group of height $h \geq 0$* over a base scheme S is an inductive system

$$G = (G_n)_{n\in\mathbb{N}}, \tag{A.1.1}$$

of finite flat commutative group schemes G_n over S, of order $(p^n)^h$, together with group scheme homomorphisms $i_n : G_n \to G_{n+1}$, where G_n is identified with $G_{n+1}[p^n]$ for all n. Cartier duality in Equation (A.1.1) gives rise to the *Serre dual of G*, a p-divisible group over S of height h given by the inductive system

$$G^D := (G_n^D)_{n\in\mathbb{N}},$$

where for all n there are group schemes isomorphisms $(D_n^D)^D \xrightarrow{\sim} G_n$, which induces an isomorphism of p-divisible groups $(G^D)^D \xrightarrow{\sim} G^D$. See [11, page 39].

Definition A.1.1. Let p be a prime number and let A be an abelian variety of dimension $g \geq 1$ over k. The p-divisible group of A of height $2g$ is a group scheme over S given by an inductive system of the form

$$A[p^\infty] := (A[p^n])_{n\geq 0}.$$

B

Affine Group Schemes

In what follows we shall assume all our group schemes to be finite, commutative, and flat. For a detailed introduction in affine group schemes we refer to [78].

Definition B.0.1. A group scheme $\pi : G \to S$ over a base scheme S is called *affine* if the morphism π is affine.

Remark B.0.2. Is the scheme S covered by open affine sets $U = \mathrm{Spec}(R)$, then π affine if $G \times_S U$ is affine and of the form $\mathrm{Spec}(R[x_1, \ldots, x_r]/I)$. In this case affine group schemes are characterized by their Hopf algebras.

Definition B.0.3. Let $G = \mathrm{Spec}(A)$ be an affine group scheme over S represented by the Hopf algebra A. Its Cartier dual $G^D = \mathrm{Spec}(A^D)$ is an affine group scheme over S represented by the dual Hopf algebra A^D. See [60, page 9].

Example B.0.4. Let $\mathbb{G}_a = \mathbb{G}_{a,k} := \mathrm{Spec}(k[x])$ be the *additive group over k* equipped with a Hopf algebra structure given by

$$\begin{aligned} &\widetilde{m} : k[x] \to k[x] \otimes_k k[x], && x \mapsto x \otimes 1 + 1 \otimes x. \\ &\widetilde{i} : k[x] \to k[x], && x \mapsto -x. \\ &\widetilde{e} : k[x] \to k, && x \mapsto 0. \end{aligned}$$

See [76, Example 3.8].

Example B.0.5. Let $\mathbb{G}_m = \mathbb{G}_{m,k} := \mathrm{Spec}(k[x, x^{-1}])$ be the *multiplicative group over k* equipped with a Hopf algebra structure given by

$$\begin{aligned} &\widetilde{m} : k[x] \to k[x] \otimes_k k[x], && x \mapsto x \otimes x. \\ &\widetilde{i} : k[x] \to k[x], && x \mapsto x^{-1}. \\ &\widetilde{e} : k[x] \to k, && x \mapsto 1. \end{aligned}$$

See [76, Example 3.8].

Definition B.0.6. Let $G = \mathrm{Spec}(A)$ be an affine group scheme over a base scheme S. A *sub affine group scheme* $H \subseteq G$ is an affine group scheme which is a closed subscheme of G compatibly with the Hopf algebra structure of A.

Example B.0.7. Let p be a prime number and let $\mathbb{G}_{a,k}$ be the additive group over k. Then

$$\alpha_p = \alpha_{p,k} := \mathrm{Spec}(k[x]/(x^p)) \subset \mathbb{G}_a$$

is a sub affine group scheme corresponding to $\ker(F : \mathbb{G}_a \to \mathbb{G}_a)$, and where the Hopf algebra structure of α_p is inherited from the Hopf algebra structure of $\mathbb{G}_a$. By [60, page 11], as an affine group schemes the Cartier dual $\alpha_p^D \cong \alpha_p$.

