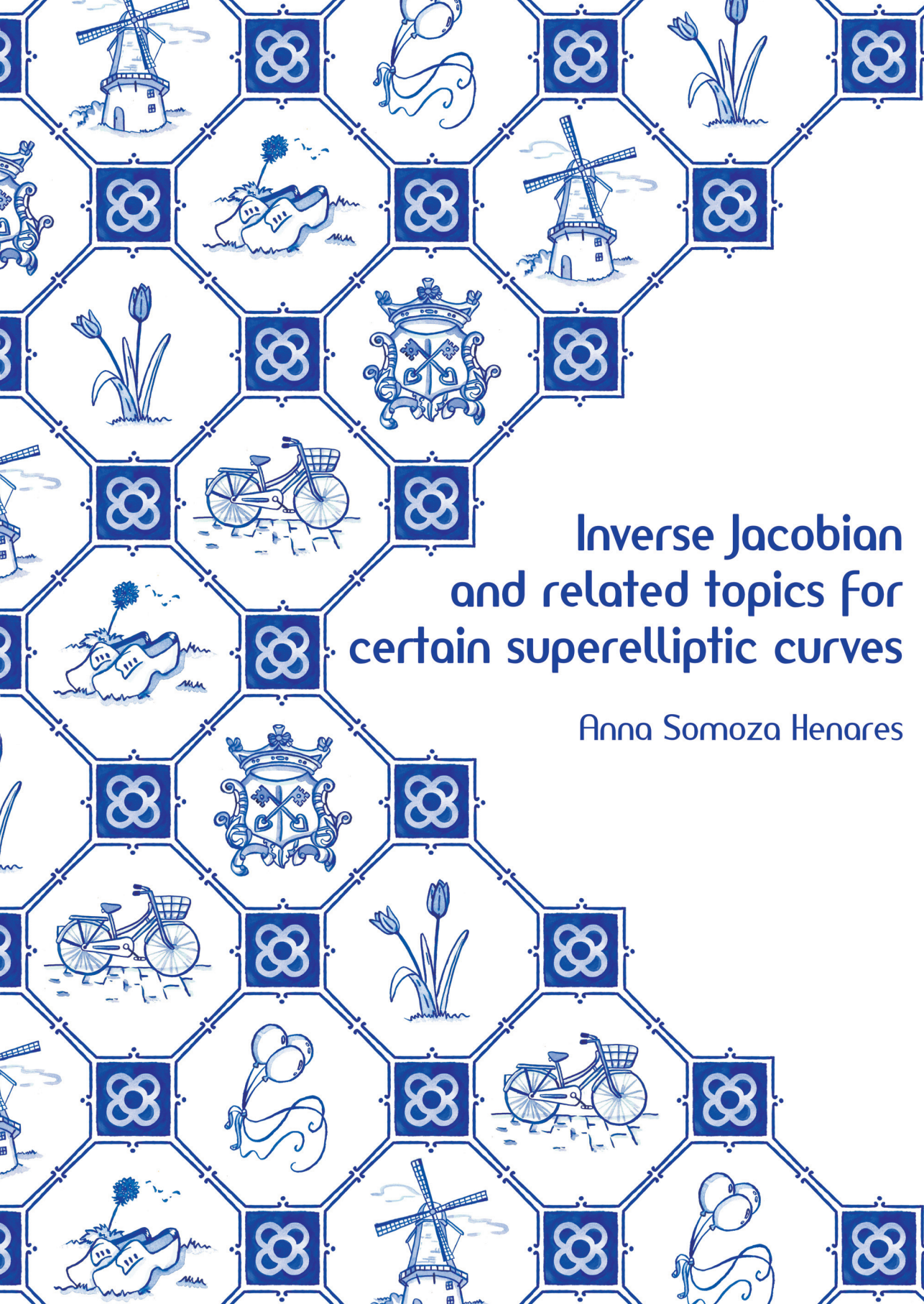


Inverse Jacobian and related topics for certain superelliptic curves

Anna Somoza Henares

Inverse Jacobian and related topics for certain superelliptic curves

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op 28 maart 2019
klokke 16:15 uur
door

Anna Somoza Henares

geboren te L'Hospitalet del Llobregat, Spanje
in 1991

Promotor: prof. dr. Joan-Carles Lario (Universitat Politècnica de Catalunya)

Promotor: prof. dr. Peter Stevenhagen

Copromotor: dr. Marco Streng

Samenstelling van de promotiecommissie:

prof. dr. Aad van der Vaart (Universiteit Leiden, voorzitter)

prof. dr. Bart de Smit (Universiteit Leiden, secretaris)

prof. dr. Bas Edixhoven (Universiteit Leiden)

prof. dr. Elisa Lorenzo García (Université de Rennes 1)

prof. dr. Jordi Guardia (Universitat Politècnica de Catalunya)

dr. Pınar Kılıçer (Rijksuniversiteit Groningen)

prof. dr. Christophe Ritzenthaler (Université de Rennes 1)

Inverse Jacobian and related topics for certain superelliptic curves

by Anna Somoza Henares

A thesis presented to obtain the

Doctoral degree in Applied Mathematics

from Universitat Politècnica de Catalunya

Supervised by
Joan-Carles Lario, Peter Stevenhagen, and Marco Streng

Departament de Matemàtiques

Barcelona 2019

Cover design by Vanessa Castillo Blanco, José Pérez Gordo and the author.

Contents

Contents **5**

Introduction **7**

1. The family of Picard curves **9**
1.1. Preliminaries on abelian varieties 10
1.1.1. Polarized abelian varieties 10
1.1.2. Polarized abelian varieties over $\mathbb{C}$ and complex tori 11
1.1.3. Jacobians and the Abel-Jacobi map 13
1.1.4. Jacobians and the Abel-Jacobi map over $\mathbb{C}$ 15
1.2. A Thomae-like formula 16
1.3. The inverse Jacobian algorithm 23
1.4. The Torelli locus of Picard curves 29
1.5. Implementation and some CM examples 30

2. The family of cyclic plane quintic curves **35**
2.1. A Thomae-like formula 36
2.2. The inverse Jacobian algorithm 39
2.3. Some CM examples 47

3. Moduli of abelian varieties with generalized CM-type **49**
3.1. CM-fields and m-CM-types 50
3.2. Polarized abelian varieties with given m-CM-type 51
3.3. The endomorphism structure of the Jacobian of a CPQ curve . . 58
3.4. Equivalence of polarized lattices 61
3.5. The Torelli locus of CPQ curves 71

4. CM cyclic plane quintic curves defined over $\mathbb{Q}$ **75**
4.1. CM-types 75
4.2. The CM class number 77
4.3. CM class number one fields for CPQ curves 80
4.3.1. Sufficient condition for CM class number one 83

4.3.2. Cyclic degree-12 CM-fields 85
4.3.3. Dicyclic degree-12 CM-fields 87
4.3.4. Final results 89

Bibliography **91**

Index **97**

Samenvatting **99**

Resumen **101**

Acknowledgements **103**

Curriculum vitae **105**

Introduction

Given an *elliptic curve* E over $\mathbb{C}$, there exists a *lattice* $\Lambda \subseteq \mathbb{C}$ such that the group $E(\mathbb{C})$ of complex points on E is isomorphic to the complex analytic group $\mathbb{C}/\Lambda$. This link between elliptic curves and one-dimensional complex tori is called the Uniformization Theorem, and one can explicitly find the curve corresponding to a given lattice with the *Weierstrass $\wp$-function*, its derivative, and the *Eisenstein series*.

Similarly, given an algebraic curve C of genus g, one associates to it a *principally polarized abelian variety* $J(C)$, the *Jacobian of* C. Over $\mathbb{C}$, the Jacobian $J(C)$ is isomorphic to a g-dimensional complex torus $\mathbb{C}^g/\Lambda$ for a lattice Λ of full rank in $\mathbb{C}^g$.

This determines a map J from the set M_g of isomorphism classes of algebraic curves of genus g to the set A_g of principally polarized abelian varieties of dimension g, and one may wonder if there exists an explicit inverse to this map, as in the case of elliptic curves. We call this the *inverse Jacobian problem*.

This problem has been solved for curves of genus 2 [37, 50] and genus 3 [1, 9, 16, 21, 48, 52, 53]. However, for genus $g \geq 4$ there is the additional obstruction that not all principally polarized abelian varieties are Jacobians of curves, hence in order to solve the inverse Jacobian problem one needs to study the image by J of M_g in A_g. The problem of describing $J(\mathsf{M}_g)$ is known as the *Riemann-Schottky problem.* .

In this thesis we treat these two problems for two families of *superelliptic curves*, that is, curves of the form $y^k = \prod_{i=1}^{l}(x - \alpha_i)$. We focus on the family of *Picard curves*, with $(k, l) = (3, 4)$ and genus 3, where we solve the inverse Jacobian problem, and the family of *cyclic plane quintic curves* (CPQ curves), with $(k, l) = (5, 5)$ and genus 6, where we solve both problems.

In Chapter 1 we first introduce some background on abelian varieties, Jacobians of curves, and Riemann theta constants, and then we present an inverse Jacobian algorithm for Picard curves. Note that Picard curves have genus 3, hence there is no obstruction to the inverse Jacobian problem.

Since Picard curves are plane quartic curves, the inverse Jacobian problem for Picard curves could be solved using the formulas for plane quartics given

in [52], but focusing on a smaller family of curves allows us to present a more efficient solution for the family of interest.

This was originally done by Koike and Weng in [16], but their exposition presents some mistakes that we address and correct here. This chapter is based on joint work with Joan-Carles Lario, see also [21].

In Chapter 2 we present an inverse Jacobian algorithm for CPQ curves. We follow a strategy analogous to the one in Chapter 1 for the case of Picard curves.

In Chapter 3 we address the Riemann-Schottky problem for CPQ curves, that is, we characterize the principally polarized abelian varieties that are Jacobians of CPQ curves. First we use a generalization of the classical theory of *complex multiplication* due to Shimura [39] to study how the existence of the automorphism of CPQ curves $(x, y) \mapsto (x, \exp(2\pi i/5)y)$ affects the structure of the Jacobians. Then we solve a class number one problem for higher-dimensional Hermitian lattices over $\mathbb{Z}[\zeta_5]$, which is key to solving the Riemann-Schottky problem for CPQ curves.

Finally, in Chapter 4 we present one application for the above algorithms: constructing curves such that their Jacobians have complex multiplication. This has previously been done for genus 2 [51, 47] and genus 3 [1, 13, 16, 21, 53]. Here we extend the methods of Kılıçer [12] to determine a complete list of CM-fields whose ring of integers occurs as the endomorphism ring over $\mathbb{C}$ of the Jacobian of a CPQ curve defined over $\mathbb{Q}$.

In particular, this allows us to list conjectural models for all CPQ curves over $\mathbb{Q}$ whose Jacobians have the maximal order of a degree-12 CM-field as endomorphism ring over $\mathbb{C}$. Our list contains the correct number of curves, which are defined over $\mathbb{Q}$ and numerically correct up to high precision.

The family of Picard curves 1

A *Picard curve* over $\mathbb{C}$ is a genus-3 smooth, plane, projective curve given by $y^3 = f(x)$ where f is a polynomial of degree 4. Such a curve has an automorphism ρ of order 3 given by $(x, y) \mapsto (x, z_3 y)$ with $z_3 = \exp\left(\frac{2\pi i}{3}\right)$. It fixes the points $(t, 0)$ with $f(t) = 0$, the *affine branch points* of C. The curve C also has a unique point at infinity, with projective coordinates $(0 : 1 : 0)$, which is also fixed by the automorphism ρ.

One can check that all isomorphisms between Picard curves are of the form

$$(x, y) \mapsto (ax + b, cy),$$

see Section 7.3 in Estrada [11, Appendix I] for details. Therefore, given a Picard curve C, every ordering of the affine branch points of C gives rise to an isomorphic Picard curve given by an equation of the form

$$y^3 = x(x-1)(x-\lambda)(x-\mu) \tag{1.1}$$

with the first affine branch point at $(0, 0)$, the second at $(0, 1)$, the third at $(0, \lambda)$ and the forth at $(0, \mu)$. We refer to the form (1.1) as a *Legendre-Rosenhain equation of a Picard curve*.

In this chapter we present a method that, given the period matrix of the Jacobian of a Picard curve, gives a numerical approximation of the equation of the curve. This was initially done by Koike and Weng in [16], but their exposition presents some gaps and mistakes that we fix in this chapter, see Remarks 1.2.14, 1.3.8, and 1.4.2.

We start by introducing some concepts needed throughout this thesis in Section 1.1, such as principally polarized abelian variety, the Jacobian of a curve and the Riemann-Schottky problem.

In Section 1.2 we give a formula to approximate the x-coordinates of the affine branch points of a Picard curve in terms of theta constants on its Jacobian, see Theorem 1.2.13.

In Section 1.3 we develop an algorithm that given the Jacobian of a Picard curve C returns the Legendre-Rosenhain equation of C, see Algorithm 1.3.9. The main step of the algorithm is applying the formula in Theorem 1.2.13, so we first identify the objects needed to apply said formula, such as the Riemann constant and the images by the Abel-Jacobi map of the affine branch points.

Finally, in Section 1.4 we characterize the polarized abelian varieties that arise as Jacobians of Picard curves, see Proposition 1.4.1, and in Section 1.5 we give some details on the implementation of Algorithm 1.3.9 and show examples of curves obtained using the algorithm.

This chapter is based on joint work with Joan-Carles Lario. In particular, Theorem 1.2.13 and the examples in Section 1.5 appeared before up to minor corrections in Joan-Carles Lario and Anna Somoza, *A note on Picard curves of CM-type*, arXiv:1611.02582 [21].

1.1 Preliminaries on abelian varieties

In this section we review some notions that will be needed throughout this thesis. We follow classical references such as Birkenhake-Lange [2], Lang [19], Milne [24, 25] or Mumford [30].

1.1.1 Polarized abelian varieties

An *abelian variety* X over a field k is a complete irreducible group variety defined over k, and it is smooth, projective and commutative. A *homomorphism of abelian varieties* is a morphism that respects the group structure. It is an *isogeny* if it is surjective and the abelian varieties have the same dimension. We say that an abelian variety is *absolutely simple* if it has no non-zero proper abelian subvarieties over the algebraic closure $\overline{k}$ of k.

Given an abelian variety X defined over k, we define the *Picard group of* X as the group $\mathrm{Pic}(X)$ of isomorphism classes of line bundles on $X_{\overline{k}}$. Given a line bundle $\mathcal{L}$ on $X_{\overline{k}}$, we define the map

$$\begin{aligned} \phi_{\mathcal{L}} : X(\overline{k}) &\to \mathrm{Pic}(X) \\ x &\mapsto [T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}], \end{aligned}$$

where T_x stands for the translation by x on $X_{\overline{k}}$ and $[\mathcal{L}]$ stands for the isomorphism class of $\mathcal{L}$ in $\mathrm{Pic}(X)$. The map $\phi_{\mathcal{L}}$ is a homomorphism, see Corollary 4 in Mumford [30, Section 2.6].

We define $\mathrm{Pic}^0(X)$ as the subgroup of $\mathrm{Pic}(X)$ consisting of classes of line bundles $\mathcal{L}$ such that the map $\phi_{\mathcal{L}}$ is zero. It is the group of $\overline{k}$-points of an abelian variety over k (see Section 2.8 in Mumford [30]), we call it the *dual variety of* X, and denote it by $\widehat{X}$.

A homomorphism of abelian varieties $f : X \to Y$ induces a map $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ that maps $\mathrm{Pic}^0(Y)$ to $\mathrm{Pic}^0(X)$, which gives us the dual homomorphism $\widehat{f} : \widehat{Y} \to \widehat{X}$.

We define a *polarization* on X as an isogeny $\lambda = \phi_{\mathcal{L}}$ where $\mathcal{L}$ is an ample line bundle on X_l for $l \supseteq k$ a finite separable extension of the field of definition k. It is called *principal* if it is an isomorphism. We say that a polarized abelian variety (X, λ) is defined over k if both X and λ are defined over k.

Two polarized abelian varieties (X_1, λ_1) and (X_2, λ_2) are *isomorphic* if there exists an isomorphism of abelian varieties $f : X_1 \to X_2$ that is compatible with the polarizations, meaning that it satisfies $\lambda_1 = \widehat{f} \circ \lambda_2 \circ f$.

Given a polarization $\lambda : X \to \widehat{X}$ and an endomorphism $f \in \mathrm{End}(X) \otimes \mathbb{Q}$, we define

$$f' := \lambda^{-1} \circ \widehat{f} \circ \lambda. \tag{1.2}$$

The map $\cdot' : \mathrm{End}(X) \otimes \mathbb{Q} \to \mathrm{End}(X) \otimes \mathbb{Q}$ given by $f \mapsto f'$ is an involution on $\mathrm{End}(X) \otimes \mathbb{Q}$, and we call it the *Rosati involution determined by* λ.

1.1.2 Polarized abelian varieties over $\mathbb{C}$ and complex tori

When considering an abelian variety X defined over $\mathbb{C}$, the complex manifold $X(\mathbb{C})$ is (complex analytically isomorphic to) a *polarizable complex torus*, that is, a complex vector space V modulo a lattice Λ of full rank that admits a *Riemann form*. A Riemann form is an anti-symmetric form $E \colon V \times V \to \mathbb{R}$ that is $\mathbb{R}$-bilinear, satisfies $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$, such that for $u, v \in V$ we have $E(iu, v) = E(iv, u)$, and such that the associated hermitian form

$$H(u, v) = E(iu, v) + iE(u, v) \tag{1.3}$$

is positive definite. A polarization of an abelian variety X defined over $\mathbb{C}$ determines a Riemann form E on the complex torus $X(\mathbb{C})$, and the determinant of E with respect to Λ is $\det E = 1$ if and only if the polarization is principal. For more details on how the two are related see [19, Section 3.4].

Given a principally polarized complex torus V/Λ of dimension g, we can choose bases $e_1, \ldots, e_g$ of V and $\lambda_1, \ldots, \lambda_{2g}$ of Λ. Writing the latter in terms of

the former, $\lambda_i = \sum_{j=1}^{g} l_{j,i} e_j$, defines a $g \times 2g$ matrix over $\mathbb{C}$,

$$\Pi = \begin{pmatrix} l_{1,1} & \cdots & \cdots & l_{1,2g} \\ \vdots & & & \vdots \\ l_{g,1} & \cdots & \cdots & l_{g,2g} \end{pmatrix}, \tag{1.4}$$

called a *big period matrix* of V/Λ, and we get $V/\Lambda \cong \mathbb{C}^g/\Pi\mathbb{Z}^{2g}$. Moreover, the form E is given with respect to the basis of Λ by the matrix $M_E = (E(\lambda_i, \lambda_j))_{ij} \in \mathbb{Z}^{2g\times 2g}$. Analogously, the form H is given with respect to the basis of V by the matrix $M_H = (H(e_i, e_j))_{ij} \in \mathbb{C}^{g\times g}$. These matrices satisfy the relation

$$M_H = 2i(\Pi M_E^{-1}\, {}^t\Pi)^{-1}. \tag{1.5}$$

We say that the basis $(\lambda_i)_i$ is *symplectic* if the matrix M_E of E with respect to that basis is

$$\begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix}. \tag{1.6}$$

In that case, the vectors $\lambda_{g+1}, \ldots, \lambda_{2g}$ form a basis of V and if we choose this basis of V, then we obtain a big period matrix of the form $(\Omega, \mathbf{1}_g)$ with $\Omega \in \mathbb{C}^{g\times g}$ symmetric and with positive definite imaginary part. We call the matrix Ω a *period matrix*, and we define the *Siegel upper-half space* $\mathbf{H}_g$ to be the set of matrices $\Omega \in \mathbb{C}^{g\times g}$ symmetric and with positive definite imaginary part.

We say that a principally polarized complex abelian variety X has period matrix $\Omega \in \mathbf{H}_g$ if $X(\mathbb{C})$ is isomorphic to $\mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ and the Riemann form determined by the polarization of X is given by the matrix (1.6).

A *homomorphism* between complex tori is a holomorphic map f from V/Λ to V'/Λ' that respects the group structure. In particular, it lifts to a $\mathbb{C}$-linear map $F : V \to V'$ that satisfies $F(\Lambda) \subseteq \Lambda'$.

This gives the map

$$\begin{aligned} \rho_a : \mathrm{Hom}(V/\Lambda, V'/\Lambda') &\to \mathrm{Hom}(V, V') \\ f &\mapsto F, \end{aligned}$$

the *analytic representation* of $\mathrm{Hom}(V/\Lambda, V'/\Lambda')$; and considering the restriction of F to the lattice we obtain the map

$$\begin{aligned} \rho_r : \mathrm{Hom}(V/\Lambda, V'/\Lambda') &\to \mathrm{Hom}(\Lambda, \Lambda') \\ f &\mapsto F|_\Lambda, \end{aligned}$$

the *rational representation*.

Let now $\Pi \in \mathbb{C}^{g\times 2g}$ and $\Pi' \in \mathbb{C}^{g'\times 2g'}$ be big period matrices of V/Λ and V'/Λ' respectively. With respect to the chosen bases, the analytic representation $\rho_a(f)$ is a $g' \times g$ matrix over $\mathbb{C}$, and the rational representation $\rho_r(f)$ is a $2g' \times 2g$ matrix over $\mathbb{Z}$. They are related by the equation

$$\rho_a(f)\Pi = \Pi'\rho_r(f). \tag{1.7}$$

In the case where $f : (V/\Lambda, E) \to (V'/\Lambda', E')$ is an isomorphism of principally polarized abelian varieties we also have for all $u, v \in \mathbb{C}^g$ the equality $E(u, v) = E'(f(u), f(v)) =: f^*E'(u, v)$. Assume now that the chosen bases are symplectic, so that the abelian varieties have respectively $\Omega, \Omega' \in \mathbf{H}_g$ as period matrices. In terms of matrices, the relation $f^*E' = E$ becomes

$$^tN \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix} N = \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix}, \tag{1.8}$$

for N the matrix of $\rho_r(f)$ with respect to symplectic bases of Λ and Λ'. We define the *symplectic group* $\mathrm{Sp}_{2g}(\mathbb{Z})$ as the group of matrices in $\mathbb{Z}^{2g\times 2g}$ that satisfy (1.8), so we have $\rho_r(f) \in \mathrm{Sp}_{2g}(\mathbb{Z})$.

Let M be the transpose matrix of $\rho_r(f)$ and consider the subdivision in $g \times g$ blocks

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = {}^t\rho_r(f).$$

It follows from (1.7) and the symmetry of the period matrices that the matrix of $\rho_a(f)$ with respect to these bases for Λ and Λ' is

$$^t(\gamma\Omega' + \delta) \tag{1.9}$$

and the period matrices Ω, Ω' are related by the equation

$$\Omega = (\alpha\Omega' + \beta)(\gamma\Omega' + \delta)^{-1} =: M(\Omega'). \tag{1.10}$$

In particular, this relation gives an action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on $\mathbf{H}_g$. For details, see Section 8.2 in [2].

1.1.3 Jacobians and the Abel-Jacobi map

Let now C be a *curve* of genus g defined over a field k, that is, a smooth, projective, geometrically irreducible algebraic curve over k of genus g. For such a curve C, let $\mathrm{Div}(C)$ (respectively $\mathrm{Div}^0(C)$) be the set of divisors on $C_{\overline{k}}$ (resp. degree-0 divisors on $C_{\overline{k}}$), let $\mathrm{Prin}(C)$ be the set of principal divisors and define $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$.

To the curve C over k one can associate in a natural way a principally polarized abelian variety of dimension g over k, its *Jacobian* $J(C)$. We have $J(C)(\overline{k}) = \mathrm{Pic}^0(C)$, and denote by λ_C its natural polarization. Its dimension is equal to the genus of C. Given a point $P \in C(\overline{k})$, we define the *Abel-Jacobi map with base point* P as the morphism of varieties over $\overline{k}$ given by

$$\begin{aligned} \alpha : C &\to J(C) \\ Q &\mapsto [Q - P], \end{aligned} \tag{1.11}$$

and we extend it additively to divisors.

Given a morphism of curves $\varphi : C \to C'$, let $J(C)$ and $J(C')$ be respectively the Jacobians of C and C'. The morphism φ induces the homomorphisms $\varphi_* : \mathrm{Div}(C) \to \mathrm{Div}(C')$ given by $[P] \mapsto [\varphi(P)]$, and $\varphi^* : \mathrm{Div}(C') \to \mathrm{Div}(C)$ given by $[Q] \mapsto \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)[P]$, where $e_\varphi(P)$ is the order at P of the function $t \circ \varphi$ for t a uniformizer at Q. These homomorphisms map degree-0 divisors to degree-0 divisors and principal divisors to principal divisors, so they induce homomorphisms $\varphi_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C')$ and $\varphi^* : \mathrm{Pic}^0(C') \to \mathrm{Pic}^0(C)$.

In particular, for α, α' the Abel-Jacobi maps with base point $P \in C$ and $\varphi(P) \in C'$ respectively, the diagram

$$\begin{array}{ccc} C & \xrightarrow{\varphi} & C' \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha'} \\ J(C) & \xrightarrow{\varphi_*} & J(C') \end{array} \tag{1.12}$$

commutes. Conversely, an isomorphism of Jacobians determines an isomorphism between the corresponding curves, due to the following result:

Theorem 1.1.1 (Torelli, see Milne [25, Section 12])**.** Let C and C' be curves over an algebraically closed field k, and let α, α' be the Abel-Jacobi maps with base point $P \in C$, $\varphi(P) \in C'$ respectively. Let $\varphi : J(C) \to J(C')$ be an isomorphism of principally polarized abelian varieties.

(1) There exists an isomorphism $\rho : C \to C'$ that satisfies $\varphi = \pm\rho_*$.
(2) Assume that the curves have genus ≥ 2. If C is not hyperelliptic, then the map ρ and the sign $\pm$ are uniquely determined by φ. If C is hyperelliptic, then the sign can be chosen arbitrarily, and ρ is uniquely determined by φ and $\pm$. □

Torelli's Theorem implies the injectivity of the map J, the *Torelli map*, from the set of curves of genus g over $\overline{k}$ up to isomorphism to the set of isomorphism classes of principally polarized abelian varieties of dimension g over $\overline{k}$. This motivates the *Riemann-Schottky problem*.

The Riemann-Schottky problem. Describe the image of J.

Our goal throughout this chapter is to give an inverse Jacobian algorithm restricted to the family $\mathcal{P}$ of Picard curves. We present Algorithm 1.3.9 which, given $X \in J(\mathcal{P})$, determines a curve C with $X \cong J(C)$. Moreover, in Section 1.4 we also give a characterization of the absolutely simple principally polarized abelian varieties in $J(\mathcal{P})$.

Proposition 1.1.2. Every Picard curve is *non-hyperelliptic*, that is, the canonical map $C \to \mathbb{P}^2$ is an embedding.

Proof. One computes that a basis of regular differentials for a Picard curve is

$$\left(\frac{dx}{y^2}, \frac{xdx}{y^2}, \frac{dx}{y}\right).$$

It follows that the canonical map is the embedding $(x : y : 1) : C \to \mathbb{P}^2$. □

1.1.4 Jacobians and the Abel-Jacobi map over $\mathbb{C}$

For a curve C defined over $\mathbb{C}$, its Jacobian is also defined over $\mathbb{C}$ and therefore isomorphic to a principally polarized complex torus. We now construct this torus explicitly, as in Birkenhake-Lange [2, Section 11.1].

Let $H^0(\omega_C)$ be the complex vector space of regular differentials of C, and let $H^0(\omega_C)^*$ denote its dual. The homology $H_1(C, \mathbb{Z})$ of C injects into $H^0(\omega_C)^*$ via the map $H_1(C, \mathbb{Z}) \to H^0(\omega_C)^*$ given by $\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$, where the integral is taken for a representative of the class $\gamma \in H_1(C, \mathbb{Z})$.

The image of $H_1(C, \mathbb{Z})$ in $H^0(\omega_C)^*$ is a lattice of rank $2g$ in a complex vector space of dimension g. The Jacobian of C is isomorphic to the g-dimensional complex torus given by the quotient $H^0(\omega_C)^*/H_1(C, \mathbb{Z})$, and the Riemann form is given by the oriented intersection paring on $H_1(C, \mathbb{Z})$.

Theorem 1.1.3. (Abel-Jacobi, see [2, Theorem 11.1.3]) Let C be a curve and let $P \in C$. The map

$$\begin{aligned} &C \to H^0(\omega_C)^*/H_1(C, \mathbb{Z}), \\ &Q \mapsto \left\{\omega \mapsto \int_P^Q \omega\right\} \end{aligned} \tag{1.13}$$

induces a canonical isomorphism $\mathrm{Pic}^0(C) \to H^0(\omega_C)^*/H_1(C, \mathbb{Z})$, which does not depend on P. □

When we identify $J(C)$ with $H^0(\omega_C)^*/H_1(C, \mathbb{Z})$, the map (1.13) is the Abel-Jacobi map with base point P as in (1.11).

1.2 A Thomae-like formula

In this section we present a formula that gives the x-coordinates of the affine branch points of a Picard curve C given by a Legendre-Rosenhain equation as a quotient of Riemann theta functions evaluated at certain points of the Jacobian $J(C)$. We start by defining these functions.

Definition 1.2.1. The *Riemann theta function* is the function $\theta : \mathbb{C}^g \times \mathbf{H}_g \to \mathbb{C}$ given by

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t \Omega n + 2\pi i n^t z).$$

Theorem 1.2.2 (Riemann's Vanishing Theorem, see [29, Corollary 3.6])**.** Let C be a curve over $\mathbb{C}$ of genus g, let $J(C)$ be the Jacobian of C with period matrix $\Omega \in \mathbf{H}_g$ and let α be an Abel-Jacobi map of C. There is an element $\Delta \in J(C)$, called a *Riemann constant* with respect to α, such that the function $\theta(\,\cdot\,, \Omega)$ vanishes at $z \in \mathbb{C}^g$ if and only if there exist $Q_1, \ldots, Q_{g-1} \in C$ that satisfy

$$z \equiv \alpha(Q_1 + \cdots + Q_{g-1}) - \Delta \mod \Omega\mathbb{Z}^g + \mathbb{Z}^g. \qquad \square$$

Next we prove that Δ is actually unique up to the choice of a base point for the Abel-Jacobi map α. We will use the following lemma.

Lemma 1.2.3. Let $\Omega \in \mathbf{H}_g$ and let $\Theta \subseteq \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ be the subset defined by $\theta(z, \Omega) = 0$. Then the map

$$\begin{aligned} \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g) &\to \{e + \Theta : e \in \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)\} \\ x &\mapsto \{z \in \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g) : \theta(z - x, \Omega) = 0\} = x + \Theta \end{aligned}$$

is injective.

Proof. See the proof of Theorem II.3.10(b) in Mumford [29]. $\square$

Proposition 1.2.4. Let C be a curve over $\mathbb{C}$ of genus g, let $J(C)$ be the Jacobian of C with period matrix $\Omega \in \mathbf{H}_g$, and let α be the Abel-Jacobi map with base point $P \in C$. The Riemann constant Δ with respect to α is uniquely determined by Theorem 1.2.2 and satisfies

$$2\Delta = \alpha(\kappa)$$

for κ a canonical divisor of C.

Proof. For the first part of the statement, let $\Delta^1, \Delta^2 \in J(C)$ satisfy Theorem 1.2.2, that is, the equality $\Theta = \alpha(\mathrm{Sym}^{g-1} C) - \Delta^i$. We have

$$\Theta = \alpha(\mathrm{Sym}^{g-1} C) - \Delta^1 = \alpha(\mathrm{Sym}^{g-1} C) - \Delta^2 + \Delta^2 - \Delta^1 = \Theta + (\Delta^2 - \Delta^1)$$

thus it follows from Lemma 1.2.3 that $\Delta^2 - \Delta^1$ is zero, hence the Riemann constant is unique.

For the second part, consider an effective divisor $D = \sum_{i=1}^{g-1} P_i$ for $P_i \in C$. By the Riemann-Roch Theorem, there exist $g-1$ points $Q_1, \ldots, Q_{g-1}$ in C that satisfy

$$\kappa - D \sim \sum_{i=1}^{g-1} Q_i,$$

or equivalently, $\alpha(\kappa - D) = \alpha(\sum_{i=1}^{g-1} Q_i)$. We get

$$\alpha(\kappa) - \alpha(\mathrm{Sym}^{g-1} C) \subseteq \alpha(\mathrm{Sym}^{g-1} C).$$

If we consider the translation $-\alpha(\mathrm{Sym}^{g-1} C) \subseteq \alpha(\mathrm{Sym}^{g-1} C) - \alpha(\kappa)$ and apply to it the bijection on $J(C)$ that maps a point x to $-x$, then we obtain

$$\alpha(\mathrm{Sym}^{g-1} C) \subseteq -\alpha(\mathrm{Sym}^{g-1} C) + \alpha(\kappa),$$

hence the equality holds.

Observe now that the Riemann theta function is symmetric in z via the map $n \mapsto -n$. In consequence the set Θ is symmetric, and we obtain

$$\alpha(\mathrm{Sym}^{g-1} C) - \Delta = -\alpha(\mathrm{Sym}^{g-1} C) + \Delta = \alpha(\mathrm{Sym}^{g-1} C) - \alpha(\kappa) + \Delta.$$

We conclude by the uniqueness of the Riemann constant that Δ satisfies the equality $\Delta = \alpha(\kappa) - \Delta$ and the result follows. □

Next we introduce a theorem of Siegel that relates the values of a function on a curve C at a *non-special* divisor with a quotient of Riemann theta functions evaluated at some points in the Jacobian.

Definition 1.2.5. We say that an effective divisor D of degree g is *special* if there exists a regular differential ω with $\mathrm{div}(\omega) \geq D$. Otherwise we call them *non-special* (called *general* in Siegel [44, pg. 154]).

Theorem 1.2.6 (Theorem 11.3 in Siegel [44])**.** Let C be a curve of genus g over $\mathbb{C}$, and let ϕ be a function on C with

$$\mathrm{div}(\phi) = \sum_{i=1}^{m} A_i - \sum_{i=1}^{m} B_i.$$

Let $P \in C$ and let ω be a basis of $H^0(\omega_C)$ for which the Jacobian $J(C)$ has period matrix $\Omega \in \mathbf{H}_g$. Let Δ be the Riemann constant with respect to the Abel-Jacobi α map with base point P.

Choose paths from the base point P to A_i and B_i that satisfy

$$\sum_{i=1}^{m} \int_P^{A_i} \omega = \sum_{i=1}^{m} \int_P^{B_i} \omega.$$

Then, given an effective non-special divisor $D = P_1 + \cdots + P_g$ of degree g that satisfies $P_j \notin \{A_i, B_i : 1 \leq i \leq m\}$, one has

$$\phi(D) := \phi(P_1) \dots \phi(P_g) = E \prod_{i=1}^{m} \frac{\theta(\sum_{j=1}^{g} \int_P^{P_j} \omega - \int_P^{A_i} \omega - \Delta, \Omega)}{\theta(\sum_{j=1}^{g} \int_P^{P_j} \omega - \int_P^{B_i} \omega - \Delta, \Omega)},$$

where $E \in \mathbb{C}^\times$ is independent of D, and the integrals from P to P_j take the same paths both in the numerator and the denominator. □

Observe that the integrals at which we are evaluating the Riemann theta functions are representatives of the image by the Abel-Jacobi map of C with base point P of the points in the divisor, see Section 1.1.4.

But if a point in $J(C)$ is a torsion point, then we can write it as a rational vector with respect to the basis of the lattice. In fact, the bijection

$$\begin{aligned} \underline{\cdot} : J(C) &\to \mathbb{R}^{2g}/\mathbb{Z}^{2g} \\ \Omega x_1 + x_2 &\mapsto (x_1, x_2) \end{aligned}$$

maps the m-torsion of $J(C)$ to $\frac{1}{m}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$.

In this section we are interested in computing the x-coordinates of the affine branch points of a Picard curve C, so we will choose non-special divisors supported on these points. Note that for every affine branch point P of a Picard curve, we have $\operatorname{div}(x - x(P)) = 3P - 3(0:1:0)$, so the image of P via the Abel-Jacobi map with base point $(0:1:0)$ is a 3-torsion point.

Therefore, it is convenient for us to rewrite Theorem 1.2.6 in terms of the following modification of the Riemann theta function:

Definition 1.2.7. The *Riemann theta function with (real) characteristic* $x = (x_1, x_2) \in \mathbb{R}^{2g}$ is the function $\theta[x] : \mathbb{C}^g \times \mathbf{H}_g \to \mathbb{C}$ given by

$$\theta[x](z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i\, {}^t(n + x_1)\Omega(n + x_1) + 2\pi i\, {}^t(n + x_1)(z + x_2)). \quad (1.14)$$

It is a translate of the Riemann theta function as in Definition 1.2.1 times an exponential factor:

$$\theta[x](z, \Omega) = \exp(\pi i x_1^t \Omega x_1 + 2\pi i x_1^t (z + x_2))\theta(z + \Omega x_1 + x_2, \Omega). \quad (1.15)$$

A *Riemann theta constant* is a Riemann theta function evaluated at $z = 0$. For notational convenience, we denote it by $\theta[x](\Omega) := \theta[x](0, \Omega)$.

Proposition 1.2.8 (Mumford [29, pg. 123])**.** The Riemann theta constants satisfy the following properties:

(1) They are symmetric with respect to x, that is

$$\theta[x](\Omega) = \theta[-x](\Omega)\,. \tag{1.16}$$

(2) They are quasi-periodic, meaning that for $m = (m_1, m_2) \in \mathbb{Z}^{2g}$ one has

$$\theta[x+m](\Omega) = \exp(2\pi i x_1 m_2)\theta[x](\Omega)\,. \tag{1.17}$$

□

Note that, due to the quasi-periodicity of the Riemann theta constants, the domain for the characteristics is $\mathbb{R}^{2g}$, rather than $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$. Therefore we fix a representative for such elements. We define the map $\widetilde{\cdot}\colon \mathbb{R}^{2g}/\mathbb{Z}^{2g} \to [0,1)^{2g}$ that maps a class in $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$ to its representative with entries in $[0,1)$.

For convenience, if the domain is clear we denote any composition of the maps

$$C \xrightarrow{\alpha} J(C) \xrightarrow{\cdot} \mathbb{R}^{2g}/\mathbb{Z}^{2g} \xrightarrow{\widetilde{\cdot}} [0,1)^{2g}$$

by the last one. For example, for $P \in C$ we write $\widetilde{P}$ instead of $\widetilde{\alpha(P)}$. Moreover, given a divisor $D = \sum n_P P$ we define $\widetilde{D} := \sum n_P \widetilde{P} \in \mathbb{R}^{2g}$.

Warning 1.2.9. Note that with our definition of $\widetilde{D}$, for most divisors D we have $\widetilde{D} \neq \widetilde{\alpha(D)}$.

We can now rewrite Theorem 1.2.6 in terms of Riemann theta constants:

Corollary 1.2.10. With the notation in Theorem 1.2.6, let a_i (resp. b_i) be the element in $\mathbb{R}^{2g}$ that satisfies $\int_P^{A_i} \omega = \Omega(a_i)_1 + (a_i)_2$ (resp. $\int_P^{B_i} \omega = \Omega(b_i)_1 + (b_i)_2$). We obtain

$$\phi(D) = E' \prod_{i=1}^{m} \frac{\theta\left[\sum_{j=1}^{g} \widetilde{P_j} - a_i - \widetilde{\Delta}\right](\Omega)}{\theta\left[\sum_{j=1}^{g} \widetilde{P_j} - b_i - \widetilde{\Delta}\right](\Omega)},$$

where $E' \in \mathbb{C}^\times$ is also independent of D.

Proof. Observe that the exponential factor in (1.15) for Riemann theta constants (that is, $z = 0$) can be written as $\exp(\pi i B(x,x))$ where B is the symmetric bilinear form given by

$$B(u,v) = {}^t u \begin{pmatrix} \Omega & \mathbf{1}_g \\ \mathbf{1}_g & 0 \end{pmatrix} v.$$

Let $Q(u) = B(u,u)$ and let $c = \left(\sum_{j=1}^{g} \widetilde{P}_j\right) - \widetilde{\Delta}$. For $j = 1, \ldots, g$ let $x_j = \widetilde{P_j}$ and choose a path from P to P_j that satisfies $\int_P^{P_j} \omega = \Omega(x_j)_1 + (x_j)_2 \in \mathbb{C}^g$.

Let $E' \in \mathbb{C}^\times$ be defined by

$$E\prod_{i=1}^{m}\frac{\theta\left(\left(\sum_{j=1}^{g}\int_P^{P_j}\omega\right)-\int_P^{A_i}\omega-\Delta,\Omega\right)}{\theta\left(\left(\sum_{j=1}^{g}\int_P^{P_j}\omega\right)-\int_P^{B_i}\omega-\Delta,\Omega\right)}=E'\prod_{i=1}^{m}\frac{\theta\left[\left(\sum_{j=1}^{g}\widetilde{P_j}\right)-a_i-\widetilde{\Delta}\right](\Omega)}{\theta\left[\left(\sum_{j=1}^{g}\widetilde{P_j}\right)-b_i-\widetilde{\Delta}\right](\Omega)}.$$

We want to prove that E' does not depend on $D=\sum_{j=1}^{g}P_j$. By (1.15) we get

$$\frac{E}{E'}=\exp\left(\pi i\sum_{i=1}^{m}(Q(c-a_i)-Q(c-b_i))\right),$$

so it suffices to show that $\sum_{i=1}^{m}(Q(c-a_i)-Q(c-b_i))$ does not depend on D. We have

$$\begin{aligned}\sum_{i=1}^{m}(Q(c-a_i)-Q(c-b_i))&=\sum_{i=1}^{m}(Q(a_i)-Q(b_i)-2B(c,a_i-b_i))\\&=\sum_{i=1}^{m}Q\left(a_i\right)-\sum_{i=1}^{m}Q\left(b_i\right)-2B\left(c,\sum_{i=1}^{m}(a_i-b_i)\right),\end{aligned}$$

but we know

$$\sum_{i=1}^{m}\int_P^{A_i}\omega=\sum_{i=1}^{m}\int_P^{B_i}\omega.$$

so in terms of characteristics we obtain $\sum_{i=1}^{m}(a_i-b_i)=0$ and then it follows that

$$\sum_{i=1}^{m}(Q(c-a_i)-Q(c-b_i))=\sum_{i=1}^{m}Q\left(a_i\right)-\sum_{i=1}^{m}Q\left(b_i\right)$$

does not depend on D. □

Lemma 1.2.11. Let C be a Picard curve over $\mathbb{C}$ given by a Legendre-Rosenhain equation, and denote $P_0=(0,0)$ and $P_\infty=(0:1:0)$. Let α be the Abel-Jacobi map with base point P_∞, let $\Omega\in\mathbf{H}_3$ be a period matrix of $J(C)$ and let $\Delta\in J(C)$ be the Riemann constant with respect to α. Then, for every effective non-special divisor $D=R_1+R_2+R_3$ of degree 3 with $R_i\neq P_0,P_\infty$, we have

$$x(R_1)x(R_2)x(R_3)=E'\,\varepsilon(D)\left(\frac{\theta[\widetilde{D}-\widetilde{P_0}-\widetilde{\Delta}](\Omega)}{\theta[\widetilde{D}-\widetilde{\Delta}](\Omega)}\right)^3,$$

with $\varepsilon(D)=\exp(6\pi i(\widetilde{D}-\widetilde{P_0}-\widetilde{\Delta})_1(\widetilde{P_0})_2)$ and $E'\in\mathbb{C}^\times$ independent of D.

Proof. Let ω be the basis of holomorphic differentials for which $J(C)$ has period matrix Ω. The divisor of the function x on C is $\mathrm{div}(x) = 3\,P_0 - 3\,P_\infty$, so in order to apply Corollary 1.2.10 for $\phi = x$ and $P = P_\infty$, we choose three times the zero path from P_∞ to itself, the path γ_1 from P_∞ to P_0 that for $a_1 = \widetilde{P_0}$ satisfies

$$\int_{\gamma_1} \omega = \Omega(a_1)_1 + (a_1)_2 \in \mathbb{C}^3,$$

and paths γ_2, γ_3 from P_∞ to P_0 that satisfy

$$\sum_{k=1}^{3} \int_{\gamma_k} \omega = 0 \text{ in } \mathbb{C}^3. \tag{1.18}$$

Let a_2, a_3 be the elements in $\mathbb{R}^6$ that satisfy

$$\int_{\gamma_k} \omega = \Omega(a_k)_1 + (a_k)_2 \text{ for } k = 2, 3.$$

Then, by Corollary 1.2.10, we have

$$\phi(D) = E' \prod_{k=1}^{3} \frac{\theta[\widetilde{D} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)} \tag{1.19}$$

for some constant $E' \in \mathbb{C}^\times$ independent of D. Note that for $k = 1, 2, 3$ we have

$$\underline{P_0} = (a_k \bmod \mathbb{Z}^6),$$

so the differences $a_i - a_j$ for $i \neq j$ are integer vectors. Applying the quasi-periodicity property (1.17), equation (1.19) becomes

$$\phi(D) = E' \frac{\exp(2\pi i(\widetilde{D} - \widetilde{P_0} - \widetilde{\Delta})_1(a_1 - a_2 + a_1 - a_3)_2)\,\theta[\widetilde{D} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)^3}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)^3}.$$

But it follows from (1.18) that the sum $a_1 + a_2 + a_3$ is zero, so we obtain $a_1 - a_2 + a_1 - a_3 = 3a_1 = 3\widetilde{P_0}$ and the statement follows. □

The final piece is to choose the right divisors and prove that they are non-special.

Lemma 1.2.12 (Koike-Weng [16, pg. 506])**.** Let C be a Picard curve and let $\mathcal{B}$ be the set of affine branch points of C. If $P, Q \in \mathcal{B}$ are distinct, then the divisor $P + 2Q$ is non-special. □

Now we have all the components to give a formula for the x-coordinates of the affine branch points of a Picard curve given by a Legendre-Rosenhain equation in terms of quotients of Riemann theta constants.

Theorem 1.2.13. Let C be a Picard curve over $\mathbb{C}$ given by the Legendre-Rosenhain equation $y^3 = x(x-1)(x-\lambda)(x-\mu)$, let $\Omega \in \mathbf{H}_6$ be a period matrix of the Jacobian $J(C)$, let α be the Abel-Jacobi map with base point $(0:1:0)$, and let Δ be the Riemann constant with respect to α. Let $P_t = (t,0)$ for $t \in \{0,1,\lambda,\mu\}$ and let $\eta \in \{\lambda,\mu\}$. Then we have

$$\eta = \varepsilon_\eta \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)} \right)^3, \tag{1.20}$$

with $\varepsilon_\eta = \exp(6\pi i((\widetilde{P_\eta} - \widetilde{P_1})_1(\widetilde{P_0})_2 + (\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3(\widetilde{P_1} + \widetilde{P_\eta}))_2))$.

Proof. We apply Lemma 1.2.11 to the divisors $D_1 = P_1 + 2P_\eta$ and $D_2 = 2P_1 + P_\eta$, which are non-special by Lemma 1.2.12. We get

$$\begin{aligned} \eta = \frac{x(P_1)x(P_\eta)^2}{x(P_1)^2x(P_\eta)} &= \frac{E'\varepsilon(D_1)\left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{\Delta}](\Omega)} \right)^3}{E'\varepsilon(D_2)\left(\frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{\Delta}](\Omega)} \right)^3} \\ &= \frac{\varepsilon(D_1)}{\varepsilon(D_2)} \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)} \right)^3. \end{aligned} \tag{1.21}$$

In order to simplify the formula we apply the symmetry (1.16) and quasi-periodicity (1.17) of the Riemann theta constants to obtain

$$\begin{aligned} \theta[\widetilde{D_2} - \widetilde{\Delta}](\Omega) &= \theta[-\widetilde{D_2} + \widetilde{\Delta}](\Omega) \\ &= \theta[\widetilde{D_1} - \widetilde{\Delta} + (2\widetilde{\Delta} + 3(\widetilde{P_1} + \widetilde{P_\eta}))](\Omega) \\ &= \exp\left(2\pi i(\widetilde{D_1} - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3(\widetilde{P_1} + \widetilde{P_\eta}))_2\right) \theta[\widetilde{D_1} - \widetilde{\Delta}](\Omega) \end{aligned}$$

so that the formula (1.21) becomes

$$\eta = \varepsilon_\eta \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)} \right)^3,$$

with

$$\begin{aligned} \varepsilon_\eta &= \frac{\varepsilon(D_1)}{\varepsilon(D_2)} \exp(2\pi i(\widetilde{D_1} - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3(\widetilde{P_1} + \widetilde{P_\eta}))_2)^3 \\ &= \frac{\exp(6\pi i(\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta})_1(\widetilde{P_0})_2)}{\exp(6\pi i(2\widetilde{P_1} + \widetilde{P_\eta} - \widetilde{P_0} - \widetilde{\Delta})_1(\widetilde{P_0})_2)} \exp(6\pi i(\widetilde{D_1} - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3(\widetilde{P_1} + \widetilde{P_\eta}))_2) \\ &= \exp(6\pi i((\widetilde{P_\eta} - \widetilde{P_1})_1(\widetilde{P_0})_2 + (\widetilde{P_1} + 2\widetilde{P_\eta} - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3(\widetilde{P_1} + \widetilde{P_\eta}))_2)) \end{aligned}$$

as desired. □

Remark 1.2.14. Compare the formula for η given in Theorem 1.2.13 with the ones given by Koike-Weng [16, Eq. 9]. The formulas in [16] are the same as (1.20) replacing ε_η by 1, hence in general they do not hold due to the absence of the precise root of unity.