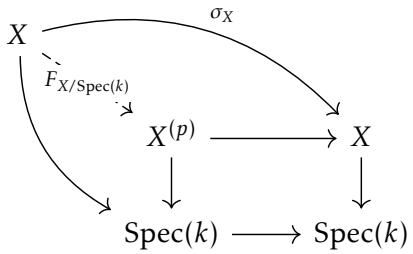
Let $S = \mathrm{Spec}(k)$ and let $f : X \to \mathrm{Spec}(k)$ be a scheme over $\mathrm{Spec}(k)$ where

$$X = \mathrm{Spec}(k[x_1, \ldots, x_n]/(f_1, \ldots, f_m))$$

with polynomials $f_i \in k[x_1,\dots,x_n]$. After [76, page 3-5], the *fibre product* $X^{(p)}$ is a scheme over $\mathrm{Spec}(k)$, where

$$X^{(p)} = \mathrm{Spec}(k[x_1,\dots,x_n]/(f_1^p,\dots,f_m^p)).$$

The *relative Frobenius* morphism $F_{X/\mathrm{Spec}(k)}$ induces the following diagram



(B.0.1)

where $\sigma_X : X \to X,\ a \mapsto a^p$ is the *absolute Frobenius* on sections of $\mathcal{O}_X$.

If X^D is the *Cartier dual* of X, then after [76, Definition 5.18], the relative Frobenius $F_{X/\mathrm{Spec}(k)}$ induces a dual homomorphism

$$(F_{X/\mathrm{Spec}(k)})^D : X^D \to (X^{(p)})^D \cong (X^D)^{(p)}.$$

Definition B.0.8. The homomorphism $V_{X^{(p)}/\mathrm{Spec}(k)} : X^{(p)} \to X$ dual to $F_{X/\mathrm{Spec}(k)}$ is called the *Verschiebung* morphism on $X^{(p)}$, respecting the relations

$$V_{X^{(p)}/\mathrm{Spec}(k)} \circ F_{X/\mathrm{Spec}(k)} = p \cdot \mathrm{id}_X,$$
$$F_{X/\mathrm{Spec}(k)} \circ V_{X^{(p)}/\mathrm{Spec}(k)} = p \cdot \mathrm{id}_{X^{(p)}}.$$

See [76, Proposition 5.19].

Remark B.0.9. If X is an abelian variety of dimension g over k, then the relative Frobenius $F_{X/k}$ and the Verschiebung $V_{X^{(p)}/k}$ morphisms are purely inseparable isogenies of degree p^g respecting the relations $V_{X^{(p)}/k} \circ F_{X/k} = [p] \cdot \mathrm{id}_X$ and $F_{X/k} \circ V_{X^{(p)}/k} = [p] \cdot \mathrm{id}_{X^{(p)}}$. See [76, Proposition 5.15, 5.20].

Remark B.0.10. Let H be an affine group scheme over $\mathrm{Spec}(k)$. The Frobenius morphism

$$F_{H/\mathrm{Spec}(k)} : H \to H^{(p)}$$

induces by Cartier duality the Verschiebung morphism

$$V_{H^{(p)}/\mathrm{Spec}(k)} : H^{(p)} \to H,$$

with respect to the relations

$$V_{H^{(p)}/\mathrm{Spec}(k)} \circ F_{H/\mathrm{Spec}(k)} = p \cdot \mathrm{id}_H,$$
$$F_{H/\mathrm{Spec}(k)} \circ V_{H^{(p)}/\mathrm{Spec}(k)} = p \cdot \mathrm{id}_{H^{(p)}}.$$

See [60, Theorem 14.4].

If $G = (H_n)_{n\in\mathbb{N}}$ is a p-divisible group over $\mathrm{Spec}(k)$, then by the inductive construction of G, H_n induces the Frobenius and Verschiebung homomorphisms on G.

Definition B.0.11. Let G be an affine group scheme over $\mathrm{Spec}(k)$. We call G *étale* if the structural morphism π is étale.

Remark B.0.12. A flat morphism of schemes $f : X \to Y$ is called *étale at* $x \in X$, if for $y = f(x)$ the homomorphism of local rings, $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ verifies $\mathfrak{m}_y \mathcal{O}_{X,x} = \mathfrak{m}_x$, and if the finite extension of residue fields $k(y)$ over $k(x)$ is separable. We call f *étale* if f is étale at every $x \in X$.