However, if we follow the original work by Picard [35, p. 131] where he constructs the period matrix of a Picard curve given by a Legendre-Rosenhain equation in a specific way (see also Shiga [38, Proposition I-3]), then we obtain that the factors ε_λ and ε_μ are 1, so in that case the formulas in [16] remain correct.

But if Ω is not specifically constructed in that way, then we have to either be lucky (and get $\varepsilon_\lambda = \varepsilon_\mu = 1$) or use the formula for ε_η.

1.3 The inverse Jacobian algorithm

In this section we present an algorithm that, given the period matrix of the Jacobian of a Picard curve C and the rational representation of the automorphism ρ_* induced by $\rho(x, y) = (x, z_3 y)$, returns a numerical approximation of the x-coordinates of the affine branch points of C.

The main step of the algorithm uses Theorem 1.2.13. To apply that theorem we need to know the Riemann constant of C with respect to the Abel-Jacobi map α with base point $(0 : 1 : 0)$ and the image by α of the affine branch points on $J(C)$.

We start by characterizing the Riemann constant of a Picard curve. We will do so by using both its uniqueness and the fact that the base point for α is fixed by the automorphism ρ.

First we show how a change of symplectic bases affects a Riemann theta function with characteristics.

Definition 1.3.1. For $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ and $c \in \mathbb{R}^{2g}$ we define

$$M[c] := {}^tM^{-1}c + \frac{1}{2}\begin{pmatrix} (\gamma\,{}^t\delta)_0 \\ (\alpha\,{}^t\beta)_0 \end{pmatrix},$$

where X_0 stands for the diagonal of the matrix X.

Note that the class $N[c] \bmod \mathbb{Z}^{2g}$ depends only on the class of $c \bmod \mathbb{Z}^{2g}$, so we denote it by $N[c \bmod \mathbb{Z}^{2g}]$. Moreover, for $x \in J(C)$ we denote the point that satisfies the equality $\underline{N[x]} = N[\underline{x}]$ by $N[x] \in J(C)$.

Proposition 1.3.2 (Proposition 8.6.1 in Birkenhake-Lange [2])**.** For a period matrix $\Omega \in \mathbf{H}_g$, a characteristic $c \in \mathbb{R}^{2g}$ and a symplectic matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}),$$

there exists a function $\kappa(M,\Omega,c,\cdot):\mathbb{C}^g\to\mathbb{C}^\times$ that satisfies for all $v\in\mathbb{C}^g$ the equality

$$\theta[M[c]]({}^t(\gamma\Omega+\delta)^{-1}v,M(\Omega))=\kappa(M,\Omega,c,v)\theta[c](v,\Omega). \qquad \square$$

Remark 1.3.3. The factor $\kappa(M,\Omega,c,v)\in\mathbb{C}^\times$ is given explicitly in Birkenhake-Lange [2, Proposition 8.6.1].

Proposition 1.3.4. Let C,C' be curves with equal genus g, let $\varphi:C\to C'$ be an isomorphism of curves, and let $\varphi_*:J(C)\to J(C')$ be the induced isomorphism on the Jacobians with period matrices $\Omega,\Omega'\in\mathbf{H}_g$ respectively. Define $N:={}^t\rho_r(\varphi_*)$. Let $P\in C$, let α be the Abel-Jacobi map with base point P, and let α' be the Abel-Jacobi map with base point $\varphi(P)$.

Let also Δ (resp. Δ') be the Riemann constant of C (resp. C') with respect to α (resp. α'). The Riemann constants satisfy

$$N[\Delta']=\Delta.$$

Proof. Recall that, given a curve C and an Abel-Jacobi map α of C, the Riemann constant Δ is determined by Theorem 1.2.2, hence it satisfies

$$\alpha(\mathrm{Sym}^{g-1}C)=\left\{x\in J(C):\theta[-\widetilde{\Delta}](x,\Omega)=0\right\}. \tag{1.22}$$

To prove the proposition, we will use that the Riemann constant is uniquely defined by (1.22) (see Proposition 1.2.4). We start by applying the isomorphism φ_*^{-1} to both sides of (1.22) in the case of the curve C'. We obtain

$$\varphi_*^{-1}\alpha'(\mathrm{Sym}^{g-1}C')=\left\{y\in J(C):\theta[-\widetilde{\Delta'}](\varphi_*(y),\Omega')=0\right\}. \tag{1.23}$$

Consider the subdivision in $g\times g$ blocks of the transpose of $\rho_r(\varphi_*)$

$$N=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\mathrm{Sp}_{2g}(\mathbb{Z}),$$

and recall that then the analytical representation of φ_* is ${}^t(\gamma\Omega+\delta)$ and the period matrices satisfy the equality $N(\Omega')=\Omega$, see (1.9) and (1.10) respectively.

Let $y_0\in\mathbb{C}^g$ be a representative of $y\in J(C)$, that is, an element satisfying $y=(y_0 \mod \Omega\mathbb{Z}^g+\mathbb{Z}^g)$, thus also $\varphi_*(y)=({}^t(\gamma\Omega+\delta)y_0 \mod \Omega'\mathbb{Z}^g+\mathbb{Z}^g)$. Then, by the theta transformation formula by N given in Proposition 1.3.2, we get

$$\begin{aligned}\theta[-\widetilde{\Delta'}]({}^t(\gamma\Omega+\delta)y_0,\Omega')&=\\ &=\kappa(N,\Omega',\Delta',{}^t(\gamma\Omega+\delta)y_0)^{-1}\theta[-N[\widetilde{\Delta'}]]({}^t(\gamma\Omega+\delta)^{-1}\,{}^t(\gamma\Omega+\delta)y_0,N(\Omega'))\\ &=\kappa(N,\Omega',\Delta',{}^t(\gamma\Omega+\delta)y_0)^{-1}\theta[-N[\widetilde{\Delta'}]](y_0,\Omega).\end{aligned}$$

Recall that by definition of φ_* we have $\varphi_* \circ \alpha = \alpha' \circ \varphi$. Therefore we obtain

$$\varphi_*^{-1}\alpha'(\mathrm{Sym}^{g-1} C') = \alpha(\mathrm{Sym}^{g-1} C),$$

and the equality of sets (1.23) becomes

$$\alpha(\mathrm{Sym}^{g-1} C) = \left\{ y \in J(C) : \theta[-N[\widetilde{\Delta'}]](y, \Omega) = 0 \right\}.$$

We conclude $N[\Delta'] = \Delta$ by the uniqueness of the Riemann constant. □

Now we can characterize the Riemann constant of a Picard curve with respect to the Abel-Jacobi map with base point $(0 : 1 : 0)$.

Corollary 1.3.5. Let C be a Picard curve, let ρ be the automorphism of C given by $(x, y) \mapsto (x, z_3 y)$. The Riemann constant with respect to the Abel-Jacobi map with base point $P_\infty = (0 : 1 : 0)$ is the only point $\Delta \in J(C)$ with

(1) $\Delta \in J(C)[2]$, and
(2) ${}^t\rho_r(\rho_*)[\Delta] = \Delta$.

Proof. By Proposition 1.2.4 we have $2\Delta = \alpha(\kappa)$ for κ a canonical divisor, and the computation $\mathrm{div}(dx/y^2) = 4P_\infty$ shows $\alpha(\kappa) = 0$, which proves (1). Moreover, since P_∞ is fixed by ρ, we obtain by Proposition 1.3.4 that the point Δ satisfies (2).

To prove that it is the only point that satisfies (1) and (2), assume that there exist $\Delta^1, \Delta^2 \in J(C)$ that satisfy (1) and (2). By (2) we have

$$\underline{\Delta}^1 - \underline{\Delta}^2 = {}^t\rho_r(\rho_*)[\underline{\Delta}^1] - {}^t\rho_r(\rho_*)[\underline{\Delta}^2] = \rho_r(\rho_*)^{-1}(\underline{\Delta}^1 - \underline{\Delta}^2),$$

thus $\Delta^1 - \Delta^2$ is an element of $J(C)[1 - \rho_*^2] \subseteq J(C)[3]$. But by (1), the difference $\Delta^1 - \Delta^2$ is also a 2-torsion point, hence we conclude $\Delta^1 - \Delta^2 = 0$. □

Next, we identify the images on $J(C)$ of the affine branch points of C.

Theorem 1.3.6. Let $J(C)$ be the Jacobian of a Picard curve C, let ρ_* be the automorphism of $J(C)$ induced by the curve automorphism $\rho(x, y) = (x, z_3 y)$. Let $\mathcal{B}$ be the set of affine branch points of C, let α be the Abel-Jacobi map with base point $P_\infty = (0 : 1 : 0)$, let Δ be the Riemann constant with respect to α and define

$$\Theta_3 := \{ x \in J(C)[1 - \rho_*] : \theta[x + \underline{\Delta}](\Omega) = 0 \}.$$

Then $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are the only subsets $\mathcal{T} \subseteq J(C)$ of four elements such that:

(i) the sum $\sum_{x \in \mathcal{T}} x$ is zero,
(ii) $\mathcal{T}$ is a set of generators of $J(C)[1 - \rho_*]$, and

(iii) the set $\mathcal{O}(\mathcal{T}) := \{\sum_{x\in\mathcal{T}} a_x x : a \in \mathbb{Z}^4_{\geq 0}, \sum_{x\in\mathcal{T}} a_x \leq 2\}$ satisfies

$$\mathcal{O}(\mathcal{T}) = \Theta_3.$$

Proof. We first show that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ satisfy (i)–(iii), and then we prove that these are the only possibilities.

That $\alpha(\mathcal{B})$ satisfies (i) follows from $\operatorname{div}(y) = \sum_{P\in\mathcal{B}} P - 4P_\infty$. That $\alpha(\mathcal{B})$ satisfies (ii) is proven by Koike and Weng in [16, Remark 8]. Next we prove that $\alpha(\mathcal{B})$ satisfies (iii). On the one hand, given $Q_1, Q_2 \in \mathcal{B} \cup \{P_\infty\}$ we have $\alpha(Q_1 + Q_2) \in \Theta_3$ by Riemann's Vanishing Theorem 1.2.2, and since we have $\alpha(P_\infty) = 0$, this implies

$$\left\{ \sum_{P\in\mathcal{B}} a_P \alpha(P) : a \in \mathbb{Z}^{\mathcal{B}}_{\geq 0}, \sum_{P\in\mathcal{B}} a_P \leq 2 \right\} \subseteq \Theta_3.$$

On the other hand let $x \in \Theta_3$. Since x satisfies $\theta[x + \underline{\Delta}](\Omega) = 0$, by Riemann's Vanishing Theorem 1.2.2 there exist $Q_1, Q_2 \in C$ such that we have $x = \alpha(Q_1 + Q_2)$. Moreover, since x is a $(1 - \rho_*)$-torsion point, we get

$$\alpha(Q_1 + Q_2) = \rho_*(\alpha(Q_1 + Q_2)) = \alpha(\rho(Q_1) + \rho(Q_2)),$$

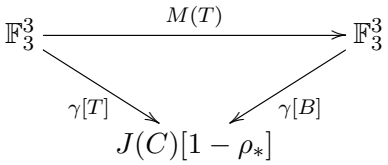
hence there exists a function h on C such that $\operatorname{div}(h) = \rho(Q_1)+\rho(Q_2)-Q_1-Q_2$. We conclude that h is constant, since otherwise it has degree at most 2, hence the curve would be hyperelliptic, contradicting Proposition 1.1.2. Therefore we have $\rho(Q_1) + \rho(Q_2) = Q_1 + Q_2$, but since ρ has order 3, the cardinality of the orbit of Q_i has length 3 or 1, thus we obtain $\rho(Q_i) = Q_i$. Therefore Q_1 and Q_2 are branch points, so the other inclusion holds.

It is clear that $-\alpha(\mathcal{B})$ satisfies (i) and (ii). To see that it satisfies (iii), it is enough to prove that Θ_3 is invariant under the map $x \mapsto -x$. But this follows from the symmetry $\theta[-x](\Omega) = \theta[x](\Omega)$ of the Riemann theta constants.

Next we prove that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are, in fact, all the subsets that satisfy (i)–(iii).

Let B denote an ordering of $\alpha(\mathcal{B})$. Given a sequence $T = (t_1, t_2, t_3, t_4)$ in $J(C)^4$ such that the set $\{t_1, t_2, t_3, t_4\}$ has 4 elements and satisfies (i)–(iii), we define the map $\gamma[T] : \mathbb{F}_3^3 \to J(C)[1 - \rho_*]$ given by $r \mapsto \sum_{i=1}^3 r_i t_i$. By Remark 8 in Koike-Weng [16] we have $\#J(C)[1 - \rho_*] \cong (\mathbb{Z}/3\mathbb{Z})^3$, thus it follows from (i) and (ii) that $\gamma[T]$ is a bijection.

Consider the diagram



where $M(T)$ is the unique invertible matrix in $\mathbb{F}_3^{3\times 3}$ that makes the diagram commutative. Note that choosing a matrix $M(T)$ determines T uniquely.

Let e_1, e_2, e_3 be the standard basis vectors of $\mathbb{F}_3^3$, and let $e_4 = -e_1 - e_2 - e_3$, so for $i = 1, \ldots, 4$ we have $\gamma[T](e_i) = t_i$. Consider

$$\mathcal{O}_0 = \left\{ \sum_{i=1}^{4} a_i e_i : a \in \mathbb{Z}_{\geq 0}^4, \sum_{i=1}^{4} a_i \leq 2 \right\} \subseteq \mathbb{F}_3^3.$$

One can check $\#\mathcal{O}_0 = 15$, and moreover we have $\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\})$. If the set of elements of T satisfies (iii), then we have

$$\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\}) = \Theta_3 = \gamma[B](\mathcal{O}_0),$$

and thus $\mathcal{O}_0$ is stable under $M(T)$.

We checked with SageMath [49] that there are exactly 48 invertible matrices in $\mathbb{F}_3^{3\times 3}$ that map $\mathcal{O}_0$ to itself. Since a matrix $M(T)$ determines T uniquely, there are 48 sequences $T \in J(C)^4$ that satisfy (i)–(iii). However, if we vary σ in the symmetric group of 4 letters and $s \in \{\pm 1\}$, then $s\sigma(B)$ gives 48 sequences, which are different. We conclude that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are the only subsets of $J(C)$ with 4 elements that satisfy (i)–(iii). □

From the proof above we obtain the following result.

Corollary 1.3.7. With the notation in Theorem 1.3.6, we get

$$\#\Theta_3 = 15.$$ □

Remark 1.3.8. With Theorem 1.3.6, we make precise the idea hinted at Corollary 11 in Koike-Weng [16]. There, they claim the existence of a 4-element set that satisfies (i) and (ii), prove that $\alpha(\mathcal{B})$ does satisfy (i) and (ii), and assume without further comments that when one finds such a set, it is $\alpha(\mathcal{B})$.

This is problematic not only because they disregard the case where the set is $-\alpha(\mathcal{B})$ but specially because they do not consider (iii) at all, but there exist 4-element sets in $J(C)$ that satisfy (i) and (ii) which are not $\alpha(\mathcal{B})$ or even $-\alpha(\mathcal{B})$.

In fact, there are $\#\,\mathrm{GL}_3(\mathbb{F}_3) = 11232$ possible sequences $T \in J(C)^4$ that satisfy (i) and (ii), hence the probability of finding one that corresponds to a permutation of B is $1/468 \approx 0.002$.

We have now all the tools to state the algorithm.

Algorithm 1.3.9

Input: The Jacobian of a Picard curve C, given by a period matrix $\Omega \in \mathbf{H}_3$, and ρ_* the automorphism on the Jacobian induced by the curve automorphism $\rho(x, y) = (x, z_3 y)$, given by its rational representation $N \in \mathbb{Z}^{6\times 6}$.

Output: The complex values λ and μ in a Legendre-Rosenhain equation $y^3 = x(x-1)(x-\lambda)(x-\mu)$ of the Picard curve C.

1. Let D be the unique solution of $N[D] = D$ in $\frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$.
2. Compute the set
$$\underline{\Theta_3} = \left\{ x \in \frac{1}{3}\mathbb{Z}^6/\mathbb{Z}^6 : Nx = x \text{ and } \theta[x+D](\Omega) = 0 \right\}$$
of cardinality 15.
3. Let $T = \{t_1, t_2, t_3, t_4\} \subseteq \underline{\Theta_3}$ be a 4-element set that satisfies
   I. $\sum_{i=1}^4 t = 0$,
   II. $\{t_1, t_2, t_3\}$ are linearly independent, and
   III. $\{\sum_{i=1}^4 a_i t_i : (a_i)_i \in \mathbb{Z}^4_{\geq 0}, \sum_{i=1}^4 a_i \leq 3\} = \underline{\Theta_3}$.
4. Compute
$$\varepsilon_\lambda = \exp(6\pi i((\widetilde{t_3} - \widetilde{t_2})_1(\widetilde{t_1})_2 + (\widetilde{t_2} + 2\widetilde{t_3} - \widetilde{D})_1(2\widetilde{D} - 3(\widetilde{t_2} + \widetilde{t_3}))_2)),$$
$$\varepsilon_\mu = \exp(6\pi i((\widetilde{t_4} - \widetilde{t_2})_1(\widetilde{t_1})_2 + (\widetilde{t_2} + 2\widetilde{t_4} - \widetilde{D})_1(2\widetilde{D} - 3(\widetilde{t_2} + \widetilde{t_4}))_2)),$$
and
$$\lambda = \varepsilon_\lambda \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^3,$$
$$\mu = \varepsilon_\mu \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^3.$$
5. Return λ and μ.

Warning 1.3.10. Algorithm 1.3.9 is a *mathematical* algorithm, but, because it involves infinite sums, complex numbers and exponentials, it cannot be run on a Turing machine or a physical computer. To do so one needs to truncate the sum on the Riemann theta constants, approximate complex numbers and keep track of the error propagation. For more details on how to do this see Section 1.5.

Proof of Algorithm 1.3.9. Let $\Delta \in J(C)$ be the Riemann constant with respect to $P_\infty = (0:1:0)$ and let $\mathcal{B}$ be the set of affine branch points of C. By Corollary 1.3.5, the point Δ is the only one that satisfies $N[\Delta] = \Delta$ and is a 2-torsion point, that is, it satisfies $\underline{\Delta} \in \frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$. We conclude $D = \underline{\Delta}$.

By Theorem 1.3.6, the sequence (t_1, t_2, t_3, t_4) is an ordering of either $\alpha(\mathcal{B})$ or $-\alpha(\mathcal{B})$. In the former case, the values λ, μ obtained in Step 4 are the x-coordinates of the affine branch points different from $(0,0)$ and $(0,1)$. A quasi-periodicity argument similar to those in the proofs of Lemma 1.2.11 or Theorem 1.2.13 yields that in the latter case that holds too. □

As a consequence of the proof we obtain the following result.

Corollary 1.3.11. If the automorphism given in the input of Algorithm 1.3.9 is ρ_*^2, then the output is also correct.

Proof. Note that the automorphism in the input only plays a role in Steps 1 and 2 of Algorithm 1.3.9, to determine the Riemann constant and the $(1-\rho_*)$-torsion points in $J(C)$.

Note that both ρ and ρ^2 fix the branch points on C. Therefore, by Proposition 1.3.4 the Riemann constant satisfies ${}^t\rho_r(\rho_*^2)[\Delta] = \Delta$. It follows that, for $M = {}^t\rho_r(\rho_*^2)$, the characteristic D in Step 1 satisfies $M[D] = D$. We also get

$$\left\{ x \in \frac{1}{3}\mathbb{Z}^6/\mathbb{Z}^6 : Mx = N^2x = x \text{ and } \theta[x+D](\Omega) = 0 \right\} = \underline{\Theta_3}. \qquad \square$$

1.4 The Torelli locus of Picard curves

In the previous section we have seen how to reconstruct a Picard curve from its Jacobian. The following theorem characterizes the abelian varieties that arise as the Jacobian of a Picard curve. It is a variation of Lemma 1 in [16], see Remark 1.4.2.

Proposition 1.4.1 (based on work of Koike-Weng and Estrada)**.** Let X be a simple principally polarized abelian variety of dimension 3 defined over an algebraically closed field k. If X has an automorphism φ of order 3, then we have $X \in J(\mathcal{P})$. Furthermore, for the curve automorphism $\rho(x,y) = (x, z_3 y)$, we get $\langle \varphi \rangle = \langle \rho_* \rangle$

Proof. Let X be a simple principally polarized abelian variety of dimension 3 with an automorphism φ of order 3. By Oort-Ueno [33], every simple principally polarized abelian variety of dimension ≤ 3 over an algebraically closed field is the Jacobian of a curve, so let C be a curve with $X \cong J(C)$.

By Torelli's Theorem 1.1.1, there is some non-trivial automorphism ν of C that satisfies $\varphi = \pm\nu_*$. Then the automorphism $\eta = \nu^4$ satisfies $\eta_* = (\nu^4)_* = (\pm\nu)_*^4 = \varphi^4 = \varphi$, hence by the uniqueness in Torelli's Theorem 1.1.1 we obtain that η has order 3.

We conclude that the automorphism η has order 3, so the degree of the map $\pi : C \to C/\langle\eta\rangle$ is also 3, and by the Riemann-Hurwitz formula one obtains that $C/\langle\eta\rangle$ has either genus 0 or 1. But X is simple, so the curve $C/\langle\eta\rangle$ is isomorphic to $\mathbb{P}^1$ and π has 5 ramification points.

Then $k(C)/k(C/\langle\eta\rangle)$ is a Kummer extension of degree 3, hence C is given by an equation of the form $y^3 = h(x)$. By Lemma 7.3 in Estrada [11, Appendix I], we obtain a model for C given by $y^3 = f(x)$ where f has degree 4 and distinct

roots and η is either the automorphism ρ given by $(x, y) \mapsto (x, z_3 y)$ or its square. □

Remark 1.4.2. While the idea behind the proof is the same in Proposition 1.4.1 and in [16, Lemma 1], the assumptions in [16] are in a way more restrictive, as Koike and Weng focus on maximal CM Picard curves (see page 33 for a definition). Moreover, the proof in [16] has a gap, which is fixed exactly by our reference to Estrada [11, Appendix I].

It follows from Proposition 1.4.1 that one can think of the input in Algorithm 1.3.9 as just a principally polarized abelian threefold with an order-3 automorphism.

1.5 Implementation and some CM examples

In this section we give some indications on how to implement Algorithm 1.3.9 so that it can run in a physical computer. In practice, in the implementation [45] we truncate the sums of the Riemann theta constants at some hypercube $[-B, B]^3 \subseteq \mathbb{Z}^3$ and use high precision floating point numbers and several checks through the implementation to make sure that the output is coherent.

If one of the checks fails or the final computation does not make sense, then we run the algorithm again for a larger bound $B \in \mathbb{Z}$. Alternatively, one could use interval arithmetic to keep track of the error propagation.

We use the following algorithm to truncate the Riemann theta constants:

Algorithm 1.5.1

Input: A real number $b \in (0, 1)$, a period matrix $\Omega \in \mathbf{H}_g$ to arbitrary precision, and a characteristic $c \in ([0, 1) \cap \mathbb{Q})^{2g}$.

Output: An approximation $\theta_b[c](\Omega)$ of $\theta[c](\Omega)$ that satisfies

$$|\theta[c](\Omega) - \theta_b[c](\Omega)| < b.$$

1. Compute $B \in \mathbb{Z}$ that satisfies
$$B > \sqrt{-\frac{\ln b + g \ln(1 - e^{-\pi\lambda(\Omega)}) - (g+1)\ln 2 - \ln g}{\pi\lambda(\Omega)}},$$
where $\lambda(\Omega)$ is the smallest eigenvalue of the imaginary part of Ω.
2. Let $b' = (2B+1)^{-g} b/2$ and for $n \in [-B, B]^g$ compute x_n that satisfies
$$|\exp(\pi i\, {}^t(n + c_1)\Omega(n + c_1) + 2\pi i\, {}^t(n + c_1)c_2) - x_n| < b'.$$
3. Return $\theta_b[c](\Omega) = \sum_{n \in [-B,B]^g} x_n$.

Proof. We will bound $|\theta_b[c](\Omega) - \theta[c](\Omega)|$. Let X and Y be respectively the real and imaginary part of Ω, so that we write $\Omega = X + iY$. Every term in the sum $\theta[c](\Omega)$ consists of an oscillatory factor F with $|F| = 1$ and a real exponential factor, hence we obtain

$$|\exp(\pi i\,{}^t(n+c_1)\Omega(n+c_1) + 2\pi i\,{}^t(n+c_1)c_2)| = \exp(-\pi\,{}^t(n+c_1)Y(n+c_1))$$

but since Y is symmetric and positive definite we get

$$|\exp(\pi i\,{}^t(n+c_1)\Omega(n+c_1) + 2\pi i\,{}^t(n+c_1)c_2)| \leq \exp(-\pi\lambda(\Omega)||n+c_1||^2),$$

and, for $Q = \exp(-\pi\lambda(\Omega))$ we have

$$\begin{aligned}
&|\theta[c](\Omega) - \theta_b[c](\Omega)| \\
&\quad \leq (2B+1)^g b' + \sum_{n\in\mathbb{Z}^g\setminus[-B,B]^g} |\exp(\pi i\,{}^t(n+c_1)\Omega(n+c_1) + 2\pi i\,{}^t(n+c_1)c_2)| \\
&\quad \leq \frac{b}{2} + \sum_{n\in\mathbb{Z}^g\setminus[-B,B]^g} Q^{||n+c_1||^2}
\end{aligned}$$

Note that for $n \in \mathbb{Z}$ and $c \in [0,1)$ we have

$$(n+c)^2 \geq \begin{cases} n^2 & \text{if } n \geq 0, \\ (n+1)^2 & \text{if } n \leq -1. \end{cases} \tag{1.24}$$

Then, in order to bound the sum above, we deal with each "quadrant" of $\mathbb{Z}^g$ separately. Using the lowerbound in (1.24) we obtain that the sum at each "quadrant" is bounded by

$$\sum_{n_1\geq B}\sum_{n_2\geq 0}\cdots\sum_{n_g\geq 0}\prod_{j=1}^{g} Q^{n_j^2},$$

and we obtain

$$\begin{aligned}
|\theta[c](\Omega) - \theta_b[c](\Omega)| &\leq \frac{b}{2} + 2^g g \sum_{n_1\geq B}\sum_{n_2\geq 0}\cdots\sum_{n_g\geq 0}\prod_{j=1}^{g} Q^{n_j^2} \\
&\leq \frac{b}{2} + 2^g g \left(\sum_{n_1\geq B} Q^{n_1^2}\right)\left(\sum_{n_2\geq 0} Q^{n_2^2}\right)\cdots\left(\sum_{n_g\geq 0} Q^{n_g^2}\right).
\end{aligned} \tag{1.25}$$

If we now apply the bound

$$\sum_{m\geq M} Q^{m^2} \leq \sum_{m\geq M^2} Q^m = \frac{Q^{M^2}}{1-Q} \text{ if } |Q| < 1$$

to (1.25), then we obtain

$$|\theta[c](\Omega) - \theta_b[c](\Omega)| \leq \frac{b}{2} + 2^g g \frac{Q^{B^2}}{(1-Q)^g},$$

which for B as in the statement implies $|\theta[c](\Omega) - \theta_b[c](\Omega)| < b$. □

Then one replaces Step 2 in Algorithm 1.3.9 by the following substeps:

I. For $b = 2^{-5}$ compute

$$\underline{\Theta_{3,b}} = \left\{ x \in \frac{1}{3}\mathbb{Z}^6/\mathbb{Z}^6 : Nx = x \text{ and } \theta_b[x + D](\Omega) < b \right\}.$$

II. If $\underline{\Theta_{3,b}}$ has more than 15 points, then square b and repeat steps I and II.

By Algorithm 1.5.1 we have

$$\underline{\Theta_3} \subseteq \underline{\Theta_{3,b}},$$

and for small enough $b > 0$ we obtain the equality. By Corollary 1.3.7, we obtain $\#\underline{\Theta_{3,b}} = 15$ in a finite number of steps.

For efficiency, we would like the smallest eigenvalue of the imaginary part of Ω to be as big as possible, due to its role in the computation of B in Algorithm 1.5.1. Since the isomorphism class of a principally polarized abelian variety only depends on the orbit of Ω under the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$, this can be achieved by choosing a representative in a certain fundamental domain of $\mathbf{H}_g$. For this we use the implementation due to Kılıçer–Streng [14] of Algorithm 2 in Labrande-Thomé [18, Section 4.1] on our period matrix before applying Algorithm 1.3.9.

Remark 1.5.2. This was enough to obtain the examples given in this section, but it might take too long for other cases. Alternatively, one could use Labrande's method [17], which computes Riemann theta functions with characteristics in quasi-linear time.

After numerically approximating the x-coordinates of the branch points of a Picard curve with Algorithm 1.3.9, we obtain a polynomial

$$f(x) = x(x-1)(x-\lambda)(x-\mu) \in \mathbb{C}[x]$$

up to some precision, while maybe the curve is actually isomorphic to $y^3 = h(x)$ for a certain polynomial h over a number field.

Given the quartic polynomial

$$p(x) = x^4 + g_2 x^2 + g_3 x + g_4 \text{ with } g_2 \neq 0$$

we define the *absolute invariants of* p as

$$j_1 = \frac{g_3^2}{g_2^3}, \qquad j_2 = \frac{g_4}{g_2^2}.$$

In order to find h from f we compute the absolute invariants of C by computing j_1 and j_2 for an isomorphic curve of the form $y^3 = x^4 + g_2x^2 + g_3x + g_4$. We then recognize j_1 and j_2 as algebraic numbers and reconstruct h from the exact absolute invariants, obtaining

$$y^3 = h(x) = x^4 + j_1x^2 + j_1^2x + j_1^2j_2.$$

Note that in order to be able to recognize j_1 and j_2 as algebraic numbers we have to compute λ and μ with enough precision.

Next we include a list of Picard curves computed with our algorithm. We define a *maximal CM Picard curve* as a Picard curve such that its Jacobian has endomorphism ring isomorphic to the maximal order of a sextic number field K. Since ρ_* is an automorphism of order 3, the field K contains a primitive 3rd root of unity $\zeta_3 \in K$. In fact, the field K is determined by a totally real cubic field K_0 that satisfies $K = K_0(\zeta_3)$.

In Section 4.1 we explain how to obtain, for a given sextic field $K = K_0(\zeta_3)$, a complete list of period matrices of principally polarized abelian varieties with endomorphism ring isomorphic to $\mathcal{O}_K$, together with the rational representation of the corresponding order-3 automorphism φ.

Using Algorithm 1.3.9 on the resulting list of pairs (Ω, N), we computed numerical approximations of some maximal CM curves. Here we present the resulting Picard curves which are numerically close (and conjecturally equal) to the maximal CM curves. In Chapter 4 we will see that, in particular, this list contains conjectural models for all Picard curves defined over $\mathbb{Q}$ with maximal CM over $\mathbb{C}$. The curves (1)–(5) also appear in [16, Section 6.1].

We obtained the following curves:

(1) $y^3 = x^4 - x$, with K_0 defined by $\nu^3 - 3\nu - 1$.

(2) $y^3 = x^4 - 2 \cdot 7^2\, x^2 + 2^3 \cdot 7^2\, x - 7^3$, with K_0 defined by $\nu^3 - \nu^2 - 2\nu + 1$.

(3) $y^3 = x^4 - 2 \cdot 7^2 \cdot 13\, x^2 + 2^3 \cdot 5 \cdot 13 \cdot 47\, x - 5^2 \cdot 13^2 \cdot 31$, with K_0 defined by $\nu^3 - \nu^2 - 4\nu - 1$.

(4) $y^3 = x^4 - 2 \cdot 7 \cdot 31 \cdot 73\, x^2 + 2^{11} \cdot 31 \cdot 47\, x - 7 \cdot 31^2 \cdot 11593$, with K_0 defined by $\nu^3 + \nu^2 - 10\nu - 8$.

(5) $y^3 = x^4 - 2 \cdot 7 \cdot 43^2 \cdot 223\, x^2 + 2^7 \cdot 11 \cdot 41 \cdot 43^2 \cdot 59\, x - 11^2 \cdot 43^3 \cdot 419 \cdot 431$, with K_0 defined by $\nu^3 - \nu^2 - 14\nu - 8$.

(6) $y^3 = x^4 - 2\cdot 3^2\cdot 5^2\cdot 7^2\,x^2 + 2^9\cdot 7^2\cdot 71\,x - 3^2\cdot 5\cdot 7^3\cdot 2621$, with K_0 defined by $\nu^3 - 21\nu - 28$.

(7) $y^3 = x^4 - 2^2\cdot 3^2\cdot 7^2\cdot 37\,x^2 + 5\cdot 7^2\cdot 149\cdot 257\,x - 2\cdot 3^2\cdot 5^2\cdot 7^3\cdot 2683$, with K_0 defined by $\nu^3 - 21\nu + 35$.

(8) $y^3 = x^4 - 2\cdot 3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\,x^2 + 2^7\cdot 11\cdot 13\cdot 59\cdot 149\,x - 3^2\cdot 5\cdot 7\cdot 13^2\cdot 17\cdot 17669$, with K_0 defined by $\nu^3 - 39\nu + 26$.

(9) For K_0 defined by $\nu^3 - \nu^2 - 6\nu + 7$, and $w^3 = 19$,

$$y^3 = x^4 + (10w^2 - 2w - 70)\,x^2 + (96w^2 - 7w - 496)\,x + (235w^2 - 215w - 1101).$$

(10) For K_0 defined by $\nu^3 - \nu^2 - 12\nu - 11$, and $w^3 = 37$,

$$y^3 = x^4 + (-2366w^2 + 490w + 24626)\,x^2 + (-257958w^2 - 686928w + 5152928)\,x + (1226851w^2 - 56922233w + 176054907).$$

(11) For K_0 defined by $\nu^3 - 109\nu - 436$, and $w^3 = 109$,

$$\begin{aligned} y^3 = x^4 &+ \big(1115888872w^2 - 4007074778w - 6321528472\big)\,x^2 \\ &+ \big(-39141169182336w^2 + 294349080537984w - 512926132238464\big)\,x \\ &+ 816342009554519305w^2 - 927632462242860 5048w \\ &+ 25684086855493144296. \end{aligned}$$

(12) For K_0 defined by $\nu^3 - \nu^2 - 42\nu - 80$, and $w^3 = 127$,

$$\begin{aligned} y^3 = x^4 &+ \big(-92075757704w^2 + 319193013538w + 721950578888\big)\,x^2 \\ &+ \big(-4940428103653824 0w^2 - 18281746350539328 0w + \\ &2167183294305193600\big)x + 21690511027003736433025w^2 - \\ &11880302908672220544980 0w + 49134882128483485627800. \end{aligned}$$

(13) For K_0 defined by $v^3 - 61v - 183$, we have four curves. The first one is defined over $\mathbb{Q}$.

$$\begin{aligned} y^3 = x^4 &- 2\cdot 3\cdot 7\cdot 61^2\cdot 1289\,x^2 + 2^3\cdot 3^7\cdot 11\cdot 41\cdot 53\cdot 61^2\,x \\ &- 3^2\cdot 7\cdot 11^2\cdot 61^3\cdot 419\cdot 4663 \end{aligned}$$

$$\begin{aligned} y^3 = x^4 &+ \big(89264v^2 - 547484v - 4059720\big)\,x^2 + \big(-29558196v^2 + 49526073v \\ &+ 772138494\big)x + 88325678v^2 - 16281030326v - 72348132021 \end{aligned}$$

(14) For K_0 defined by $v^3 - v^2 - 22v - 5$, similarly one gets:

$$y^3 = x^4 + 2\cdot 7\cdot 67\cdot 179\,x^2 + 2^3\cdot 3^3\cdot 5\cdot 67\cdot 137\,x + 5^2\cdot 7\cdot 67^2\cdot 71\cdot 89$$

$$\begin{aligned} y^3 = x^4 &+ \big(12222v^2 - 263088v - 1290744\big)\,x^2 + \big(-19721880v^2 + 232016400v \\ &+ 1277237160\big)x + 11453819175v^2 - 62791404525v - 447679991475\,. \end{aligned}$$

The family of cyclic plane quintic curves

2

A *cyclic plane quintic curve* (from now on *CPQ curve*) over $\mathbb{C}$ is a genus-6 smooth, plane, projective curve given by the equation $Y^5 = f(X, Z)$ where f is a homogeneous polynomial of degree 5 with distinct roots. Such a curve has an automorphism ρ of order 5 given by $(X : Y : Z) \mapsto (X : z_5 Y : Z)$, with $z_5 = \exp(2\pi i/5)$. It fixes the points $(\alpha : 0 : \beta)$ with $f(\alpha, \beta) = 0$, the *branch points* of C.

The isomorphisms between CPQ curves are of the form

$$(X : Y : Z) \mapsto (aX + bZ : Y : cX + dZ).$$

Therefore, every ordering of the branch points gives rise to an isomorphic model with the three first branch points at $(0 : 0 : 1)$, $(1 : 0 : 1)$ and $(1 : 0 : 0)$. In that case, if we consider the patch $Z \neq 0$ and define the affine coordinates $x = X/Z$ and $y = Y/Z$, then a CPQ curve is determined by the x-coordinates of the remaining branch points $(\lambda, 0)$ and $(\mu, 0)$ as

$$y^5 = x(x-1)(x-\lambda)(x-\mu).$$

We refer to this form as a *Legendre-Rosenhain equation of a CPQ curve*.

In this chapter we present a method that, given the period matrix of the Jacobian of a CPQ curve, computes a numerical approximation of the equation of the curve. We follow the general idea of the algorithm for Picard curves presented in Chapter 1, and we highlight the similarities and differences between both cases.

The structure of the chapter runs parallel to that of Chapter 1. In Section 2.1, we give a formula to approximate the x-coordinates of the branch points of a CPQ curve in terms of quotients of Riemann theta constants on its Jacobian, see Theorem 2.1.7.

In Section 2.2, we show how to identify the points in the Jacobian needed to apply said formula, such as the Riemann constant and the images by the Abel-Jacobi map of the branch points, see Theorem 2.2.4. We also give an inverse Jacobian algorithm for CPQ curves, that is, an algorithm that given the Jacobian of a CPQ curve C returns the x-coordinates of the branch points of C, see Algorithm 2.2.6.

Finally, in Section 2.3 we discuss how to obtain exact models from the approximations given by the algorithm, and we show some interesting examples of curves obtained using it.

2.1 A Thomae-like formula

The goal of this section is to prove a result for CPQ curves analogous to Theorem 1.2.13, that is, a formula that gives the x-coordinates of the branch points as quotients of Riemann theta constants on the Jacobian using Siegel's Theorem 1.2.6. To do so, we start by identifying a family of non-special divisors.

Definition 2.1.1. Let C be a curve, and let ω be a regular differential of C. Given a point P, a local parameter u at P and a non-negative integer n, we define the n-th derivative of ω at P with respect to u to be the complex number

$$\partial_u^n \omega(P) = n!\, a_n,$$

for $\omega = \sum_{k\geq 0} a_k u^k\, du \in \mathcal{O}_P(C)du \cong \mathbb{C}[[u]]du$ the series of ω at the local ring $\mathcal{O}_P(C)$.

Example 2.1.2. Let C be a CPQ curve with equation

$$y^5 = x^4 - 6x^3 + 11x^2 - 6x.$$

At the point $P = (0, 0)$ the function y is a local parameter, and we can write x as

$$x = \frac{1}{6}(-y^5 + x^4 - 6x^3 + 11x^2)$$

If we substitute this equation into itself recursively, then we obtain x as a power series in y,

$$x = -\frac{1}{6}y^5 + \frac{11}{216}y^{10} - \frac{103}{3888}y^{15} + \dots .$$

Consider now the regular differential $\omega = dx/y^2$. We have

$$\omega = \frac{dx}{y^2} = (-\frac{5}{6}y^2 + \frac{55}{108}y^7 - \frac{515}{1296}y^{12} + \dots)dy.$$

Therefore, the zero derivative of ω at P with respect to y is

$$\partial_y^0 \omega(P) = 0,$$

and the second derivative of ω at P with respect to y is

$$\partial_y^2 \omega(P) = -\frac{5}{3}.$$

The following proposition characterizes non-special divisors.

Proposition 2.1.3 (Siegel [44, pg. 154])**.** Let C be a curve and let $\omega_1, \ldots, \omega_g$ be a basis of regular differentials of C.

Given a point P and a positive integer n_P, consider the $g \times n_P$ matrix $W(P, n_P)$ given by the first n_P derivatives of the differentials relative to a local parameter u at the point, that is

$$W(P, n_P) = \left(\partial_u^j \omega_i(P)\right)_{\substack{1 \le i \le g \\ 0 \le j \le n_P - 1}} \in \mathbb{C}^{g \times n_P}.$$

Given $D = \sum n_P P$ an effective degree-g divisor, we define the $g \times g$ matrix $W(D)$ as the concatenation of the matrices $W(P, n_P)$ for the points P in D.

The divisor D is non-special if and only if the matrix $W(D)$ is invertible. □

In order to apply this result to the case of CPQ curves we need to choose a basis of regular differentials.

Proposition 2.1.4. Let l be a prime and let C be a curve given by an equation

$$Y^l = F(X, Z) = \prod_{i=1}^{l} (\alpha_i X - \beta_i Z)$$

such that all the branch points $P_i = (\beta_i : 0 : \alpha_i)$ for $i = 1, \ldots, l$ are distinct. Let g be the genus of C, which satisfies $g = \frac{1}{2}(l-1)(l-2)$. Consider the affine coordinates $x = X/Z$ and $y = Y/Z$. The differentials

$$\left(\frac{x^i y^j dx}{y^{l-1}} : i, j \ge 0,\ i + j \le l - 3 \right)$$

form a basis of the space of holomorphic differentials $H^0(\omega_C)$ of C.

Proof. Following [8, Section 2.9], we define the Newton polygon $\mathcal{N}(C)$ of a plane curve C given by the equation $G(x, y) = 0$ as the convex hull of all points $(i, j) \in \mathbb{Z}^2$ for which the coefficient of $x^i y^j$ in G is non-zero.

For each interior integer point $(i, j) \in \mathcal{N}(C)$, one may construct a differential

$$\omega = \frac{x^{i-1} y^{j-1} dx}{\partial_y G(x, y)}.$$

We obtain g differentials, and they are all holomorphic and linearly independent (see [8, paragraph after Equation (2.52)]).

In the case at hand we have $G(x,y) = y^l - F(x,1)$, hence the Newton polygon $\mathcal{N}(C)$ is contained in the triangle T of vertices $(0,l)$, $(l,0)$ and $(0,0)$ and contains all the interior points of T. The result follows. □

Corollary 2.1.5. Given a CPQ curve C, the differentials

$$\left(\frac{dx}{y^4}, \frac{xdx}{y^4}, \frac{x^2dx}{y^4}, \frac{dx}{y^3}, \frac{xdx}{y^3}, \frac{dx}{y^2}\right)$$

form a basis of the space of holomorphic differentials $H^0(\omega_C)$. □

This result allows us to prove that our chosen divisors are non-special.

Proposition 2.1.6. Let C be a CPQ curve and let $\mathcal{B}$ be the set of branch points of the curve C. Let $P, Q, R \in \mathcal{B}$ be distinct. Then the divisor $P + 2Q + 3R$ is non-special.

Proof. Consider the basis of differentials in Corollary 2.1.5 and compute the matrix $W(P+2Q+3R)$ as defined in Proposition 2.1.3. One checks that it has maximal rank, hence by Proposition 2.1.3 the divisor is non-special. □

We can now state a formula that gives the x-coordinates of the branch points of a CPQ curve in terms of quotients of Riemann theta constants.

Theorem 2.1.7. Let C be a CPQ curve over $\mathbb{C}$ given by a Legendre-Rosenhain equation

$$Y^5 = X(X-Z)(X-\lambda Z)(X-\mu Z)Z,$$

and consider the points $P_t = (t:0:1)$ for $t \in \{0, 1, \lambda, \mu\}$ and $P_\infty = (1:0:0)$. Let $J(C)$ be the Jacobian of C with period matrix $\Omega \in \mathbf{H}_6$, let α be the Abel-Jacobi map with base point P_∞, let Δ be the Riemann constant with respect to α, and let $\{\eta, \nu\} = \{\lambda, \mu\}$. We have

$$\eta = \varepsilon_\eta \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)} \right)^5,$$

where $\varepsilon_\eta = \exp(10\pi i((\widetilde{P_\eta} - \widetilde{P_1})_1(\widetilde{P_0})_2))$.

Proof. Let ω be the basis of holomorphic differentials for which $J(C)$ has period matrix Ω. The divisor of the function x is $\operatorname{div}(x) = 5P_0 - 5P_\infty$. Then, in order to apply Corollary 1.2.10 for $\phi = x$ and $P = P_\infty$, we choose five times the zero path from P_∞ to itself; the path γ_1 from P_∞ to P_0 that for $a_1 = \widetilde{P_0}$ satisfies

$$\int_{\gamma_1} \omega = \Omega(a_1)_1 + (a_1)_2 \in \mathbb{C}^6;$$

and, for $k = 2, \ldots, 5$, some paths γ_k from P_∞ to P_0 that satisfy

$$\sum_{k=1}^{5} \int_{\gamma_k} \omega = 0 \text{ in } \mathbb{C}^6.$$

For $k = 2, \ldots, 5$ we denote by a_k be the element in $\mathbb{R}^{12}$ that satisfies

$$\int_{\gamma_k} \omega = \Omega(a_k)_1 + (a_k)_2.$$

By Corollary 1.2.10, given an effective divisor D of degree 6 we have

$$\phi(D) = E' \prod_{k=1}^{5} \frac{\theta[\widetilde{D} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)} \tag{2.1}$$

for some constant E' independent of D.

Consider now the divisors $D_\eta = P_1 + 2P_\eta + 3P_\nu$ and $D_1 = 2P_1 + P_\eta + 3P_\nu$, which are general because of Proposition 2.1.6, and divide the corresponding equalities given by (2.1). We obtain

$$\begin{aligned} \eta &= \frac{\phi(P_\eta)}{\phi(P_1)} = \frac{\phi(D_\eta)}{\phi(D_1)} \\ &= \prod_{k=0}^{5} \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - a_k - \widetilde{\Delta}](\Omega)} \right). \end{aligned} \tag{2.2}$$

The result then follows from applying the quasi-periodicity property of the Riemann theta constants to the equation (2.2), as we did in the proof of Theorem 1.2.13. □

2.2 The inverse Jacobian algorithm

The end goal of this section is to provide an algorithm that, given a period matrix of the Jacobian of a CPQ curve and the rational representation of its induced automorphism ρ_*, returns a numerical approximation of the x-coordinates of the branch points of C.

The main step in the algorithm is based on Theorem 2.1.7. To apply that theorem we need to identify the Riemann constant of C with respect to an Abel-Jacobi map α with a branch point as base point and the image by α of the branch points on $J(C)$.

We start by characterizing the Riemann constant of a CPQ curve.

Corollary 2.2.1. Let C be a CPQ curve, let ρ be the automorphism given by $(x, y) \mapsto (x, z_5 y)$. Let α be an Abel-Jacobi map with a branch point as base point. The Riemann constant with respect to α is the only point $\Delta \in J(C)$ with

(1) $\Delta \in J(C)[2]$, and
(2) ${}^t\rho_r(\rho_*)[\Delta] = \Delta$.

Proof. Let $P_0 \in \mathcal{B}$ be the base point of the Abel-Jacobi map α. By Proposition 1.2.4 the Riemann constant satisfies $2\Delta = \alpha(\kappa)$ for κ a canonical divisor. Since we have

$$\operatorname{div}\left(\frac{(x - x(P_0))^2 dx}{y^4}\right) = 10P_0,$$

we conclude that Δ is a 2-torsion point, that is, the point Δ satisfies (1). Moreover, by Proposition 1.3.4 we have $\Delta = \rho_r(\rho_*)[\Delta']$ for Δ' the Riemann constant with respect to $\rho(P_0)$. But since P_0 is fixed by ρ, the point Δ satisfies (2).

To prove that it is the only point that satisfies (1) and (2), assume that there exist $\Delta^1, \Delta^2 \in J(C)$ that satisfy (1) and (2). By (2) we have

$$\underline{\Delta}^1 - \underline{\Delta}^2 = {}^t\rho_r(\rho_*)[\underline{\Delta}^1] - {}^t\rho_r(\rho_*)[\underline{\Delta}^2] = \rho_r(\rho_*)^{-1}(\underline{\Delta}^1 - \underline{\Delta}^2),$$

thus $\Delta^1 - \Delta^2$ is an element of $J(C)[1 - \rho_*^4] \subseteq J(C)[5]$. But by (1), the difference $\Delta^1 - \Delta^2$ is also a 2-torsion point, hence we conclude $\Delta^1 - \Delta^2 = 0$. □

Next we are interested in identifying the images of the branch points in the Jacobian. We aim to state a theorem analogous to Theorem 1.3.6 for CPQ curves, hence we start by studying the $(1 - \rho_*)$-torsion of the Jacobian.