Proposition B.0.13. *If k is a field of characteristic 0, then any affine group scheme over k is étale.*

Proof. See [60, Theorem 13.2]. □

Definition B.0.14. Let G be an affine group scheme over $\mathrm{Spec}(k)$ and let G^0 be the connected component of the zero section in G. Then G^0 is a closed subgroup scheme in G and we call G *local* if $G = G^0$. See [60, page 32-33].

Theorem B.0.15. *Any affine group scheme G over* $\mathrm{Spec}(k)$ *splits canonically into four factors*

$$G \cong G^{\text{é-é}} \times G^{\text{é-c}} \times G^{\text{c-é}} \times G^{\text{c-c}}$$

with $G^{\text{é-é}}$ corresponding to the étale with étale dual part, $G^{\text{é-c}}$ corresponding to the étale with connected dual part, $G^{\text{c-é}}$ corresponding to the connected with étale dual part, and $G^{\text{c-c}}$ corresponding to the connected with connected dual part of G.

Proof. See [76, page 68]. □

B.1 α-Groups and a-Numbers

In this section we define the *alpha group* of an commutative group scheme G over an algebraically closed field k of $\mathrm{char}(k) = p > 0$.

Definition B.1.1. An affine group scheme G over S is called an α-group scheme if G is of p-power order, and

$$\begin{aligned} \ker\left(F_{G/k} : G \to G^{(p)}\right) &= 0, \\ \ker\left(V_{G/k} : G^{(p)} \to G\right) &= 0. \end{aligned}$$

Proposition B.1.2. *Any affine commutative group scheme G over k is an α-group scheme if and only if $G \cong (\alpha_p)^r$ for some positive integers r.*

Proof. See [11, Proposition 3.1.10]. □

Definition B.1.3. Let G be a commutative group scheme over k. The a-number of G is defined as

$$a(G) = \dim_k(\mathrm{Hom}(\alpha_p, G)).$$

Lemma B.1.4. *For any p-divisible group G over k, the a-numbers $a(G)$ and $a(G^t)$ are equal.*

Proof. See [11, Corollary 3.2.4]. □

Bibliography

[1] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

[2] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. Genus 3. `https://github.com/christellevincent/genus3`, 2016.

[3] H. U. Besche, B. Eick, and E. O'Brien. The GAP Small Groups Library. Database available at `https://www.gap-system.org/Packages/smallgrp.html`, 2019.

[4] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004.

[5] S. J. Bloch, editor. *Algebraic Geometry - Bowdoin 1985, Part 1. Proceedings of Symposia in Pure Mathematics*, volume 46. American Mathematical Society, 1987.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[7] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, and E. Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in numbers Europe*, volume 2 of *Assoc. Women Math. Ser.*, pages 109–151. Springer, Cham, 2015.

[8] F. Bouyer and M. Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.

[9] R. Bröker, D. Gruenewald, and K. Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra Number Theory*, 5(4):495–528, 2011.

[10] Diem C. An index calculus algorithm for plane curves of small degree. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 543–557. Springer, 2006.

[11] C.-L. Chai, B. Conrad, and F. Oort. *Complex Multiplication and Lifting Problems*. American Mathematical Society, 2010.

[12] C.-L. Chai and F. Oort. Abelian varieties isogenous to a Jacobian. *Annals of Mathematics*, 176(1):589–635, 2012.

[13] H. Cohen. *Advanced topics in computational number theory*. Springer-Verlag, New York, 1991.

[14] E. Costa, N. Mascot, and J. Sijsling. Rigorous computation of the endomorphism ring of a Jacobian. `https://github.com/edgarcosta/endomorphisms/`, 2017.

[15] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[16] D. A. Cox. *Primes of the form $x^2 + ny^2$*, volume 2. Wiley, 2012.

[17] B. Dina and S. Ionica. Genus 3 hyperelliptic curves with CM via Shimura reciprocity. *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), Mathematical Sciences Publishers, Berkeley, 2020*, pages 161–178, 2020.

[18] B. Dina, S. Ionica, and J. Sijsling. `cm-calculations`, a Magma package for calculating with CM curves. https://github.com/JRSijsling/cm-calculations, 2021.