Proposition 2.2.2. Let l be a prime, let C be a curve given by an equation

$$Y^l = F(X, Z) = \prod_{i=1}^{l} (\alpha_i X - \beta_i Z)$$

such that all the branch points $P_i = (\beta_i : 0 : \alpha_i)$ for $i = 1, \ldots, l$ are distinct, and let $\mathcal{B}$ be the set of branch points. Let ρ be the automorphism of C given by $\rho(X : Y : Z) = (X : z_l Y : Z)$ with $z_l = \exp(2\pi i/l)$. We have

$$J(C)[1 - \rho_*] = \langle [P_i - P_l] : 1 \leq i < l \rangle,$$

where all the points $[P_i - P_l]$ are distinct and satisfy $\sum_{i=1}^{l-1} [P_i - P_l] = 0$.

One of the steps in the proof is to compute $\#J(C)[1 - \rho_*] = \deg(1 - \rho_*)$. To do so, we use the following lemma.

Lemma 2.2.3 (Birkenhake-Lange [2, Section 5.1])**.** Let $X = V/\Lambda$ be an abelian variety over $\mathbb{C}$, and let $f \in \mathrm{End}(X)$ be an endomorphism with characteristic polynomial $P_f^r(t) := \det(t\,\mathrm{id}_\Lambda - \rho_r(f))$. Then for all $n \in \mathbb{Z}$ we have

$$\deg(n - f) = P_f^r(n). \qquad \square$$

Proof of Proposition 2.2.2. Let $\mathcal{B} = \{P_i : 1 \le i \le l\}$ be the set of branch points of C, define the group $\mathcal{D} := \{D \in \mathrm{Div}^0(C) : \mathrm{Supp}(D) \subseteq \mathcal{B}\} \cong \mathbb{Z}^{l-1}$, and consider the map

$$\begin{aligned} \Psi : \mathcal{D} &\to \mathrm{Pic}^0(C)[1 - \rho_*] = J(C)[1 - \rho_*], \\ D &\mapsto [D]. \end{aligned}$$

We start by computing the kernel of Ψ. Let $D \in \mathcal{D}$ be a principal divisor, say $D = \mathrm{div}(h)$. Then h satisfies

$$\mathrm{div}(h \circ \rho) = \rho^* D = D = \mathrm{div}(h),$$

so we get $h \circ \rho = c \cdot h$ for some $c \in \mathbb{C}^\times$. Actually, we obtain $c = z_l^m$ for some $m \in \mathbb{Z}/l\mathbb{Z}$.

Consider now $x = X/Z$ and $y = Y/Z$, define the function

$$g = \frac{Y}{\alpha_l X - \beta_l Z} = \frac{y}{\alpha_l x - \beta_l},$$

and note that it satisfies $g^m \circ \rho = z_l^m g^m$ and $\mathrm{div}(g) = \sum_{P \in \mathcal{B}} P - lP_l \in \mathcal{D}$.

It follows that the function $h/g^m \in \mathbb{C}(x)[y]/(y^l - F(x,1))$ satisfies

$$\frac{h}{g^m} \circ \rho = \frac{h}{g^m},$$

so that we actually have $h/g^m \in \mathbb{C}(x)$ and we can write $h = g^m f$ for some function $f \in \mathbb{C}(x)$ whose divisor is also in $\mathcal{D}$.

Since the function f only depends on x, the morphism $f : C \to \mathbb{P}^1$ factors through $C/\langle\rho\rangle$. Thus the divisor of f is the pullback by $\pi : C \to C/\langle\rho\rangle$ of a function f' on $\mathbb{P}^1$ of degree l and which is ramified at the branch points of C.

We conclude

$$D = \mathrm{div}(h) = m\,\mathrm{div}(g) + \pi^*\,\mathrm{div}(f') = m\,\mathrm{div}(g) + l \cdot D' \text{ for some } D' \in \mathcal{D},$$

and therefore we obtain

$$\ker \Psi \subseteq l\mathcal{D} + \mathbb{Z}\,\mathrm{div}(g). \tag{2.3}$$

Clearly we have $\operatorname{div}(g) \in \ker \Psi$. Moreover, for $k = 1, \ldots, l$, the function

$$\phi_k = \frac{\alpha_k X - \beta_k Z}{\alpha_l X - \beta_l Z}$$

has divisor $\operatorname{div} \phi_k = lP_k - lP_l$, so we obtain $l\mathcal{D} \subseteq \ker \Psi$; and the equality in (2.3) holds.

Altogether we obtain $\operatorname{Im} \Psi \cong \mathcal{D}/\ker \Psi \cong (\mathbb{Z}/l\mathbb{Z})^{l-1}/\langle (1, \ldots, 1) \rangle$, so $\operatorname{Im} \Psi$ has l^{l-2} elements.

Since the minimal polynomial of the automorphism ρ_* is the cyclotomic polynomial $\prod_{k=1}^{l-1}(x - z_l^k) \in \mathbb{Q}[x]$, which is irreducible, and its characteristic polynomial has degree $2g = (l-1)(l-2)$, we get

$$P_f^r(t) = \prod_{k=1}^{l-1}(x - z_l^k)^{l-2} \in \mathbb{Q}[x].$$

Then by Lemma 2.2.3 we obtain

$$\deg(1 - \rho_*) = \prod_{k=1}^{l-1}(1 - z_l^k)^{l-2} = l^{l-2}.$$

It follows that $J(C)[1-\rho_*]$ has l^{l-2} elements, so we conclude that Ψ is surjective and the result follows. □

We can now prove the theorem that allows us to identify the image of the branch points in the Jacobian.

Theorem 2.2.4. Let $J(C)$ be the Jacobian of a CPQ curve C with period matrix $\Omega \in \mathbf{H}_6$, let ρ_* be the automorphism on $J(C)$ induced by the curve automorphism $\rho(x, y) = (x, z_5 y)$ and let $\mathcal{B}$ be the set of branch points of C. Let Δ be the only point in $J(C)[2]$ that satisfies $\rho_r(\rho_*)[\Delta] = \Delta$ and define

$$\Theta_5 := \{x \in J(C)[1 - \rho_*] : \theta[\underline{x} + \underline{\Delta}](\Omega) = 0\}.$$

Then there exists a subset $\mathcal{T} \subseteq J(C)$ of four elements such that:

(i) the sum $\sum_{x \in \mathcal{T}} x$ is zero,
(ii) $\mathcal{T}$ is a set of generators of $J(C)[1 - \rho_*]$, and
(iii) the set $\mathcal{O}(\mathcal{T}) := \{\sum_{x \in \mathcal{T}} a_x x : a \in \mathbb{Z}^4_{\geq 0}, \sum_{x \in \mathcal{T}} a_x \leq 5\}$ satisfies

$$\mathcal{O}(\mathcal{T}) = \Theta_5.$$

Furthermore, for every such subset there exists $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ for which $\mathcal{T}$ satisfies

$$\mathcal{T} = \{\kappa[P - Q] : P \in \mathcal{B} \backslash \{Q\}\}.$$

Proof. Let $Q \in \mathcal{B}$ and let $\mathcal{S}_Q$ denote the set $\{[P-Q] : P \in \mathcal{B}\backslash\{Q\}\}$

We start by proving that $\mathcal{S}_Q$ satisfies (i)–(iii), and then we prove so for $\kappa\mathcal{S}_Q$ with $\kappa \in \mathbb{F}_5^\times$. Finally we prove that the sets $\kappa\mathcal{S}_Q$ as κ ranges over $\mathbb{F}_5^\times$ and Q over $\mathcal{B}$ are the only 4-element sets in $J(C)$ that satisfy (i)–(iii). We assume without loss of generality that Q is an affine point (because no statement depends on the model).

That $\mathcal{S}_Q$ satisfies (i) follows from

$$\operatorname{div}\left(\frac{y}{x-x(Q)}\right) = \sum_{P\in\mathcal{B}} P - 5Q.$$

That $\mathcal{S}_Q$ satisfies (ii) follows from Proposition 2.2.2.

Next we prove that $\mathcal{S}_Q$ satisfies (iii). Let α be the Abel-Jacobi map with a branch point $P' \in \mathcal{B}$ as base point so by Corollary 2.2.1 the point Δ is the Riemann constant with respect to α.

Given $Q_1, \ldots, Q_5 \in \mathcal{B}$, we have $\alpha(Q_1 + \cdots + Q_5) \in \Theta_5$ by the Riemann Vanishing Theorem 1.2.2. We also have $5\alpha(Q) = 0$, since the divisor of the function $(x - x(Q))/(x - x(P'))$ is $5Q - 5P'$. Therefore we write

$$\alpha(Q_1 - Q) + \cdots + \alpha(Q_5 - Q) = \alpha(Q_1 + \cdots + Q_5) \in \Theta_5,$$

which by definition of $\mathcal{O}(S_Q)$ implies

$$\mathcal{O}(\mathcal{S}_Q) \subseteq \Theta_5. \tag{2.4}$$

To prove that it is actually an equality, we show that the sets have the same cardinality.

First we give a lower-bound for $\#\Theta_5$ via computing $\#\mathcal{O}(S_Q)$. Given a sequence $T = (t_1, t_2, t_3, t_4)$ such that the set $\{t_1, t_2, t_3, t_4\}$ has 4 elements and satisfies (i)–(ii), we define the map $\gamma[T] : \mathbb{F}_5^3 \to J(C)[1-\rho_*]$ that maps $r \in \mathbb{F}_5^3$ to the sum $\sum_{i=1}^3 r_i t_i \in J(C)[1-\rho_*]$. Note that $\gamma[T]$ is a bijection.

Let e_1, e_2, e_3 be the standard basis vectors of $\mathbb{F}_5^3$, and let $e_4 = -e_1 - e_2 - e_3$, so for $i = 1, \ldots, 4$ we have $\gamma[T](e_i) = t_i$. Consider

$$\mathcal{O}_0 = \left\{ \sum_{i=1}^4 a_i e_i : a \in \mathbb{Z}^4_{\geq 0}, \sum_{i=1}^4 a_i \leq 5 \right\} \subseteq \mathbb{F}_5^3.$$

One can check $\#\mathcal{O}_0 = 101$, and moreover we have $\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, \ldots, t_4\})$.

In particular, we obtain $\#\mathcal{O}(\mathcal{S}_Q) = 101$ and thus by (2.4) we get

$$\#\Theta_5 \geq 101. \tag{2.5}$$

Next we give an upper-bound for $\#\Theta_5$. By Proposition 2.1.6 the divisors $3P + 2Q + R$ with P, Q, R distinct branch points are non-special, that is, they

satisfy $\deg D = g$ and $\dim \mathcal{L}(\kappa - D) = 0$. Therefore by the Riemann-Roch Theorem they are the only effective divisor in their class. In particular, if P, Q, R are different from P' then we have $\alpha(3P+2Q+R) \neq \alpha(Q_1+\cdots+Q_5)$ for every $Q_1, \ldots, Q_5 \in C$, so by Riemann's Vanishing Theorem 1.2.2 we obtain that $\theta[3\underline{P} + 2\underline{Q} + \underline{R} - \underline{\Delta}](\Omega)$ is non-zero.

There are 24 such divisors with $\{P, Q, R\} \not\ni P'$, which in turn determine 24 distinct divisor classes, hence we conclude

$$\#\{x \in J(C)[1-\rho_*] : \theta[x + \underline{\Delta}](\Omega) \neq 0\} \geq 24. \tag{2.6}$$

Since by Proposition 2.2.2 we have $\#J(C)[1-\rho_*] = 125$, it follows that both (2.5) and (2.6) are equalities and therefore $\mathcal{S}_Q$ satisfies (iii).

Next we consider the sets $\kappa\mathcal{S}_Q$ with $\kappa \in \mathbb{F}_5^\times$. It is clear that $\kappa\mathcal{S}_Q$ also satisfies (i)–(ii). We checked with Magma [3] that $\mathcal{O}_0$ is invariant under the map $x \mapsto \kappa x$ for $\kappa \in \mathbb{F}_5^\times$, and we have the equality

$$\gamma[\kappa T](\mathcal{O}_0) = \gamma[T](\kappa\mathcal{O}),$$

so it follows that (iii) also holds for $\kappa\mathcal{S}_Q$.

Finally, we prove that the 4-element sets κS_Q for $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ are the only 4-element sets in $J(C)$ that satisfy (i)–(iii). To do so, let B denote an ordering of $\mathcal{S}_{P'} = \alpha(\mathcal{B})\backslash\{0\}$, consider a sequence $T = (t_1, t_2, t_3, t_4) \in J(C)^4$ such that the set $\{t_1, t_2, t_3, t_4\}$ has 4 elements and satisfies (i)–(iii), and let $\gamma[T]$ be the bijection defined above. Consider the diagram

$$\begin{array}{ccc} \mathbb{F}_5^3 & \xrightarrow{\quad M(T) \quad} & \mathbb{F}_5^3 \\ & {\scriptstyle\gamma[T]}\searrow \quad \swarrow{\scriptstyle\gamma[B]} & \\ & J(C)[1-\rho_*] & \end{array}$$

where $M(T)$ is the unique invertible matrix in $\mathbb{F}_5^{3\times 3}$ that makes the diagram commutative. Note that choosing a matrix $M(T)$ determines T uniquely.

If the set of elements of T satisfies (iii), then we get

$$\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\}) = \Theta_5 = \gamma[B](\mathcal{O}_0),$$

and thus $\mathcal{O}_0$ is stable under $M(T)$.

We checked with Magma [3] that there are exactly 480 invertible matrices in $\mathbb{F}_5^{3\times 3}$ that map $\mathcal{O}_0$ to itself. Since a matrix $M(T)$ determines T uniquely, there are 480 sequences $T \in J(C)^4$ that satisfy (i)–(iii). However, if we vary $\kappa \in \mathbb{F}_5^\times$, the point $Q \in \mathcal{B}$, and the labeling of the elements in $\mathcal{S}_Q$ we get 480 sequences, and they are different by the equality in (2.3), see proof of Proposition 2.2.2. We conclude that κS_Q for $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ are the only 4-element subsets of $J(C)$ that satisfy (i)–(iii). □

From the proof above we obtain the following result.

Corollary 2.2.5. With the notation in Theorem 1.3.6, we get

$$\#\Theta_5 = 101.$$ □

We have now all the tools to give the inverse Jacobian algorithm.

Algorithm 2.2.6

Input: The Jacobian of a CPQ curve C, given by a period matrix $\Omega \in \mathbf{H}_6$, and ρ_* the automorphism on the Jacobian induced by the curve automorphism $\rho(x,y) = (x, z_5 y)$, given by its rational representation $N \in \mathbb{Z}^{12\times 12}$.

Output: Two pairs (l,m) of which at least one is the pair (λ,μ) in a Legendre-Rosenhain equation $y^5 = x(x-1)(x-\lambda)(x-\mu)$ of the CPQ curve C.

1. Let D be the unique solution of $N[D] = D$ in $\frac{1}{2}\mathbb{Z}^{12}/\mathbb{Z}^{12}$.
2. Compute
$$\underline{\Theta_5} = \left\{ \frac{1}{5}\mathbb{Z}^{12}/\mathbb{Z}^{12} : Nx = x \text{ and } \theta[x+D](\Omega) = 0 \right\}.$$
3. Let $X = \{x_1, x_2, x_3, x_4\} \subseteq \underline{\Theta_5}$ be a 4-element set that satisfies
   I. $\sum_{x\in X} x = 0$,
   II. $\{x_1, x_2, x_3\}$ are linearly independent, and
   III. $\{\sum_{x\in X} a_x x : a \in \mathbb{Z}^X_{\geq 0}, \sum_{x\in X} a_x \leq 5\} = \underline{\Theta_5}$.
4. For each $T = \{t_1, t_2, t_3, t_4\} \in \{X, 2X\}$ compute
$$\varepsilon_l = \exp(10\pi i((\widetilde{t_3} - \widetilde{t_2})_1 (\widetilde{t_1})_2)),$$
$$\varepsilon_m = \exp(10\pi i((\widetilde{t_4} - \widetilde{t_2})_1 (\widetilde{t_1})_2),$$
and
$$l_T = \varepsilon_l \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_3} + 3\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[\widetilde{t_2} + 2\widetilde{t_3} + 3\widetilde{t_4} - \widetilde{D}](\Omega)} \frac{\theta[2\widetilde{t_2} + \widetilde{t_3} + 3\widetilde{t_4} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_3} + 3\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^5,$$
$$m_T = \varepsilon_m \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_4} + 3\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[\widetilde{t_2} + 2\widetilde{t_4} + 3\widetilde{t_3} - \widetilde{D}](\Omega)} \frac{\theta[2\widetilde{t_2} + \widetilde{t_4} + 3\widetilde{t_3} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_4} + 3\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^5.$$
5. Return (l_X, m_X) and (l_{2X}, m_{2X}).

Warning 2.2.7. As we already saw in the case of Picard curves, Algorithm 2.2.6 is a *mathematical* algorithm but, since it involves infinite sums, complex numbers and exponentials, it cannot be run on a Turing machine or a physical computer. To do so one needs to truncate the sum on the Riemann theta constants, approximate complex numbers and keep track of the error propagation, see Section 1.5 for more details on how to do that.

After applying the algorithm, we obtain two candidates for the approximations of λ and μ. One may then use an algorithm to check which results are correct.

Let (l, m) be one of the pairs from the output, let C be the associated Legendre-Rosenhain equation and let $\Omega' \in \mathbf{H}_6$ satisfy $J(C) \cong \mathbb{C}^6/\Omega'\mathbb{Z}^6 + \mathbb{Z}^6$. If the pair (l, m) is an approximation of (λ, μ), then there exists an isomorphism between $\mathbb{C}^6/\Omega\mathbb{Z}^6 + \mathbb{Z}^6$ and $\mathbb{C}^6/\Omega'\mathbb{Z}^6 + \mathbb{Z}^6$.

One could find such an isomorphism using methods like the numerical computation of homomorphisms in Costa-Mascot-Sijsling-Voight [7].

Remark 2.2.8. In all the cases where we have applied Algorithm 2.2.6 (see Section 2.3), both pairs (l_X, m_X) and (l_{2X}, m_{2X}) yielded isomorphic curves.

Proof of Algorithm 2.2.6. Let $\mathcal{B}$ be the set of branch points of C. By Theorem 2.2.4, the set X in Step 3 is equal to $\{\kappa\underline{[P - P_\infty]} : P \in \mathcal{B}\backslash\{P_\infty\}\}$ for a certain $\kappa \in \mathbb{F}_5^\times$ and $P_\infty \in \mathcal{B}$. We assume without loss of generality $P_\infty = (1 : 0 : 0)$, and that C is given by a Legendre-Rosenhain equation. Let α be the Abel-Jacobi map with base point P_∞. Then we obtain

$$\alpha(\mathcal{B})\backslash\{0\} \in \{X, 2X, -X, -2X\}.$$

Let $\Delta \in J(C)$ be the Riemann constant Δ with respect to P_∞. By Corollary 2.2.1, the Riemann constant Δ is the only point in $J(C)$ that is a 2-torsion point, hence satisfies $\underline{\Delta} \in \frac{1}{2}\mathbb{Z}^{12}/\mathbb{Z}^{12}$, and also satisfies $N[\Delta] = \Delta$. We conclude $D = \underline{\Delta}$ and by Theorem 2.1.7, the pair (l_T, m_T) as in Step 6 is the pair (λ, μ) for some $T \in \{X, 2X, -X, -2X\}$.

Furthermore, since the Riemann theta constants are symmetric and quasi-periodic, the values of l and m do not change if we replace $\widetilde{t_i}$ by $-\widetilde{t_i}$, thus we only need to consider $T \in \{X, 2X\}$, which completes the proof. □

As a consequence of the proof we obtain the following result.

Corollary 2.2.9. If the automorphism given in the input on Algorithm 2.2.6 is ρ_*^k for some $k \in \{2, 3, 4\}$, then the output is also correct.

Proof. Note that the automorphism in the input only plays a role in Steps 1 and 2 of Algorithm 1.3.9, to determine the Riemann constant and the $(1 - \rho_*)$-torsion points in $J(C)$.

Let $k \in \{2, 3, 4\}$ and let α be an Abel-Jacobi map with a branch point as base point. Note that ρ^k fixes the branch points on C. Therefore, by Proposition 1.3.4 the Riemann constant with respect to α satisfies ${}^t\rho_r(\rho_*^k)[\Delta] = \Delta$. It follows that, for $M = {}^t\rho_r(\rho_*^k)$, the characteristic D in Step 1 satisfies $M[D] = D$. We also get

$$\left\{x \in \frac{1}{5}\mathbb{Z}^{12}/\mathbb{Z}^{12} : Mx = N^k x = x \text{ and } \theta[x + D](\Omega) = 0\right\} = \underline{\Theta_5}. \qquad \square$$

2.3 Some CM examples

As in the Picard case (see Section 1.5), after numerically approximating the x-coordinates of the branch points of a CPQ curve with Algorithm 2.2.6, we obtain a polynomial

$$f(x) = x(x-1)(x-\lambda)(x-\mu) \in \mathbb{C}[x]$$

up to some precision. However, the curve may actually be isomorphic to $y^5 = h(x)$ for a certain polynomial h over a number field.

In this case, in order to find h from f we use the invariants of quintic binary forms, recognize them as algebraic numbers and reconstruct h from the exact invariants. This was originally done by Clebsch in [6] and recently implemented by Noordsij in [32, 31].

Note that in order to be able to recognize the invariants as algebraic numbers we have to compute λ and μ with enough precision.

Next we include a list of CPQ curves computed with our algorithm. Analogously to what we saw for Picard curves in Section 1.5, we define a *maximal CM CPQ curve* as a CPQ curve such that its Jacobian has endomorphism ring isomorphic to the maximal order of a degree-12 number field K. We will see in Chapter 4 that K contains a primitive 5th root of unity $\zeta_5 \in K$, and is determined by a totally real cubic field K_0 that satisfies $K = K_0(\zeta_5)$.

For details on how to obtain period matrices for the Jacobians of maximal CM CPQ curves and the corresponding automorphism from the field K see Section 4.1.

Using Algorithm 2.2.6 we computed numerical approximations of some maximal CM curves. Here we present the resulting CPQ curves which are numerically close (and conjecturally equal) to the maximal CM curves. In Chapter 4 we will see that, in particular, this list contains conjectural models for all CPQ curves defined over $\mathbb{Q}$ with maximal CM over $\mathbb{C}$.

We obtained the following curves:

(1) $y^5 = x^4 - 24x^3 + 3x^2 + x$ with K_0 defined by $x^3 - 3x - 1$.
(2) $y^5 = x^4 - 7x^2 + 7x$ with K_0 defined by $x^3 - x^2 - 2x + 1$.
(3) $y^5 = x^4 - 390x^2 + 13000x + 257725$ with K_0 defined by $x^3 - x^2 - 4x - 1$.
(4) $y^5 = x^4 + 1290x^2 + 35000x + 228525$ with K_0 defined by $x^3 - 12x - 14$.

Moduli of abelian varieties with generalized CM-type

3

The goal for this chapter is to characterize the Jacobians of CPQ curves among the principally polarized abelian varieties of dimension 6, as an analogous result to Proposition 1.4.1 for Picard curves, which said that all simple principally polarized abelian threefolds over an algebraically closed field with order-3 automorphisms are Jacobians of Picard curves.

But when considering the case of CPQ curves, we have to take into account that not all principally polarized abelian varieties of dimension 6 are Jacobians of curves. Fortunately, the existence of the automorphism of CPQ curves given by $(x, y) \mapsto (x, \exp(2\pi i/5)y)$ and the corresponding automorphism on the Jacobian set some conditions on the structure of the Jacobian. We will show that these conditions are enough to determine a moduli space with the same dimension as the family of CPQ curves, and that said moduli space is connected. This will allow us to give a result analogous to Proposition 1.4.1, see Theorem 3.5.3.

In Sections 3.1 and 3.2 we introduce a generalization of the classical CM-theory due to Shimura to define the moduli space of principally polarized abelian varieties with given *generalized CM-type*. We follow [39], and also Birkenhake-Lange [2, Section 9.6].

We apply this theory in Section 3.3 to study the Jacobians of CPQ curves. We explicitly construct the complex torus and polarization, and study the structure of $\mathbb{Z}[\rho_*] \subseteq \mathrm{End}(J(C))$ for ρ_* the automorphism of the Jacobian induced by $\rho(x, y) = (x, z_5 y)$ with $z_5 = \exp(2\pi i/5)$. We show that the moduli space of principally polarized abelian varieties with the generalized CM-type $\mathfrak{Z}$ induced by ρ_* has dimension 2, as does the family of CPQ curves.

In Section 3.4 we introduce the concept of *polarized $\mathcal{O}_K$-lattice* and explain how the equivalence classes of certain polarized $\mathcal{O}_K$-lattices relate to the connected components of the moduli space of principally polarized abelian varieties

with generalized CM-type $\mathfrak{Z}$. Using this relation we then prove, among other things, that the moduli space given in Section 3.3 is connected.

Finally, in Section 3.5 we put all the pieces together to prove the result analogous to Proposition 1.4.1, see Theorem 3.5.3.

3.1 CM-fields and m-CM-types

A *CM-field* is a totally imaginary quadratic extension K of a totally real number field K^+. The non-trivial element κ of $\mathrm{Aut}(K/K^+)$ satisfies $\phi\circ\kappa = \bar{\cdot}\circ\phi$ for every embedding $\phi : K \hookrightarrow \mathbb{C}$, where $\bar{\cdot}$ stands for the complex conjugation in $\mathbb{C}$. We call κ *complex conjugation* and denote it also by $\bar{\cdot}$.

Let K be a CM-field of degree $2e$. An *m-CM-type* of K is a multiset Ψ whose elements are elements of $\mathrm{Hom}(K,\mathbb{C})$ and such that for every homomorphism $\phi : K \to \mathbb{C}$ we have $\mathrm{mult}_\Psi(\phi) + \mathrm{mult}_\Psi(\overline{\phi}) = m$. We get $\#\Psi = em$. To it, we associate the representation

$$\rho_\Psi = \bigoplus_{\phi\in\Psi} \phi$$

of dimension em over $\mathbb{C}$.

Definition 3.1.1. With the notation above, a *polarized abelian variety with m-CM-type* (K,Ψ) is a triple (X,E,ι) with:

- $X \cong \mathbb{C}^{em}/\Lambda$ a complex torus of dimension em,
- E a Riemann form, and
- $\iota : K \hookrightarrow \mathrm{End}(X)\otimes\mathbb{Q}$ an embedding such that
  - the analytic representation $\rho_a\circ\iota$ and the representation ρ_Ψ are equivalent, and
  - the Rosati involution on $\mathrm{End}(X)\otimes\mathbb{Q}$ with respect to the polarization given by the Riemann form E extends the complex conjugation on K via ι.

Two polarized abelian varieties (X,E,ι) and (X',E',ι') with m-CM-type (K,Ψ) are *isomorphic* if there exists an isomorphism $f : X \to X'$ that satisfies $f^*E' = E$ and $f\circ\iota(a) = \iota'(a)\circ f$ for all $a \in K$.

Choose $\Phi = (\phi_1,\dots,\phi_e)$ a sequence of e embeddings $K \to \mathbb{C}$ such that $\{\phi_1,\overline{\phi_1},\dots,\phi_e,\overline{\phi_e}\}$ is the set of all $2e$ embeddings. Then, by abuse of notation, an m-CM-type is a list $(\mathbf{r},\mathbf{s}) = ((r_1,\dots,r_e),(s_1,\dots,s_e))$ of non-negative integers with $r_i + s_i = m$ for all $i = 1,\dots,e$ via taking $r_i = \mathrm{mult}(\phi_i)$ and $s_i = \mathrm{mult}(\overline{\phi_i})$. In this case we denote the m-CM-type by $(\mathbf{r},\mathbf{s})$, and the associated representation is given by

$$\rho_{\mathbf{r},\mathbf{s}}(a) = \mathrm{diag}(\phi_1(a)\mathbf{1}_{r_1},\overline{\phi_1}(a)\mathbf{1}_{s_1},\dots,\phi_e(a)\mathbf{1}_{r_e},\overline{\phi_e}(a)\mathbf{1}_{s_e}). \tag{3.1}$$

The choice of Φ also determines an embedding $\jmath : (K \otimes_{\mathbb{Q}} \mathbb{R})^m \to \mathbb{C}^{2em}$, given by

$$\mathbf{a} \mapsto \jmath(\mathbf{a}) = \begin{pmatrix} \phi_1(\mathbf{a}) \\ \overline{\phi_1}(\mathbf{a}) \\ \vdots \\ \phi_e(\mathbf{a}) \\ \overline{\phi_e}(\mathbf{a}) \end{pmatrix},$$

and it allows us to define a parametrization of the family of polarized abelian varieties with m-CM-type $(\mathbf{r}, \mathbf{s})$ as follows:

Let $\mathcal{H}_{r,s}$ be the set of matrices $Z \in \mathbb{C}^{r\times s}$ such that $\mathbf{1}_s - {}^t\overline{Z}Z$ is positive definite, which we write as $\mathbf{1}_s - {}^t\overline{Z}Z > 0$. Let $\Upsilon(\mathbf{r}, \mathbf{s})$ be the set of pairs $(\mathcal{M}, T)$ such that:

- ▷ $\mathcal{M}$ is a free $\mathbb{Z}$-submodule of K^m of rank $2em$,
- ▷ T is an $m \times m$ antihermitian matrix over K,
- ▷ the alternating bilinear form $\mathcal{M} \times \mathcal{M} \to \mathbb{Q}$ given by $(a, b) \mapsto \mathrm{tr}_{K/\mathbb{Q}}({}^taT\bar{b})$ is integer-valued,
- ▷ T has *signature* $(\mathbf{r}, \mathbf{s})$, that is, for every $\nu = 1, \ldots, e$ there exists an invertible matrix $W_\nu \in \mathbb{C}^{m\times m}$ that satisfies

$$\phi_\nu(T) = {}^t\overline{W_\nu} \begin{pmatrix} i\mathbf{1}_{r_\nu} & 0 \\ 0 & -i\mathbf{1}_{s_\nu} \end{pmatrix} W_\nu. \tag{3.2}$$

Remark 3.1.2. One can check that $\mathbf{1}_r - Z\,{}^t\overline{Z} = (\mathbf{1}_r + Z(\mathbf{1}_s - {}^t\overline{Z}Z)^{-1}\,{}^t\overline{Z})^{-1}$ is also a positive-definite matrix. In particular, the map $Z \mapsto {}^t\overline{Z}$ gives a bijection between $\mathcal{H}_{r,s}$ and $\mathcal{H}_{s,r}$.

Remark 3.1.3. If $rs = 0$ we get $\mathcal{H}_{r,s} = \{0\}$, a space with a single point.

The choice of an m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ determines the product $\mathcal{H}_{\mathbf{r},\mathbf{s}} := \mathcal{H}_{r_1,s_1} \times \cdots \times \mathcal{H}_{r_e,s_e}$. In Section 3.2 we show how to associate a polarized abelian variety with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ to every element $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$ and $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$ and vice versa.

3.2 Polarized abelian varieties with given m-CM-type

Our goal in this section is to give a correspondence between the set of polarized abelian varieties with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ and the space $\mathcal{H}_{\mathbf{r},\mathbf{s}} \times \Upsilon(\mathbf{r}, \mathbf{s})$.

We first construct a polarized abelian variety with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ and then prove that every such polarized abelian variety can be obtained through that construction.

This result for CM-fields is a particular case of the results in Shimura [39]. It is also explained in Birkenhake-Lange [2, Section 9.6], where some proofs for

this case are left to the reader. We present them here for completeness, as we will use them in Section 3.3.

Fix a pair $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$, matrices $W_1, \dots, W_e$ as in (3.2), and an element $Z = (Z_1, \dots, Z_e) \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$. We start by constructing a complex torus.

Consider the complex vector space homomorphism $\Gamma : \mathbb{C}^{2em} \to \mathbb{C}^{em}$ given by the block diagonal matrix

$$\Gamma = \operatorname{diag}(\Gamma_1, \dots, \Gamma_e) \text{ with } \Gamma_\nu = \begin{pmatrix} (\mathbf{1}_{r_\nu} \; Z_\nu)\overline{W_\nu} & 0 \\ 0 & ({}^t Z_\nu \; \mathbf{1}_{s_\nu}) W_\nu \end{pmatrix} \in \mathbb{C}^{m \times 2m}. \tag{3.3}$$

Remark 3.2.1. If we have $r_\nu = 0$ or $s_\nu = 0$, then we get $\Gamma_\nu = (0 \;\; W_\nu)$ or $\Gamma_\nu = (\overline{W_\nu} \;\; 0)$, respectively.

Lemma 3.2.2. Γ restricted to $\jmath((K \otimes_{\mathbb{Q}} \mathbb{R})^m) \subseteq \mathbb{C}^{2em}$ is an isomorphism of real vector spaces.

Proof. This is a particular case of Lemma 9.6.2 in Birkenhake-Lange [2]; we write the details of the proof for completeness. We proceed to prove it by blocks, hence assume $e = 1$ and omit the subindices.

Consider the map $\pi : \mathbb{C}^m \to \mathbb{C}^m$ given by

$$x \mapsto \pi(x) = \begin{pmatrix} \mathbf{1}_r & Z \\ {}^t\overline{Z} & \mathbf{1}_s \end{pmatrix} \overline{W} x.$$

Since W is non-singular by definition and the matrix

$$\begin{pmatrix} \mathbf{1}_r & Z \\ {}^t\overline{Z} & \mathbf{1}_s \end{pmatrix} \begin{pmatrix} \mathbf{1}_r & -Z \\ -{}^t\overline{Z} & \mathbf{1}_s \end{pmatrix} = \begin{pmatrix} \mathbf{1}_r - Z\,{}^t\overline{Z} & 0 \\ 0 & \mathbf{1}_s - {}^t\overline{Z} Z \end{pmatrix}$$

is positive definite, thus non-singular, the map π is a $\mathbb{C}$-isomorphism. Moreover, let $\kappa : \mathbb{C}^m \to \mathbb{C}^{2m}$ be given by $\kappa(x) = \begin{pmatrix} x \\ \overline{x} \end{pmatrix}$ and $\eta : \mathbb{C}^{r+s} \to \mathbb{C}^{r+s}$ be given by $\eta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ \overline{y} \end{pmatrix}$. Then, as $\kappa \circ \phi$ is the map $\jmath$, the statement follows from the equality $\pi = \eta \circ \Gamma \circ \kappa$. □

We conclude that the image $(\Gamma \circ \jmath)(\mathcal{M})$ is a lattice in $\mathbb{C}^{em}$ and the quotient $X := \mathbb{C}^{em}/(\Gamma \circ \jmath)(\mathcal{M})$ is a complex torus.

Next, we determine the polarization of X by determining a hermitian form. We define the map $H : \mathbb{C}^{em} \times \mathbb{C}^{em} \to \mathbb{C}$ as $H(x, y) = 2\,{}^t x \operatorname{diag}(H_1, \dots, H_e)\overline{y}$ with

$$H_\nu = \begin{pmatrix} (\mathbf{1}_{r_\nu} - \overline{Z_\nu}\,{}^t Z_\nu)^{-1} & 0 \\ 0 & (\mathbf{1}_{s_\nu} - {}^t\overline{Z_\nu} Z_\nu)^{-1} \end{pmatrix} \in \mathbb{C}^{m \times m}, \tag{3.4}$$

which is positive definite and hermitian by definition. To see that it defines a polarization we need to see that the associated alternating form $E = \operatorname{Im} H$ is integer-valued on the lattice $(\Gamma \circ \jmath)(\mathcal{M})$. Given a linear map $f : A \to B$ and a real bilinear form $E : B \times B \to \mathbb{R}$, we define the real bilinear form $f^*E := E(f(\cdot), f(\cdot)) : A \times A \to \mathbb{R}$.

Lemma 3.2.3. For all $\mathbf{a}, \mathbf{b} \in (K \otimes \mathbb{R})^m$ we have

$$((\Gamma \circ \jmath)^* E)(\mathbf{a}, \mathbf{b}) = \operatorname{tr}_{K\otimes\mathbb{R}/\mathbb{R}}({}^t\mathbf{a} T \overline{\mathbf{b}}).$$

Proof. This is a particular case of Lemma 9.6.3 in Birkenhake-Lange [2]; we write the details of the proof for completeness. As before, we proceed to prove it by blocks, hence assume $e = 1$ and omit the subindices.

On the one hand we have

$$\begin{aligned}
(\Gamma\circ\jmath)^*E(\mathbf{a},\mathbf{b}) &= 2\operatorname{Im}\left({}^t\jmath(\mathbf{a})\,{}^t\Gamma H \overline{\Gamma}\,\overline{\jmath(\mathbf{b})}\right) \\
&= 2\operatorname{Im}\left({}^t\begin{pmatrix}\phi(\mathbf{a})\\ \overline{\phi}(\mathbf{a})\end{pmatrix} \begin{pmatrix} {}^t\overline{W}\begin{pmatrix}\mathbf{1}_r\\ {}^tZ\end{pmatrix} & 0 \\ 0 & {}^tW\begin{pmatrix}Z\\ \mathbf{1}_s\end{pmatrix}\end{pmatrix} \right. \\
&\qquad \left. \begin{pmatrix}(\mathbf{1}_r - \overline{Z}\,{}^tZ)^{-1} & 0\\ 0 & (\mathbf{1}_s - {}^t\overline{Z}Z)^{-1}\end{pmatrix} \begin{pmatrix}(\mathbf{1}_r\ \overline{Z})W & 0\\ 0 & ({}^t\overline{Z}\ \mathbf{1}_s)\overline{W}\end{pmatrix} \overline{\begin{pmatrix}\phi(\mathbf{b})\\ \overline{\phi}(\mathbf{b})\end{pmatrix}} \right) \\
&= 2\operatorname{Im}\Big({}^t\phi(\mathbf{a})\,{}^t\overline{W}\begin{pmatrix}\mathbf{1}_r\\ {}^tZ\end{pmatrix}(\mathbf{1}_r - \overline{Z}\,{}^tZ)^{-1}(\mathbf{1}_r\ \overline{Z})W\overline{\phi(\mathbf{b})} \\
&\qquad + {}^t\overline{\phi(\mathbf{a})}\,{}^tW\begin{pmatrix}Z\\ \mathbf{1}_s\end{pmatrix}(\mathbf{1}_s - {}^t\overline{Z}Z)^{-1}({}^t\overline{Z}\ \mathbf{1}_s)\overline{W}\phi(\mathbf{b})\Big) \\
&= 2\operatorname{Im}\Big({}^t\phi(\mathbf{a})\,{}^t\overline{W}\begin{pmatrix}\mathbf{1}_r\\ {}^tZ\end{pmatrix}(\mathbf{1}_r - \overline{Z}\,{}^tZ)^{-1}(\mathbf{1}_r\ \overline{Z})W\overline{\phi(\mathbf{b})} \\
&\qquad - {}^t\phi(\mathbf{a})\,{}^t\overline{W}\begin{pmatrix}\overline{Z}\\ \mathbf{1}_s\end{pmatrix}(\mathbf{1}_s - {}^tZ\overline{Z})^{-1}({}^tZ\ \mathbf{1}_s)W\overline{\phi(\mathbf{b})}\Big) \\
&= 2\operatorname{Im}\Big({}^t\phi(\mathbf{a})\,{}^t\overline{W}\Big(\begin{pmatrix}\mathbf{1}_r\\ {}^tZ\end{pmatrix}(\mathbf{1}_r - \overline{Z}\,{}^tZ)^{-1}(\mathbf{1}_r\ \overline{Z}) \\
&\qquad - \begin{pmatrix}\overline{Z}\\ \mathbf{1}_s\end{pmatrix}(\mathbf{1}_s - {}^tZ\overline{Z})^{-1}({}^tZ\ \mathbf{1}_s)\Big)W\overline{\phi(\mathbf{b})}\Big) \\
&= 2\operatorname{Im}\left({}^t\phi(\mathbf{a})\,{}^t\overline{W}\begin{pmatrix}\mathbf{1}_r & 0\\ 0 & -\mathbf{1}_s\end{pmatrix}W\overline{\phi(\mathbf{b})}\right) = 2\operatorname{Im}\left(i\,{}^t\phi(\mathbf{a})\phi(T)\overline{\phi(\mathbf{b})}\right) \\
&= 2\operatorname{Re}\phi\left({}^t\mathbf{a}T\overline{\mathbf{b}}\right).
\end{aligned}$$

And on the other hand we get

$$\operatorname{tr}_{K\otimes\mathbb{R}/\mathbb{R}}({}^t\mathbf{a}T\overline{\mathbf{b}}) = \phi({}^t\mathbf{a}T\overline{\mathbf{b}}) + \overline{\phi}({}^t\mathbf{a}T\overline{\mathbf{b}}) = 2\operatorname{Re}\phi({}^t\mathbf{a}T\overline{\mathbf{b}}). \qquad \square$$

Lastly we determine an embedding $K \hookrightarrow \operatorname{End}(X)\otimes\mathbb{Q}$. Let $\mathcal{O}$ be the order $\{\alpha \in K : \alpha\mathcal{M} \subseteq \mathcal{M}\}$. Note that $\mathcal{O}$ acts on $\mathcal{M}$ via a natural action, which induces an $\mathbb{R}$-linear action on the lattice $(\Gamma\circ\jmath)(\mathcal{M})$ in $\mathbb{C}^{em}$. This gives an embedding $\mathcal{O} \hookrightarrow \operatorname{End}(X)$ which extends to an embedding

$$\iota : K \hookrightarrow \operatorname{End}(X)\otimes\mathbb{Q}.$$

We now have all the elements needed to determine a polarized abelian variety with m-CM-type, so we can state the result.

Proposition 3.2.4. Let $(\mathcal{M}, T) \in \Upsilon(\mathbf{r},\mathbf{s})$ and $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$. The triple $(X, \operatorname{Im} H, \iota)$ as defined above is a polarized abelian variety with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$.

Proof. This is a particular case of Lemma 9.6.4 in Birkenhake-Lange [2]; we write the details of the proof for completeness.

We need to prove that the analytic representation $\rho_a \circ \iota$ is equivalent to the representation $\rho_{\mathbf{r},\mathbf{s}}$ defined in (3.1) and that the Rosati involution on $\operatorname{End}(X)\otimes\mathbb{Q}$ with respect to the polarization extends the complex conjugation via ι.

The equivalence of representations follows from the equality

$$\rho_{\mathbf{r},\mathbf{s}}(a)(\Gamma\circ\jmath)(\mathbf{b}) = (\Gamma\circ\jmath)(a\mathbf{b}).$$

As before, we proceed to prove it by blocks, hence assume $e = 1$ and omit the subindices.

We have

$$\begin{aligned}
\rho_{\mathbf{r},\mathbf{s}}(a)(\Gamma\circ\jmath)(\mathbf{b}) &= \begin{pmatrix} \phi(a)\mathbf{1}_r & 0 \\ 0 & \overline{\phi}(a)\mathbf{1}_s \end{pmatrix} \begin{pmatrix} (\mathbf{1}_r\ Z)\overline{W} & 0 \\ 0 & ({}^tZ\ \mathbf{1}_s)W \end{pmatrix} \begin{pmatrix} \phi(\mathbf{b}) \\ \overline{\phi}(\mathbf{b}) \end{pmatrix} \\
&= \begin{pmatrix} (\mathbf{1}_r\ Z)\overline{W} & 0 \\ 0 & ({}^tZ\ \mathbf{1}_s)W \end{pmatrix} \begin{pmatrix} \phi(a)\mathbf{1}_m & 0 \\ 0 & \overline{\phi}(a)\mathbf{1}_m \end{pmatrix} \begin{pmatrix} \phi(\mathbf{b}) \\ \overline{\phi}(\mathbf{b}) \end{pmatrix} \\
&= (\Gamma\circ\jmath)(a\mathbf{b}),
\end{aligned}$$

so the equality holds.

That the Rosati involution on $\operatorname{End}(X)\otimes\mathbb{Q}$ with respect to the polarization extends the complex conjugation on K via ι is a consequence of the definition of ι as the unique extension of the natural action of K on $\mathcal{M}\otimes\mathbb{Q}$. $\square$

This construction defines a map A from $\mathcal{H}_{\mathbf{r},\mathbf{s}} \times \Upsilon(\mathbf{r},\mathbf{s})$ to the set of isomorphism classes of polarized abelian varieties with m-CM-type $(K,\Phi,\mathbf{r},\mathbf{s})$ given by $A(Z,\mathcal{M},T) = (X, \operatorname{Im} H, \iota)$. The next proposition shows that the map is surjective.

Proposition 3.2.5 (Shimura [39], see Birkenhake-Lange [2, Proposition 9.6.5])**.** Every polarized abelian variety (X, E, ι) with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ is isomorphic to $A(Z, \mathcal{M}, T)$ for some $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$ and $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$.

Proof. We give the proof since it is omitted in Birkenhake-Lange [2] and because we will use it in Section 3.3.

Let the triple $(X = V/\Lambda, E, \iota)$ be a polarized abelian variety with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$. There exists a basis of V such that, for all $a \in K$, the analytic representation of $\iota(a)$ is the diagonal matrix $\rho_{\mathbf{r},\mathbf{s}}(a)$. We identify V with $\mathbb{C}^{em}$ via this choice. Since $\Lambda \otimes \mathbb{Q} \subseteq \mathbb{C}^{em}$ is a vector space over K of dimension m via $\rho_{\mathbf{r},\mathbf{s}}$, we choose a basis $b_1, \ldots, b_m \in \Lambda \otimes \mathbb{Q}$ and consider the isomorphism $\eta : K^m \to \Lambda \otimes \mathbb{Q}$ given by this basis. Then $\mathcal{M} = \eta^{-1}(\Lambda)$ is a $\mathbb{Z}$-module of rank $2em$ in K^m.

Next, consider the maps $\pi_{ij} : K \to \mathbb{Q}$ given by $a \mapsto E(ab_i, b_j)$ for all $1 \leq i, j \leq m$. These are $\mathbb{Q}$-linear maps, hence there exist $t_{ij} \in K$ such that $E(ab_i, b_j) = \operatorname{tr}(at_{ij})$ holds for all $a \in K$. The matrix $T = (t_{ij})_{ij} \in K^{m\times m}$ satisfies

$$\eta^* E(\mathbf{a}, \mathbf{b}) = \operatorname{tr}({}^t\mathbf{a} T \overline{\mathbf{b}}) \in \mathbb{Z} \tag{3.5}$$

for all $\mathbf{a}, \mathbf{b} \in \mathcal{M}$. Shimura also proves that T is antihermitian and has signature $(\mathbf{r}, \mathbf{s})$ as a consequence of E being a Riemann form. For details see [39, pp. 158–160]. Let W_ν for $\nu = 1, \ldots, e$ be arbitrary matrices satisfying (3.2).

We have then a pair $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$. We only need to find $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$ such that (X, E, ι) is isomorphic to $A(Z, \mathcal{M}, T)$.

A vector $b \in \mathbb{C}^{em}$ can be written as

$$b = \begin{pmatrix} u^1 \\ v^1 \\ \vdots \\ u^e \\ v^e \end{pmatrix}$$

with $u^\nu \in \mathbb{C}^{r_\nu}$ and $v^\nu \in \mathbb{C}^{s_\nu}$ for every $\nu = 1, \ldots, e$.

Consider such subdivision for the basis $b_1, \ldots, b_m$ of $\Lambda \otimes \mathbb{Q}$. We define the matrices

$$U_\nu = \begin{pmatrix} u_1^\nu & \cdots & u_m^\nu \end{pmatrix} \in \mathbb{C}^{r_\nu \times m}, \quad V_\nu = \begin{pmatrix} v_1^\nu & \cdots & v_m^\nu \end{pmatrix} \in \mathbb{C}^{s_\nu \times m},$$
$$X_\nu = \begin{pmatrix} U_\nu & 0 \\ 0 & V_\nu \end{pmatrix} \in \mathbb{C}^{m \times 2m}$$

and write

$$\begin{pmatrix} U_\nu & 0 \\ 0 & V_\nu \end{pmatrix} \begin{pmatrix} \overline{W}_\nu^{-1} & 0 \\ 0 & W_\nu^{-1} \end{pmatrix} = \begin{pmatrix} A_\nu & B_\nu & 0 & 0 \\ 0 & 0 & C_\nu & D_\nu \end{pmatrix}, \tag{3.6}$$

where we have $A_\nu \in \mathbb{C}^{r_\nu \times r_\nu}$, $B_\nu \in \mathbb{C}^{r_\nu \times s_\nu}$, $C_\nu \in \mathbb{C}^{s_\nu \times r_\nu}$, and $D_\nu \in \mathbb{C}^{s_\nu \times s_\nu}$.