[19] B. Dina, S. Ionica, and J. Sijsling. Isogenous hyperelliptic and non-hyperelliptic jacobians with maximal complex multiplication. arxiv:2104.04519, 2021.

[20] B Dodson. The structure of Galois groups of CM-fields. *Trans. Amer. Math. Soc.*, 283(1), May 1984.

[21] A.-S. Elsenhans. Good models for cubic surfaces. Preprint available at `https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf`.

[22] A. Enge and E. Thomé. Computing class polynomials for abelian surfaces. *Experimental Mathematics*, 23(2):129–145, 2014.

[23] J.-M. Fontaine. Groupes p-divisibles sur les corps locaux. *Société mathématique de France*, 498610(47–48), 1977.

[24] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic cm method for genus 2 curves with application to cryptography. In *ASIACRYPT*, pages 114–129, 2006.

[25] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comput.*, 76(257):475–492, 2007.

[26] E. Girondo and G. González-Diez. *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*. Cambridge University press, 2012.

[27] Eyal Z. Goren. *Lectures on Hilbert Modular Varieties and Modular Forms*, volume 14. American Mathematical Society, 2002.

[28] J. Hanselman. *Gluing curves of genus 2 and genus 1 along their 2-torsion*. PhD thesis, Universität Ulm, 2020.

[29] M. Hindry and J. Silverman. *Diophantine Geometry An Introduction*. Springer, 1991.

[30] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compos. Math.*, 57(2):127–152, 1986.

[31] J.-i. Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[32] S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, A. Mânzăţeanu, and C. Vincent. Counting multiplicities for primes of bad reduction for genus 3 curves. Unpublished manuscript, 2021.

[33] S. Ionica, P. Kılıçer, K. E. Lauter, E. Lorenzo García, A. Mânzăţeanu, M. Massierer, and C. Vincent. Modular invariants for genus 3 hyperelliptic curves. *Research in Number Theory*, 5:1–22, 2018.

[34] D. Jetchev and B. Wesolowski. Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem. *Acta Arithmetica*, 187(4):381–404, 2019.

[35] T. Katsura and F. Oort. Supersingular abelain varieties of dimension two or three and class numbers. *Advanced Studies in Pure Mathematics*, (10):253–281, 1987.

[36] B. Klingler and A. Yafaev. The André-Oort conjecture. *Annals of Mathematics*, 180:867–925, 2014.

[37] P. Kılıçer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arith.*, 185(2):127–156, 2018.

[38] Hugo Labrande. Computing Jacobi's theta in quasi-linear time. *Math. Comp.*, 87(311):1479–1508, 2018.

[39] S. Lang. *Complex Multiplication*. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1983.

[40] J.-C. Lario and C.) Somoza, A. (appendix by Vincent. An inverse Jacobian algorithm for Picard curves. `https://arxiv.org/pdf/1611.02582.pdf`, 2020.

[41] R. Lercier, Q. Liu, E. Lorenzo García, and C. Ritzenhaler. Reduction type of smooth plane quartics. *Algebra & Number Theory*, 2020.

[42] R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.

[43] R. Lercier, C. Ritzenthaler, and J. Sijsling. Reconstructing plane quartics from their invariants. *Discrete Comput. Geom.*, 63(1):73–113, 2020.

[44] R. Lercier, C. Ritzenthaler, and J. Sijsling. `hyperelliptic`, a Magma package for reconstruction and isomorphisms of hyperelliptic curves. `https://github.com/JRSijsling/hyperelliptic`, 2021.

[45] R. Lercier, C. Ritzenthaler, and J. Sijsling. `quartic`, a Magma package for calculating with smooth plane quartic curves. `https://github.com/JRSijsling/quartic`, 2021.

[46] K.-Z. Li and F. Oort. *Moduli of Supersingular Abelian Varieties*. Springer, 1998.

[47] D. Lombardo, E. Lorenzo García, C. Ritzenthaler, and J. Sijsling. Decomposing jacobians via galois covers. Preprint available at arXiv:2003.07774, to appear in Exp. Math., 2020.

[48] E. Lorenzo García. On different expressions for invariants of hyperelliptic curves of genus 3. https://arxiv.org/pdf/1907.05776.pdf, to appear in *Journal of the Mathematical Society of Japan*, 2019.