Shimura proves that the matrices A_ν and D_ν are invertible and satisfy $A_\nu^{-1}B_\nu = {}^t(D_\nu^{-1}C_\nu)$. This follows from the same reasoning that gives the signature of T, see [39, (30) and the paragraph after]. Since it is not relevant for the use of the construction we omit the details here.

We define $Z_\nu = A_\nu^{-1}B_\nu = {}^t(D_\nu^{-1}C_\nu) \in \mathbb{C}^{r_\nu \times s_\nu}$ and change the basis of V by the matrix $\operatorname{diag}(A_1^{-1}, D_1^{-1}, \ldots, A_e^{-1}, D_e^{-1})$, so that without loss of generality (3.6) becomes

$$\begin{pmatrix} U_\nu & 0 \\ 0 & V_\nu \end{pmatrix} \begin{pmatrix} \overline{W}_\nu^{-1} & 0 \\ 0 & W_\nu^{-1} \end{pmatrix} = \begin{pmatrix} \mathbf{1}_{r_\nu} & Z_\nu & 0 & 0 \\ 0 & 0 & {}^tZ_\nu & \mathbf{1}_{s_\nu} \end{pmatrix} \in \mathbb{C}^{m \times 2m},$$

or equivalently,

$$X_\nu = \begin{pmatrix} U_\nu & 0 \\ 0 & V_\nu \end{pmatrix} = \begin{pmatrix} (\mathbf{1}_{r_\nu}\ Z_\nu)\overline{W_\nu} & 0 \\ 0 & ({}^tZ_\nu\ \mathbf{1}_{s_\nu})W_\nu \end{pmatrix} \in \mathbb{C}^{m \times 2m},$$

that is, with this basis the matrix X_ν is the ν-component of Γ as defined in (3.3).

Then, for all $\mathbf{a} \in (K \otimes \mathbb{R})^m$ we have

$$\begin{aligned} \eta(\mathbf{a}) &= \sum_{i=1}^{m} \rho_{\mathbf{r},\mathbf{s}}(a_i)b_i \\ &= \sum_{i=1}^{m} \begin{pmatrix} \phi_1(a_i)u_i^1 \\ \overline{\phi}_1(a_i)v_i^1 \\ \vdots \\ \phi_e(a_i)u_i^e \\ \overline{\phi}_e(a_i)v_i^e \end{pmatrix} = \begin{pmatrix} U_1 & 0 & \cdots & 0 & 0 \\ 0 & V_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & U_e & 0 \\ 0 & 0 & \cdots & 0 & V_e \end{pmatrix} \begin{pmatrix} \phi_1(\mathbf{a}) \\ \overline{\phi}_1(\mathbf{a}) \\ \vdots \\ \phi_e(\mathbf{a}) \\ \overline{\phi}_e(\mathbf{a}) \end{pmatrix} = (\Gamma \circ \jmath)(\mathbf{a}), \end{aligned}$$

hence we obtain $\eta = \Gamma \circ \jmath$. We claim that $Z = (Z_1, \ldots, Z_e)$ is in $\mathcal{H}_{\mathbf{r},\mathbf{s}}$ and the triple (X, H, ι) is isomorphic to $A(Z, \mathcal{M}, T)$.

In order to prove $\mathbf{1}_s - {}^t\overline{Z}Z > 0$, and hence $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$, we will use the definition of H in (3.4) and its positive-definiteness. Let $\mu_1, \ldots, \mu_{2em} \in \mathcal{M}$ be a $\mathbb{Z}$-basis and let $x_i = \eta(\mu_i)$ be the corresponding basis of Λ. The matrices of H and E satisfy the equality $M_H = 2i(\overline{\Pi}M_E^{-1}\,{}^t\Pi)^{-1}$ (see (1.5)) where Π is the big period matrix (see (1.4)) of the complex torus with respect to the chosen bases, so we start by computing Π and M_E.

The period matrix Π has as columns the vectors $x_i = \eta(\mu_i) = \Gamma\jmath(\mu_i)$, hence we write $\Pi = \Gamma M$ with $M = (\jmath(\mu_i))_i \in \mathbb{C}^{2em\times 2em}$. The matrix of E is $M_E = (E(x_i, x_j))_{i,j} \in \mathbb{Z}^{2em\times 2em}$ so we compute

$$\begin{aligned}
E(x_i, x_j) &= \eta^* E(\mu_i, \mu_j) \\
&= \operatorname{tr}({}^t\mu_i T\overline{\mu_j}) = \sum_{j=1}^{e}({}^t\phi_j(\mu_i)\phi_j(T)\phi_j(\overline{\mu_j}) + {}^t\overline{\phi}_j(\mu_i)\overline{\phi}_j(T)\overline{\phi}_j(\overline{\mu_j})) \\
&= {}^t\jmath(\mu_i)\operatorname{diag}(\phi_1(T), \overline{\phi}_1(T), \dots, \phi_e(T), \overline{\phi}_e(T))\jmath(\overline{\mu_j}) \\
&= {}^t\jmath(\mu_i)\operatorname{diag}(\phi_1(T), \overline{\phi_1(T)}, \dots, \phi_e(T), \overline{\phi_e(T)})\overline{\jmath(\mu_j)},
\end{aligned}$$

hence we obtain

$$M_E = {}^tM\operatorname{diag}(\phi_1(T), \overline{\phi_1(T)}, \dots, \phi_e(T), \overline{\phi_e(T)})\overline{M}. \tag{3.7}$$

We can now compute M_H. It is again enough to compute M_H by blocks, hence we assume $e = 1$ and omit the subindices. Altogether it gives us

$$\begin{aligned}
M_H &= 2i(\overline{\Pi}M_E^{-1}\,{}^t\Pi)^{-1} = 2i[\overline{(\Gamma M)}(\overline{M}^{-1}\operatorname{diag}(\phi(T), \overline{\phi(T)})^{-1}\,{}^tM^{-1})\,{}^t(\Gamma M)]^{-1} \\
&= 2i(\overline{\Gamma}\operatorname{diag}(\phi(T), \overline{\phi(T)})^{-1}\,{}^t\Gamma)^{-1} \\
&= 2i\left[\begin{pmatrix}(\mathbf{1}_r\ \overline{Z})W & 0\\ 0 & ({}^t\overline{Z}\ \mathbf{1}_s)\overline{W}\end{pmatrix}\begin{pmatrix}\phi(T)^{-1} & 0\\ 0 & \overline{\phi(T)}^{-1}\end{pmatrix}\begin{pmatrix}{}^t\overline{W}\begin{pmatrix}\mathbf{1}_r\\ {}^tZ\end{pmatrix} & 0\\ 0 & {}^tW\begin{pmatrix}Z\\ \mathbf{1}_s\end{pmatrix}\end{pmatrix}\right]^{-1} \\
&= 2\left[\begin{pmatrix}\mathbf{1}_r & \overline{Z} & 0 & 0\\ 0 & 0 & {}^t\overline{Z} & \mathbf{1}_s\end{pmatrix}\begin{pmatrix}\mathbf{1}_r & 0 & 0 & 0\\ 0 & -\mathbf{1}_s & 0 & 0\\ 0 & 0 & -\mathbf{1}_r & 0\\ 0 & 0 & 0 & \mathbf{1}_s\end{pmatrix}\begin{pmatrix}\mathbf{1}_r & 0\\ {}^tZ & 0\\ 0 & Z\\ 0 & \mathbf{1}_s\end{pmatrix}\right]^{-1} \\
&= 2\begin{pmatrix}\mathbf{1}_r - \overline{Z}\,{}^tZ & 0\\ 0 & \mathbf{1}_s - {}^t\overline{Z}Z\end{pmatrix}^{-1},
\end{aligned}$$

and since H is positive definite and hermitian by definition, we obtain $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$. It follows that (X, H, ι) is isomorphic to $A(Z, \mathcal{M}, T)$ by construction. □

Observe that the equality (3.7) implies the following result.

Corollary 3.2.6. The pair $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$ determines whether the polarization of $A(Z, \mathcal{M}, T)$ is principal. □

3.3 The endomorphism structure of the Jacobian of a CPQ curve

As we have seen in Chapter 2, every CPQ curve can be given by a Legendre-Rosenhain equation

$$y^5 = x(x-1)(x-\lambda)(x-\mu)$$

with $\lambda, \mu \in \mathbb{C}\backslash\{0,1\}$ distinct, and has an order-5 automorphism ρ given by $\rho(x,y) = (x, z_5 y)$.

In this section we give the Jacobian $J(C)$ of a CPQ curve C following the explicit construction explained in Section 1.1, together with its Riemann form, and we study the structure of the subring $\mathbb{Z}[\rho_*] \subseteq \mathrm{End}(J(C))$.

First we choose a $\mathbb{Z}$-basis for $H_1(C,\mathbb{Z})$. Note that the curve is a 5-cover of the projective line and the automorphism ρ cycles through the different sheets. Therefore, by studying the intersections in the x-plane of the paths in the $\mathbb{Q}(\zeta_5)$-basis of $H_1(C,\mathbb{Z})\otimes\mathbb{Q}$ appearing in Figure 3.1, we obtain the whole intersection matrix.

Take the paths b_1, b_2, b_3 appearing in Figure 3.1 and consider the paths $\rho^j b_i := \rho^j \circ b_i$ for $i = 1,2,3$ and $j = 1,\dots,4$. We claim that

$$\gamma = (b_1, \rho b_1, \rho^2 b_1, \rho^3 b_1, b_2, \rho b_2, \rho^2 b_2, \rho^3 b_2, b_3, \rho b_3, \rho^2 b_3, \rho^3 b_3) \tag{3.8}$$

is a $\mathbb{Z}$-basis of $H_1(C,\mathbb{Z})$.

Recall $J(C) = H^0(\omega_C)^*/H_1(C,\mathbb{Z})$, and that the principal polarization attached to $J(C)$ is given by the oriented intersection pairing. We compute the oriented intersection between the paths in (3.8).

See for example the intersections corresponding to b_1. We can see in Figure 3.1 that the solid part of the path intersects b_2 and b_3 on the same sheet, and the dashed part crosses all three paths in the solid sheet. Therefore, the path b_1 intersects once the paths b_2, b_3, ρb_1, ρb_2 and ρb_3. The intersection sign is positive (resp. negative) if the angle going from the first path to the second is counterclockwise (resp. clockwise). For example, the five intersections $E(b_1,\cdot)$ listed here are $+1, +1, -1, -1$ and -1 respectively.

Working analogously for the other paths, we obtain the matrix of E with respect to γ

$$E_0 = \begin{pmatrix} A & B & B \\ -{}^tB & A & B \\ -{}^tB & -{}^tB & A \end{pmatrix},$$

with

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

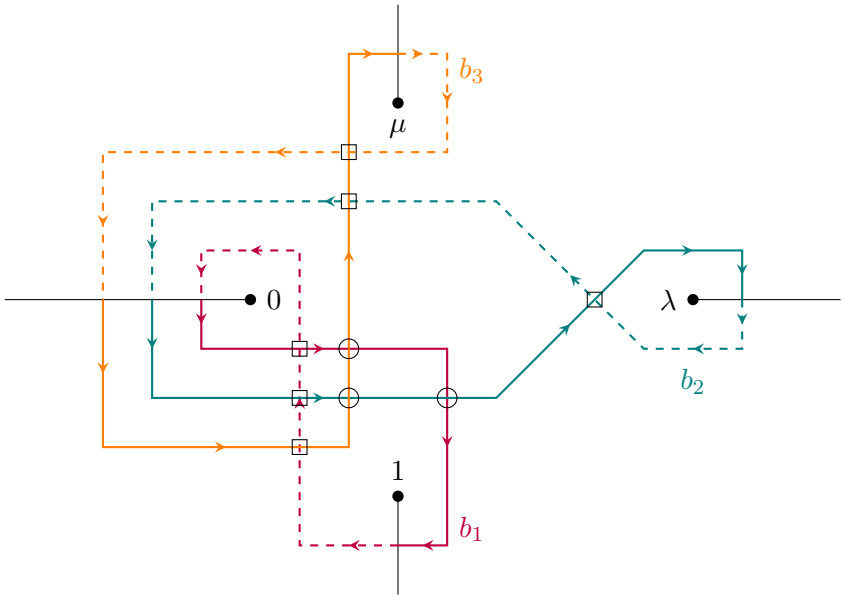


Figure 3.1: Representation on the x-plane of a $\mathbb{Q}(\zeta_5)$-basis of $H_1(C, \mathbb{Z}) \otimes \mathbb{Q}$ given by $\{b_1, b_2, b_3\}$. The solid black lines are branch cuts, which intersect at ∞. Crossing a branch cut clockwise around one affine branch point corresponds to switching to the next sheet, and it is represented by a change on the pattern of the path. Therefore circles indicate intersections on C and squares indicate intersections on the x-plane that are not intersections on C.

and since the determinant of E_0 is $\det E_0 = 1$, the choice (3.8) is indeed a $\mathbb{Z}$-basis of $H_1(C,\mathbb{Z})$. This basis, together with the basis of $H^0(\omega_C)$ given in Corollary 2.1.5, determines a big period matrix

$$\Pi = \begin{pmatrix} \int_{b_1} \frac{dx}{y^4} & \cdots & \int_{\rho^3 b_3} \frac{dx}{y^4} \\ \vdots & & \vdots \\ \int_{b_1} \frac{xdx}{y^2} & \cdots & \int_{\rho^3 b_3} \frac{xdx}{y^2} \end{pmatrix},$$

so that $J(C) \cong \mathbb{C}^6/\Pi\mathbb{Z}^{12}$.

Finally, we want to compute the analytic representation with respect to these bases of the automorphism ρ_* of the Jacobian induced by ρ.

The automorphism ρ induces a morphism $\rho^* : H^0(\omega_C) \to H^0(\omega_C)$ given by

$$\rho^*(fdg) = (f \circ \rho)d(g \circ \rho).$$

The morphism ρ^* acts on the basis chosen in Corollary 2.1.5 of $H^0(\omega_c)$ as $\rho^*(x^i y^{-j} dx) = z_5^{-j} x^i y^{-j} dx$, that is, as the diagonal matrix

$$A = \operatorname{diag}(z_5, z_5, z_5, z_5^2, z_5^2, z_5^3).$$

This basis has a dual basis of $H^0(\omega_C)^*$, and one can prove that ρ_* with respect to this dual basis acts as ${}^tA = A$ by using the definitions of α and ρ^*, so we get $\rho_a(\rho_*) = A$. We define the embedding $\iota : \mathbb{Q}(\zeta_5) \to \operatorname{End}(J(C)) \otimes \mathbb{Q}$ by taking $\iota(\zeta_5) = \rho_*$.

Proposition 3.3.1. Let C be a CPQ curve. Let $\phi_1, \phi_2 : \mathbb{Q}(\zeta_5) \to \mathbb{C}$ be the embeddings given by $\phi_1(\zeta_5) = z_5$ and $\phi_2(\zeta_5) = z_5^2$ respectively, and let $\iota : \mathbb{Q}(\zeta_5) \to \operatorname{End}(J(C)) \otimes \mathbb{Q}$ be the embedding that maps ζ_5 to ρ_*. Then $(J(C), \lambda_C, \iota)$ has 3-CM-type $\mathfrak{Z} = (\mathbb{Q}(\zeta_5), (\phi_1, \phi_2), (3,2), (0,1))$.

Proof. We just saw that $\rho_{\mathfrak{Z}}$ and $\rho_a \circ \iota$ are equivalent representations, since they map ζ_5 to the same diagonal matrix.

All that is left to do is prove that the Rosati involution on $\operatorname{End}(J(C)) \otimes \mathbb{Q}$ with respect to the polarization λ_C extends complex multiplication on $\mathbb{Q}(\zeta_5)$ via ι.

Let α be an Abel-Jacobi map with a branch point as base point, hence fixed by ρ. Recall the diagram (1.12) that relates an automorphism of a curve ρ with its induced automorphism ρ_* on the Jacobian,

$$\begin{array}{ccc} C & \xrightarrow{\rho} & C \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ J(C) & \xrightarrow{\rho_*} & J(C). \end{array} \tag{3.9}$$

If we apply the functor Pic^0 to the diagram, then we obtain

$$\begin{array}{ccc} \mathrm{Pic}^0(C) = J(C) & \xleftarrow{\rho^*} & \mathrm{Pic}^0(C) = J(C) \\ \uparrow{\scriptstyle \alpha^*} & & \uparrow{\scriptstyle \alpha^*} \\ \mathrm{Pic}^0(J(C)) = \widehat{J(C)} & \xleftarrow{\widehat{\rho_*}} & \mathrm{Pic}^0(J(C)) = \widehat{J(C)}, \end{array} \tag{3.10}$$

where α^* is the inverse of the polarization λ_C of $J(C)$, see Proposition 11.3.5 in Birkenhake-Lange [2]. Therefore ρ_* and ρ^* are dual to each other, in the sense that they satisfy $\widehat{\rho_*} = \lambda_C \rho^* \lambda_C^{-1}$, and by definition of the Rosati involution (see (1.2)) we obtain $\rho'_* = \rho^*$.

Since we have $\rho_* \rho^* = 1$, we conclude that $\iota(\zeta_5)' = \rho'_* = \rho_*^{-1} = \iota(\overline{\zeta_5})$ holds. Thus the statement follows. □

We have proven that $(J(C), \lambda_C, \iota)$ has 3-CM-type $\mathfrak{Z}$, so by Proposition 3.2.5 there exists a pair $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ such that the triple $(J(C), \lambda_C, \iota)$ is of the form $A(Z, \mathcal{M}, T)$ for some $Z \in \mathcal{H}_{\mathfrak{Z}}$. The constructive proof of that proposition gives us the recipe to find that pair $(\mathcal{M}, T)$.

The dual of the $\mathbb{C}$-basis of $H^0(\omega_C)$ given in Corollary 2.1.5 already satisfies $\rho_a \circ \iota = \rho_{\mathbf{r},\mathbf{s}}$, and we choose $\{b_i\}_{i=1}^3$ as a $\mathbb{Q}(\zeta_5)$-basis of $H_1(C, \mathbb{Z}) \otimes \mathbb{Q}$. We obtain $\mathcal{M} = \eta^{-1}(H_1(C, \mathbb{Z})) = \mathcal{O}_K^3$.

Next we want to find a matrix $T \in \mathbb{Q}(\zeta_5)^{3\times 3}$ that satisfies

$$E(ab_i, b_j) = \mathrm{tr}(at_{ij}) \tag{3.11}$$

for all $a \in \mathbb{Q}(\zeta_5)$. For every $i, j = 1, \ldots, 3$ consider the condition (3.11) for $a \in \{\zeta_5^k : 1 \le k \le 4\}$. This gives a linear system whose solution determines t_{ij} uniquely, and we obtain

$$T = \frac{1}{5} \begin{pmatrix} \zeta_5 - \zeta_5^4 & 1 - \zeta_5^4 & 1 - \zeta_5^4 \\ -1 + \zeta_5 & \zeta_5 - \zeta_5^4 & 1 - \zeta_5^4 \\ -1 + \zeta_5 & -1 + \zeta_5 & \zeta_5 - \zeta_5^4 \end{pmatrix}. \tag{3.12}$$

We double-check that T has signature $((3, 2), (0, 1))$, which is consistent with Proposition 3.3.1.

We conclude that for every CPQ curve C there exists $Z \in \mathcal{H}_{\mathfrak{Z}}$ such that the triple $(J(C), \lambda_C, \iota)$ is of the form $A(Z, \mathcal{M}, T)$.

3.4 Equivalence of polarized lattices

We have seen in Corollary 3.2.6 that the pair $(\mathcal{M}, T)$ in $\Upsilon(\mathbf{r}, \mathbf{s})$ determines whether the polarization of a polarized abelian variety with m-CM-type $(K, \Phi, \mathbf{r}, \mathbf{s})$ is principal.

In this section we characterize the pairs that determine principal polarizations with the end goal of identifying the preimage of the set of principally polarized abelian varieties with 3-CM-type $\mathfrak{Z}$ and an order-5 automorphism by the map A defined in Section 3.2.

We start by presenting the concept of equivalent pairs $(\mathcal{M}, T) \in \Upsilon(\mathbf{r}, \mathbf{s})$ and how it relates to the map A.

Definition 3.4.1. Let $(K, \Phi, \mathbf{r}, \mathbf{s})$ be an m-CM-type. We say that two pairs $(\mathcal{M}_1, T_1)$ and $(\mathcal{M}_2, T_2)$ in $\Upsilon(\mathbf{r}, \mathbf{s})$ are *equivalent* if there exists $U \in \mathrm{GL}_m(K)$ that satisfies

$$U(\mathcal{M}_1, T_1) := (U\mathcal{M}_1, {}^tU^{-1}T_1\overline{U}^{-1}) = (\mathcal{M}_2, T_2).$$

Example 3.4.2. Consider the 3-CM-type $\mathfrak{Z}$ and define $\mathcal{M} = \mathcal{O}_K^3$ and T as in (3.12). The matrix

$$U = \begin{pmatrix} 1 & \zeta_5^3 & -\zeta_5^3 - \zeta_5 - 1 \\ 0 & -\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1 & 1 \\ 0 & \zeta_5 + 1 & 0 \end{pmatrix}$$

determines the equivalent pair $(\mathcal{M}_0, T_0) = U(\mathcal{M}, T)$ with $\mathcal{M}_0 = \mathcal{O}_K^3$ and

$$T_0 = \mathrm{diag}\left(\frac{1}{5}\zeta_5^3 + \frac{1}{5}\zeta_5^2 + \frac{2}{5}\zeta_5 + \frac{1}{5}, \frac{1}{5}\zeta_5^3 + \frac{1}{5}\zeta_5^2 + \frac{2}{5}\zeta_5 + \frac{1}{5}, -\frac{1}{5}\zeta_5^3 + \frac{1}{5}\zeta_5^2\right).$$

Proposition 3.4.3 (Proposition 4 in Shimura [39])**.** Let $(K, \Phi, \mathbf{r}, \mathbf{s})$ be an m-CM-type. Given two pairs $(\mathcal{M}, T), (\mathcal{M}', T') \in \Upsilon(\mathbf{r}, \mathbf{s})$ and two elements $Z, Z' \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$, the polarized abelian varieties $A(Z, \mathcal{M}, T)$ and $A(Z', \mathcal{M}', T')$ are isomorphic only if $(\mathcal{M}, T)$ and $(\mathcal{M}', T')$ are equivalent.

Conversely, if the pairs $(\mathcal{M}, T), (\mathcal{M}', T') \in \Upsilon(\mathbf{r}, \mathbf{s})$ are equivalent, then for every $Z \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$ there exists $Z' \in \mathcal{H}_{\mathbf{r},\mathbf{s}}$ such that the triple $A(Z, \mathcal{M}, T)$ is isomorphic to $A(Z', \mathcal{M}', T')$. □

Remark 3.4.4. If we consider the set $\Upsilon(\mathbf{r}, \mathbf{s})$ as a discrete topological space, then the map A coinduces a topology on the set of polarized abelian varieties with 3-CM-type $\mathfrak{Z}$. Moreover, it follows from Proposition 3.4.3 that the topological subspace of principally polarized abelian varieties with 3-CM-type $\mathfrak{Z}$ has as many connected components as equivalence classes of pairs $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ determining principal polarizations.

In this section we present the majority of the original work in this chapter. We will prove the following theorem, which is key for the proof of the main result of the chapter.

Theorem 3.4.5. Let $\phi_1, \phi_2 : \mathbb{Q}(\zeta_5) \to \mathbb{C}$ be the embeddings that map ζ_5 to z_5 and z_5^2 respectively, and let $\mathfrak{Z}$ be the 3-CM-type $(\mathbb{Q}(\zeta_5), (\phi_1, \phi_2), (3,2), (0,1))$. Let $Z \in \mathcal{H}_{\mathfrak{Z}}$, and consider a pair $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ such that $\zeta_5 \mathcal{M} \subseteq \mathcal{M}$. Then the polarization of $A(Z, \mathcal{M}, T)$ is principal if and only if the pair $(\mathcal{M}, T)$ is equivalent to $(\mathcal{M}_0, T_0)$.

The end goal is then to prove that the pair $(\mathcal{M}_0, T_0)$ defined in Example 3.4.2 is the only pair in $\Upsilon(\mathfrak{Z})$ up to equivalence such that the abelian varieties $A(\,\cdot\,, \mathcal{M}_0, T_0)$ are principally polarized and such that $\iota(\zeta_5)$ is an endomorphism of the abelian variety. We focus on the algebraic structure of $(\mathcal{M}, T)$ letting go of its relation to m-CM-types as much as possible. We use some results by Shimura [40] to define and characterize these pairs.

Let K be a CM-field of degree $2e$, let K^+ be its maximal totally real subfield, and let m be a positive integer. An *$\mathcal{O}_K$-lattice* $\mathcal{M}$ in K^m is a finitely generated $\mathcal{O}_K$-module in K^m that spans K^m over $\mathcal{O}_K$.