[49] J. S. Milne. Abelian varieties. `www.jmilne.org/math/`, 2008.

[50] R. Miranda. *Algebraic Curves and Riemann Surfaces*, volume 5. American Mathematical Society, 2000.

[51] P. Molin and C. Neurohr. Computing period matrices and the Abel-Jacobi map of superelliptic curves. *Math. Comp.*, 88(316):847–888, 2019.

[52] B. Moonen and F. Oort. The Torelli locus and special subvarieties. In *Handbook of Moduli*, volume II, pages 549–594. International Press, 2013.

[53] D. Mumford. *Abelain Varieties*. Oxford University Press, Oxford, 1985.

[54] D. Mumford. *Tata lectures on theta. I*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007.

[55] D. Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[56] M. Newman. *Integral matrices*, volume 45 of *Pure and Applied Mathematics*. Academic Press, 1972.

[57] F. Oort and K. Ueno. Principally polarized abelian variaties dimension two or three are jacobian varieties. 1973.

[58] Andreas Pieper. Constructing all genus 2 curves with supersingular jacobian, 2021.

[59] J. Pila and J. Tsimerman. Ax-Lindemann for $\mathcal{A}_g$. *Annals of Mahematics*, 179:659–681, 2014.

[60] R. Pink. Finite group schemes.

[61] C. Poor. The hyperelliptic locus. *Duke Math. J.*, 76(3):809–884, 1994.

[62] S. Roman. *Advanced Linear Algebra*. Springer-Verlag, 1997.

[63] G. Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[64] T. Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967.

[65] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 2 of *Graduate Texts in Mathematics*. Springer, 2000.

[66] B. A. Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 163–180. Springer, 2008.

[67] M. Stoll. Reduction theory of point clusters in projective space. *Groups Geom. Dyn.*, 5(2):553–565, 2011.

[68] M. Stoll and J. E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.

[69] M. Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Leiden, 2010.

[70] M. Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.

[71] M. Streng. An explicit version of Shimura's reciprocity law for siegel modular functions. https://arxiv.org/abs/1201.0020, 2018.

[72] K. Takase. A generalization of Rosenhain's normal form for hyperelliptic curves with an application. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(7):162–165, 1996.

[73] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 30 October 2019].

[74] J. Tsimerman. The André-Oort conjecture for $\mathcal{A}_g$. *Annals of Mathematics*, 187:379–390, 2018.

[75] S. Tsuyumine. On the Siegel modular field of degree 3. *Compos. Math.*, 63(1):83..98, 1987.

[76] G. van der Geer and B. Moonen. Abelian varieties. Unpublished manuscript available at `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`, 2020.

[77] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[78] W. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, 1979.

[79] A. Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.

Zusammenfassung in deutscher Sprache

Überblick

Diese Arbeit befasst sich mit der algorithmischen Konstruktion von Gleichungen algebraischer Kurven von Geschlecht 2 und 3. Ausgehend von ihren hauptpolarisierten Abelschen Varietäten bestimmen wir mit Hilfe des Computers (numerische) Invarianten der Kurven. Diese entsprechen (approximationen) algebraischen Zahlen, mit denen wir eine explizite Gleichung der Kurven darstellen.

Im ersten Hauptteil dieser Arbeit, welches die Kapitel 7 und 8 umfasst, beschäftigen wir uns mit der Konstruktion von Gleichungen algebraischer Kurven von Geschlecht 3 mit komplexen Multiplikation. Wir beschreiben und implementieren Algorithmen für die Konstruktion von hauptpolarisierten Abelschen Varietäten von Diemension 3 über $\mathbb{C}$. Wir geben in einem bestimmten Fall explizite Gleichungen von Kurven von Geschlecht 3 über Zahlkörper an.

Im zweiten Hauptteil dieser Arbeit, welches das Kapitel 9 umfasst, befassen wir uns mit der Theorie von supersingulären polarisierten Abelschen Varietäten in Charakteristik $p > 0$. Wir geben eine explizite Version einiger Ergebnisse von Li–Oort [46] über den Modulraum hauptpolarisierter, supersingulärer Abelscher Varietäten der Dimension 2 und 3. Unsere Version der Ergebnisse von Li–Oort machen diese leichter nutzbar für algorithmische Anwendungen.

Inhalt

Es ist bekannt, dass es im Fall $g = 3$ zwei Arten von algebraischen Kurven gibt, nämlich hyperelliptische und nicht-hyperelliptische Kurven von Geschlecht 3. Unser Ziel ist es, eine Gleichung der Kurve über dem „kleinstmöglichen“ Zahlenkörper und nicht nur über $\mathbb{C}$ zu finden. Der entscheidende Schritt ist hier, Invarianten der Kurve zu finden. Im hyperelliptischen Fall betrachten wir die Rosenhain- und Shioda-Invarianten. Im nicht-hyperelliptischen Fall verwenden wir stattdessen die Dixmier-Ohno-Invarianten. Zur Bestimmung der Invarianten einer Kurve X betrachten wir die Jacobische $\mathrm{Jac}(X)$ von X.

Sei K ein CM-Körper von Grad 6. Dann ist K eine rein-imaginäre quadratische Erweiterung eines total-reellen Zahlkörpers. Die Jacobische $\mathrm{Jac}(X)$ einer Kurve X mit CM ist ein hauptpolarisierte Abelsche Varietät, die die durch ein Tripel

$$(\Phi, \mathfrak{a}, \xi)$$

beschrieben werden kann. Hier sind Φ ein primitiver CM-Typ auf K, $\mathfrak{a}$ ein gebrochenes $\mathcal{O}_K$-ideal, und ξ ein Element in K mit einigen zusätzlichen Eigenschaften, was eine Riemann Form auf dem Gitter $\Phi(\mathfrak{a})$ induziert. Ausgehend von solchen Tripeln $(\Phi, \mathfrak{a}, \xi)$ bestimmen wir (numerische) Invariante von Kurven.

Teile dieser Arbeit (genauer gesagt, das Kapitel 7) wurden motiviert durch folgende Fragestellung: Gibt es CM-Körper von Grad 6, für die es (nicht-)hyperelliptische Jacobische der Dimension 3 mit CM durch die Maximalordnung dieses Körpers gibt? Ein solcher CM-Körper war bereits vor dieser Arbeit bekannt.

Die wichtigsten Ergebnisse in Kapitel 7 werden gegeben durch:

In Theorem 7.2.1 zeigen wir: Heuristisch gibt es 14 CM-Körper K von Grad 6, für die es sowohl eine hyperelliptische als auch eine nicht-hyperelliptische Kurve gibt, deren Jacobische CM mit der maximalen Ordnung $\mathcal{O}_K$ von K hat. Alle diese Körper haben die Galoisgruppe

$$\mathrm{Gal}(K|\mathbb{Q}) \simeq C_2^3 \rtimes S_3.$$

Es ist bekannt, dass der Hyperelliptische Ort von Dimension 5 ist im Modulraum der Kurven von Geschlecht 3. Da dieser Dimension 6 hat, ist es unwahrscheinlich dass eine zufällig gewählte Kurve hyperelliptisch ist.

Wir zeigen in Theorem 7.2.3, dass es heuristisch, einschließlich der in Theorem 7.2.1 erwähnten Körper, 3.422 CM-Körper K, für die es eine hyperelliptische Kurve gibt, deren Jacobische CM mit der maximalen Ordnung $\mathcal{O}_K$ von K hat. Von diesen Körpern haben 348 (bzw. 3.057 bzw. 17) eine Galoisgruppe isomorph zu C_6 (bzw. D_6 bzw. $C_2^3 \rtimes S_3$). Wir haben $\mathbb{Q}(i) \subset K$ für alle außer 19 dieser Körper K. Unter den Ausnahmefällen haben 2 (bzw. 17) eine Galoisgruppe isomorph zu C_6 (bzw. $C_2^3 \rtimes S_3$).

Wir beweisen in Theorem 7.2.6 auch eine explizite Version von Theorem 7.2.1: Für den CM-Körper K mit kleinster absoluter Diskriminante unter den Körpern aus Theorem 7.2.1, definiert durch das Polynom $t^6 + 10t^4 + 21t^2 + 4$, bestimmen wir die Gleichungen (7.2.1) und (7.2.2) einer hyperelliptischen Kurve X und einer nicht-hyperelliptischen Kurve Y mit $\mathrm{Jac}(X)$ und $\mathrm{Jac}(Y)$, beide mit CM mit $\mathcal{O}_K$. Außerdem existiert heuristisch eine Isogenie vom Grad 2 zwischen $\mathrm{Jac}(X)$ und $\mathrm{Jac}(Y)$.

In Kapitel 8 betrachten die Rosenhain-Invarianten hyperelliptischer Kurven von Geschlecht 3 mit CM. Mit ihrer Hilfe, und dem Shimura Reziprozitätsgesetz bestimmen wir so genannte Rosenhain-Klassenpolynome.

Das Hauptergebnis aus dem Kapitel 8 dieser Dissertation ist das Theorem 8.5.9 welches, gegeben eine Jacobische $\mathrm{Jac}(X)$ einer ausgezeichneten hyperelliptischen Kurve X von Geschlecht 3 über $\mathbb{C}$ mit CM durch die Maximalordnung $\mathcal{O}_K$ eines CM-Körpers K, bestimmen wir mittels Shimura Reziprozitätsgesetz eine Approximation der galoiskonjugierten Rosenhain-Invarianten von X.

Die Beschreibungen in Kapitel 9 dienen als Einstieg und Vorbereitung in die Theorie der supersingulären polarisierten abelschen Varietäten der Dimension g über Körper in positiver Charakteristik. In diesem Kapitel führen wir die Konstruktion der so genannten polarized flag type quotients (pftq's) ein. Im Hauptteil dieses Kapitels beschreiben wir explizit die Lineare-Algebra-Struktur, die sich auf die endlichen kommutativen Gruppenschemata von pftqs der Dimension 2 und 3 beziehen. Die explizite Beschreibung von pftqs unter Verwendung von Lineare Algebra-Objekte ermöglicht die Beantwortung algorithmischer Fragestellungen in diesem Bereich.

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich die Arbeit selbstständig angefertigt habe und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht habe.

Ulm, den 05. August 2021

.....

Bogdan Adrian Dina

Personal Details

Name	Bogdan Adrian Dina
Birth	1978, Hunedoara, Romania
Nationality	German, Romanian

Education

since 2021	**PhD Student**, *Universität Ulm*, Under Prof. Dr. Irene Ingeborg Bouw.
2016–2021	**Research Assistant**, *Institut für Theoretische Informatik*, Universität Ulm.
2013–2016	**MSc. Mathematical Sciences**, *Universität Ulm*, Master's thesis: Isogeny Graphs of Supersingular Elliptic Curves, Under Prof. Dr. Irene Ingeborg Bouw.
2008–2012	**BSc. Computer Science**, *Hochschule für Technik, Stuttgart*, Bachelor's thesis: ElGamal-Encription and Cryptography with Elliptic Curves, Under Prof. Dr. Peter Hauber.
2006–2008	**Elektrotechniker**, *Gottlieb-Daimler-Schule 1*, Sindelfingen.
2001–2005	**Ausbildung zum Energieelektroniker**, *Institut für Thermodynamik der Luft-und Raumfahrt*, Universität Stuttgart.
1991–1997	**Secondary school**, *Realschule am Goldberg*, Sindelfingen.
1985–1990	**Elementary school**, *Grundschule Nr. 1*, Petrosani, Romania.

Publications and Preprints

Genus 3 hyperelliptic curves with CM via Shimura reciprocity, *ANTS: The Open Book Series, Vol 4 (2020), 161-178*, with Sorina Ionica.

Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal complex multiplication, *Preprint: arXiv:2104.04919 (2021)*, with Sorina Ionica and Jeroen Sijsling.

References

Elisa Lorenzo García
Institut de Mathématiquese
Université de Neuchâtel, Suisse
✉ elisa.lorenzo@unine.ch

Irene Bouw
Institut für Algebra und Zahlentheorie
Universität Ulm, Germany
✉ irene.bouw@uni-ulm.de

Jeroen Sisjling
Institut für Algebra und Zahlentheorie
Universität Ulm, Germany
✉ jeroen.sijsling@uni-ulm.de