We also define a *polarized $\mathcal{O}_K$-lattice* to be a pair $(\mathcal{M}, T)$ with $\mathcal{M}$ an $\mathcal{O}_K$-lattice and $T \in K^{m \times m}$ an antihermitian matrix such that the alternating bilinear form

$$\begin{aligned} E : \mathcal{M} \times \mathcal{M} &\to \mathbb{Q} \\ (u, v) &\mapsto \operatorname{tr}_{K/\mathbb{Q}}({}^t u T \overline{v}) \end{aligned}$$

satisfies $E(\mathcal{M}, \mathcal{M}) \subseteq \mathbb{Z}$. We say that it is *principally polarized* if the matrix of E with respect to a basis of $\mathcal{M}$ has determinant 1.

Two polarized $\mathcal{O}_K$-lattices $(\mathcal{M}_1, T_1)$ and $(\mathcal{M}_2, T_2)$ are *equivalent* if there exists $U \in \mathrm{GL}_m(K)$ that satisfies

$$U(\mathcal{M}_1, T_1) := (U\mathcal{M}_1, {}^t U^{-1} T_1 \overline{U}^{-1}) = (\mathcal{M}_2, T_2).$$

We denote it by $(\mathcal{M}_1, T_1) \sim (\mathcal{M}_2, T_2)$

Our goal is to characterize principally polarized $\mathcal{O}_K$-lattices and study their equivalence classes.

We define the *trace dual* as

$$\mathcal{M}^\vee = \{\alpha \in K^m : \operatorname{tr}({}^t \alpha \mathcal{M}) \subseteq \mathbb{Z}\}.$$

Proposition 3.4.6 (2.15 in Shimura [40])**.** Let $\mathcal{M}$ be an $\mathcal{O}_K$-lattice in K^m and consider $c \in K$, $\alpha \in K^{m \times m}$ and $\sigma \in \mathrm{Aut}(K)$. The trace dual satisfies:

(1) $(c\mathcal{M})^\vee = c^{-1}\mathcal{M}^\vee$,
(2) $(\alpha\mathcal{M})^\vee = {}^t\alpha^{-1}\mathcal{M}^\vee$,
(3) $(\mathcal{M}^\sigma)^\vee = (\mathcal{M}^\vee)^\sigma$. □

We define the *different of K* as the inverse as a fractional ideal of the trace dual of the ring of integers $\mathcal{D}_K^{-1} = \mathcal{O}_K^\vee$.

Proposition 3.4.7. A polarized $\mathcal{O}_K$-lattice $(\mathcal{M}, T)$ is principally polarized if and only if it satisfies

$$ {}^tT\mathcal{M} = \overline{\mathcal{M}}^\vee. $$

Proof. Let $b_1, \dots, b_{2em}$ be a $\mathbb{Q}$-basis of $V = K^m$, and let $b_1^*, \dots, b_{2em}^*$ be the corresponding dual basis of $V^* = \mathrm{Hom}(V, \mathbb{Q})$. They satisfy $b_i^* b_j = \delta_{ij}$ for all $i, j = 1, \dots, 2em$. Consider also the $\mathbb{Q}$-bilinear form

$$ \begin{aligned} \mathrm{tr}_{K/\mathbb{Q}} : V \times V &\to \mathbb{Q} \\ (u, v) &\mapsto \mathrm{tr}_{K/\mathbb{Q}}({}^t u v). \end{aligned} $$

It defines an isomorphism $\phi : V \to V^*$ given by $u \mapsto \mathrm{tr}_{K/\mathbb{Q}}({}^t u \cdot)$, hence we can define a new $\mathbb{Q}$-basis of V as $b_i^\vee = \phi^{-1}(b_i^*)$, which satisfies $\mathrm{tr}_{K/\mathbb{Q}}(b_i^\vee b_j) = \delta_{ij}$.

Assume now that $(b_i)_i$ is a basis of $\mathcal{M}$. It follows that $(b_i^\vee)_i$ is a basis of $\mathcal{M}^\vee$, and since $(\mathcal{M}, T)$ is a polarized $\mathcal{O}_K$-lattice, we also have ${}^tT\mathcal{M} \subseteq \overline{\mathcal{M}}^\vee$. Moreover, the index $[\overline{\mathcal{M}}^\vee : {}^tT\mathcal{M}]$ is equal to the determinant of E for the basis $(b_i)_i$ of $\mathcal{M}$, so the equality holds if and only if the determinant is 1. □

Given $\mathcal{L}$ and $\mathcal{M}$ two $\mathcal{O}_K$-lattices in K^m for $m \in \mathbb{Z}_{>0}$, we define the *ideal index of* $\mathcal{M}$ *in* $\mathcal{L}$ as the fractional $\mathcal{O}_K$-ideal

$$ [\mathcal{L}/\mathcal{M}]_K = (\det(\alpha) : \alpha \in K^{m\times m} \text{ such that } \alpha\mathcal{L} \subseteq \mathcal{M}). $$

Whenever the field is clear by context, we leave the subindex out of the notation.

Proposition 3.4.8 (2.15 in Shimura [40])**.** Let $\mathcal{L}, \mathcal{M}, \mathcal{N}$ be $\mathcal{O}_K$-lattices in K^m, let $\alpha \in \mathrm{GL}_m(K)$, and let $\sigma \in \mathrm{Aut}(K)$. Then we have

(1) $[\mathcal{L}/\mathcal{M}][\mathcal{M}/\mathcal{N}] = [\mathcal{L}/\mathcal{N}]$,
(2) $[\mathcal{L}/\alpha\mathcal{L}] = \det(\alpha)\mathcal{O}_K$, and
(3) If we have $\mathcal{L} \supseteq \mathcal{M}$ and there exists an $\mathcal{O}_K$-ideal $\mathfrak{b}$ that satisfies $\mathcal{L}/\mathcal{M} \cong \mathcal{O}_K/\mathfrak{b}$, then the ideal index of $\mathcal{M}$ in $\mathcal{L}$ is $[\mathcal{L}/\mathcal{M}] = \mathfrak{b}$. □

Using the concepts introduced, we characterize now principally polarized $\mathcal{O}_K$-lattices.

Proposition 3.4.9. Let K be a CM-field with class number 1 and let K^+ be its maximal totally real subfield. Let $\mathcal{D}_K$ be the different of K and assume that there exists $\delta \in K$ generating $\mathcal{D}_K$ such that $\overline{\delta} = -\delta$. Every principally polarized $\mathcal{O}_K$-lattice $(\mathcal{M}, T)$ satisfies

$$ \mathrm{N}_{K/K^+}([\mathcal{O}_K^m/\mathcal{M}]) = (\det(\delta T)^{-1})\mathcal{O}_{K^+}. $$

In order to prove Proposition 3.4.9 we need the following result.

Lemma 3.4.10. Let K be a number field with class number 1, let m be a positive integer, and let $\mathcal{M}$ be a $\mathcal{O}_K$-lattice in K^m. There exists $\gamma \in \mathrm{GL}_m(K)$ that satisfies

$$\mathcal{M} = \gamma \mathcal{O}_K^m.$$

Proof. It follows from the fact that K has class number one and the structure theorem of finitely generated modules over PIDs. □

Proof of Proposition 3.4.9. Consider the equality

$$[\mathcal{O}_K^m / {}^tT\mathcal{M}] = [\mathcal{O}_K^m/\mathcal{M}][\mathcal{M}/{}^tT\mathcal{M}]. \tag{3.13}$$

Then we directly have

$$[\mathcal{M}/{}^tT\mathcal{M}] = (\det T)\mathcal{O}_K.$$

By Lemma 3.4.10 there exists $\gamma \in \mathrm{GL}_m(K)$ that satisfies $\mathcal{M} = \gamma\mathcal{O}_K^m$, and hence we get

$$[\mathcal{O}_K^m/\mathcal{M}] = (\det \gamma)\mathcal{O}_K.$$

Moreover, it follows from Proposition 3.4.7 that if $(\mathcal{M}, T)$ is principally polarized, then it satisfies ${}^tT\mathcal{M} = \overline{\mathcal{M}}^\vee$. By definition of the different ideal we have $(\mathcal{O}_K^m)^\vee = (\mathcal{D}_K^{-1})^m = \delta^{-1}\mathcal{O}_K^m$.

Therefore, if $(\mathcal{M}, T)$ is principally polarized, then we have

$$\begin{aligned}[\mathcal{O}_K^m/{}^tT\mathcal{M}] &= [\mathcal{O}_K^m/\overline{\mathcal{M}}^\vee] = \overline{[\mathcal{O}_K^m/\mathcal{M}^\vee]} = \overline{[\mathcal{O}_K^m/{}^t\gamma^{-1}(\mathcal{O}_K^m)^\vee]} \\ &= \overline{[\mathcal{O}_K^m/\delta^{-1}{}^t\gamma^{-1}\mathcal{O}_K^m]} = \overline{\det(\delta\gamma)^{-1}\mathcal{O}_K} = \overline{\det(\delta\gamma)}^{-1}\mathcal{O}_K\end{aligned}$$

Altogether, (3.13) gives that if $(\mathcal{M}, T)$ is principally polarized, then we obtain

$$\overline{\det(\delta\gamma)}^{-1}\mathcal{O}_K = (\det\gamma)\mathcal{O}_K \cdot (\det T)\mathcal{O}_K,$$

or equivalently

$$(\det\gamma)\overline{(\det\gamma)}\mathcal{O}_K = \overline{\det(\delta T)}^{-1}\mathcal{O}_K = \det(\delta T)^{-1}\mathcal{O}_K.$$

We conclude

$$\begin{aligned}\mathrm{N}_{K/K^+}([\mathcal{O}_K^m/\mathcal{M}]) &= \mathrm{N}_{K/K^+}((\det\gamma)\mathcal{O}_K) \\ &= (\det\gamma)\overline{(\det\gamma)}\mathcal{O}_{K^+} = (\det(\delta T)^{-1})\mathcal{O}_{K^+}.\end{aligned}$$ □

Remark 3.4.11. The assumption that K has class number one is not necessary in Proposition 3.4.9, but it does simplify the proof and it is enough for our case $K = \mathbb{Q}(\zeta_5)$. One could also justify the equality by proving it locally for all primes $\mathfrak{p} \in \mathcal{O}_K$.

In the situation above we define the matrix $S = \delta T$, which is hermitian. We say that a hermitian matrix $S \in \mathrm{GL}_m(K)$ has *signature* $((r_1, \dots, r_e), (s_1, \dots, s_e))$ if for every $\nu = 1, \dots, e$, the matrix $\phi_\nu(S)$ has r_ν positive eigenvalues and s_ν negative ones. In the case above we obtain that the signature of S is completely determined by the signature of T and the image by ϕ_ν of δ. The following result characterizes the equivalence between hermitian matrices with the same signature.

Theorem 3.4.12 (Shimura)**.** Let K be a CM-field, let K^+ be its maximal totally real subfield and let m be an odd positive integer. If $S_1, S_2 \in \mathrm{GL}_m(K)$ are hermitian matrices with equal signature, then there exist a matrix $U \in \mathrm{GL}_m(K)$, and a constant $c \in (K^+)^{>>0}$ that satisfy $cS_2 = {}^tUS_1\overline{U}$.

Proof. This is a special case of Proposition 5.9 in Shimura [40]. The notation in [40] is introduced in paragraphs 5.0 and 5.7, and it is very different from ours. For reference, we now say how it is related.

The condition "$J_\lambda(V, \Phi) = J_\lambda(V, \Phi')$ for $1 \leq \lambda \leq t$" translates to the signature equality condition. The fact that in our case K is a CM-field means that this signature equality holds for all embeddings of K into $\mathbb{C}$, that is, for "$t = r$" in Shimura's notation.

Then [40, Proposition 5.9] states exactly that there exist $U \in \mathrm{GL}_m(K)$ and $c \in (K^+)^\times$ such that $cS_2 = {}^tUS_1\overline{U}$. In the proof of Proposition 5.9 in [40], Shimura concludes that the constant c in the statement satisfies "$c \equiv 1 \pmod{\prod_{\lambda=1}^t \mathfrak{p}_{\infty_\lambda}}$", which in our setting translates to c being totally positive. □

Proposition 3.4.13. Let $K = \mathbb{Q}(\zeta_5)$ and let $(\mathcal{M}, T)$ be a principally polarized $\mathcal{O}_K$-lattice with $\mathrm{sign}(T) = ((3, 2), (0, 1))$. There exists an $\mathcal{O}_K$-lattice $\mathcal{M}'$ that satisfies

$$(\mathcal{M}, T) \sim (\mathcal{M}', T_0)$$

for T_0 as defined in Example 3.4.2.

In order to prove the proposition we need the following easy lemmas, which can be easily proven with SageMath [49].

Lemma 3.4.14. Let $K = \mathbb{Q}(\zeta_5)$ and $K^+ = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. We have

$$(\mathcal{O}_{K^+}^\times)^{>>0} = \mathrm{N}_{K/K^+}(\mathcal{O}_K^\times) \subseteq \mathrm{N}_{K/K^+}(K^\times). \qquad \square$$

Lemma 3.4.15. The element $\delta = -4\zeta_5^3 + 2\zeta_5^2 - 2\zeta_5 - 1$ is a generator of $\mathcal{D}_K$ that satisfies $\overline{\delta} = -\delta$. □

Proof of Proposition 3.4.13. Let δ be as in Lemma 3.4.15, and define $S = \delta T$ and $S_0 = \delta T_0$.

By Lemma 3.4.10 there exists $\gamma \in \mathrm{GL}_3(K)$ such that $\mathcal{M} = \gamma\mathcal{O}_K^3$, hence we can assume without loss of generality $\mathcal{M} = \mathcal{O}_K^3$, and by Proposition 3.4.8 we get $\det S \in \mathcal{O}_{K^+}^\times$.

Moreover, by Theorem 3.4.12 there exist $\alpha \in \mathrm{GL}_3(K)$ and $c \in (K^+)^{>>0}$ that satisfy

$$ {}^t\alpha S\overline{\alpha} = cS_0. \tag{3.14}$$

Taking determinants of (3.14) we obtain

$$ \mathrm{N}_{K/K^+}(\det\alpha)\det S = c^3 \det S_0, \tag{3.15}$$

so for $u = \det S/\det S_0$ and $\beta = \frac{c}{\det\alpha}\alpha$ we get

$$ {}^t\beta S\overline{\beta} = \frac{c^2}{N_{K/K^+}(\det\alpha)}\,{}^t\alpha S\overline{\alpha} = \frac{c^3}{N_{K/K^+}(\det\alpha)}S_0 = uS_0. \tag{3.16}$$

If we apply Proposition 3.4.9 to the principally polarized $\mathcal{O}_K$-lattice $(\mathcal{M}, T)$, then we obtain $\det S \in \mathcal{O}_{K^+}^\times$, and we can compute $\det S_0 \in \mathcal{O}_{K^+}^\times$, thus we have $u = \det S/\det S_0 \in \mathcal{O}_{K^+}^\times$. Moreover, the unit u is totally positive, because S and S_0 have the same signature. Then it follows from Lemma 3.4.14 that there exists an element $d \in K^\times$ which satisfies $u = \mathrm{N}_{K/K^+}(d)$, so by taking $\gamma = \beta/d$ we get ${}^t\gamma S\overline{\gamma} = S_0$. We conclude that $(\mathcal{M}, T)$ is equivalent to $(\gamma^{-1}\mathcal{M}, T_0)$. □

Definition 3.4.16. Let $S \in \mathrm{GL}_m(K)$ be a hermitian matrix, and let $\mathcal{M}$ be an $\mathcal{O}_K$-lattice.

- ▷ The *S-norm* of $\mathcal{M}$ is the fractional $\mathcal{O}_{K^+}$-ideal $\mu^S(\mathcal{M}) = ({}^tuS\overline{u} : u \in \mathcal{M})$.
- ▷ The *S-scale* of $\mathcal{M}$ is the fractional $\mathcal{O}_K$-ideal $\mu_0^S(\mathcal{M}) = ({}^tuS\overline{v} : u, v \in \mathcal{M})$.
- ▷ An $\mathcal{O}_K$-lattice is *S-maximal* if it is inclusion-maximal among those with the same S-norm.
- ▷ We define the group of matrices $\mathcal{G}(S) = \{V \in \mathrm{GL}_m(K) : {}^tVSV = S\}$.

Theorem 3.4.17. Let K be a CM-field, let K^+ be its maximal totally real subfield and assume that their class numbers h_K, h_{K^+} are equal. Let m be an odd positive integer, let $S \in \mathrm{GL}_m(K)$ be a hermitian matrix and assume that there exists an embedding $\phi : K \to \mathbb{C}$ with respect to which the signature of S is neither $(m, 0)$ nor $(0, m)$. Then for every S-maximal $\mathcal{O}_K$-lattice $\mathcal{L}$ in K^m, the $\mathcal{G}(S)$-orbit of $\mathcal{L}$ consists of all the S-maximal $\mathcal{O}_K$-lattices $\mathcal{M}$ with the same S-norm.

Proof. In [40], Shimura introduces the concept of *genus* of $\mathcal{O}_K$-lattices with respect to $\mathcal{G}(S)$ as a local version of class with respect to $\mathcal{G}(S)$. Given a non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_{K^+}$ we denote by $K_\mathfrak{p}^+$ the completition of K^+ with respect to $\mathfrak{p}$, and we write $K_\mathfrak{p} = K \otimes K_\mathfrak{p}^+$ and $\mathcal{L}_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}^+}\mathcal{L}$. With this notation, two

$\mathcal{O}_K$-lattices belong to the same genus with respect to $\mathcal{G}(S)$ if for every $\mathfrak{p}$ there exists a matrix $U \in \mathcal{G}_{\mathfrak{p}}(S) = \{V \in \mathrm{GL}_3(K_{\mathfrak{p}}) : {}^tVSV = S\}$ such that $U\mathcal{L}_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}$.

By [40, Proposition 5.24(i)] we have that, since the respective class numbers of K and K^+ are equal, every genus with respect to $\mathcal{G}(S)$ consists of a single class. Moreover, by [40, Proposition 5.25(iv)] the genus of an S-maximal $\mathcal{O}_K$-lattice $\mathcal{L}$ with respect to $\mathcal{G}(S)$ is the set of all S-maximal $\mathcal{O}_K$-lattices $\mathcal{M}$ with the same S-norm, which completes the proof. □

We will use the following two easy lemmas, whose proofs are in Shimura [40].

Lemma 3.4.18 (Proposition 2.11 in Shimura [40])**.** Let K be a CM-field, let K^+ be its maximal totally real subfield, let m be a positive integer and let $\mathcal{D}_{K/K^+}$ be the relative different of K/K^+. Let $\mathcal{M}$ be an $\mathcal{O}_K$-lattice in K^m and let $S \in \mathrm{GL}_m(K)$ be a hermitian matrix. The S-norm $\mu^S(\mathcal{M})$ and S-scale $\mu_0^S(\mathcal{M})$ of $\mathcal{M}$ satisfy the inclusions

$$\mu^S(\mathcal{M})\mathcal{O}_K \subseteq \mu_0^S(\mathcal{M}) \subseteq \mathcal{D}_{K/K^+}^{-1}\mu^S(\mathcal{M}).$$ □

Lemma 3.4.19 (Proposition 2.14 in Shimura [40])**.** Let $\mathcal{M}$ be an $\mathcal{O}_K$-lattice in K^m and let $S \in \mathrm{GL}_m(K)$ be a hermitian matrix. There exists an S-maximal $\mathcal{O}_K$-lattice $\mathcal{L}$ that contains $\mathcal{M}$. □

Proposition 3.4.20. Let $K = \mathbb{Q}(\zeta_5)$ and let δ be as in Lemma 3.4.15. Let $(\mathcal{M}, T)$ be a principally polarized $\mathcal{O}_K$-lattice and let $S = \delta T$. Then we have

$$\mu_0^S(\mathcal{M}) = \mathcal{O}_K \quad \text{and} \quad \mu^S(\mathcal{M}) = \mathcal{O}_{K^+}.$$

Moreover let $\mathcal{M}' \supsetneq \mathcal{M}$ be an S-maximal $\mathcal{O}_K$-lattice with $\mu^S(\mathcal{M}') = \mu^S(\mathcal{M})$. Then we have

$$\mu_0^S(\mathcal{M}') = (\zeta_5 - 1)^{-1}\mathcal{O}_K.$$

Proof. We start by computing the S-scale of $\mathcal{M}$. Since $(\mathcal{M}, T)$ is principally polarized, given $u, v \in \mathcal{M}$ we have

$$\mathrm{tr}_{K/\mathbb{Q}}(r\,{}^tuT\overline{v}) \in \mathbb{Z} \text{ for all } r \in \mathcal{O}_K.$$

In consequence we get ${}^tuT\overline{v} \in \mathcal{O}_K^\vee = \delta^{-1}\mathcal{O}_K$, hence ${}^tuS\overline{v} \in \mathcal{O}_K$ holds. Conversely, we want to show that there exist $u, v \in \mathcal{M}$ that satisfy ${}^tuS\overline{v} = 1$. By Lemma 3.4.10 we assume without loss of generality $\mathcal{M} = \mathcal{O}_K^3$, so we have $S \in \mathcal{O}_K^{3\times 3}$, and by Proposition 3.4.9 the matrix S has determinant $\det S \in \mathcal{O}_{K^+}^\times$. Then, for $v = {}^t(1,0,0)$ and $u = {}^tS^{-1}\,{}^t(1,0,0) \in \mathcal{M}$ we have ${}^tuS\overline{v} = 1$.

We compute now the S-norm of $\mathcal{M}$. The different of K/K^+ is the prime ideal $\mathfrak{p} = (\zeta_5 - 1)\mathcal{O}_K$, hence by Lemma 3.4.18 we have

$$\mathfrak{p} \subseteq \mu^S(\mathcal{M})\mathcal{O}_K \subseteq \mathcal{O}_K.$$

But $\mu^S(\mathcal{M})$ is an $\mathcal{O}_{K^+}$-ideal, and $\sqrt{5}\mathcal{O}_{K^+}$ ramifies in K/K^+ into $\mathfrak{p}^2$, so we conclude $\mu^S(\mathcal{M}) = \mathcal{O}_{K^+}$.

For the second part of the statement consider again Lemma 3.4.18 for $\mathcal{M}'$. By assumption we have $\mu^S(\mathcal{M}') = \mu^S(\mathcal{M}) = \mathcal{O}_{K^+}$, hence we obtain

$$\mathcal{O}_K \subseteq \mu_0^S(\mathcal{M}') \subseteq \mathfrak{p}^{-1}. \tag{3.17}$$

We have $\mathcal{M}' \supsetneq \mathcal{O}_K^3$, hence given an element

$$u = (u_1, u_2, u_3) \in \mathcal{M}' \backslash \mathcal{O}_K^3,$$

we assume without loss of generality $u_1 \notin \mathcal{O}_K$. Take also $v = \overline{S}^{-1}\,{}^t(1,0,0) \in \mathcal{M}'$. Then we have

$$\mu_0^S(\mathcal{M}') \ni {}^t u S \overline{v} = (u_1, u_2, u_3) S S^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = u_1 \notin \mathcal{O}_K,$$

thus we obtain $\mu_0^S(\mathcal{M}') \supsetneq \mathcal{O}_K$. The result then follows from (3.17), since $\mathfrak{p}$ is a prime ideal. □

Using the properties above and SageMath [49] we have found that, for $\mathfrak{p} = \mathcal{D}_{K/K^+} = (\zeta_5 - 1)\mathcal{O}_K$ and $S_0 = \delta T_0$, the $\mathcal{O}_K$-lattice

$$\mathcal{L} = \mathcal{O}_K^3 + \mathfrak{p}^{-1}(1, 2, 0) \tag{3.18}$$

is an S_0-maximal $\mathcal{O}_K$-lattice with S_0-norm $\mathcal{O}_{K^+}$ strictly containing $\mathcal{M}_0$, thus $\mathcal{M}_0$ is not S_0-maximal. Therefore we cannot use Theorem 3.4.17 directly on $\mathcal{M}_0$, but we use it on $\mathcal{L}$.

Proposition 3.4.21. Let $K = \mathbb{Q}(\zeta_5)$, let $(\mathcal{M}, T)$ be a principally polarized $\mathcal{O}_K$-lattice with $\operatorname{sign}(T) = ((3,2),(0,1))$ and let $\mathcal{L}$ be as in (3.18). Then there exists an $\mathcal{O}_K$-lattice $\mathcal{M}'$ in K^3 that satisfies $(\mathcal{M}, T) \sim (\mathcal{M}', T_0)$, $\mathcal{M}' \subseteq \mathcal{L}$ and $\mathcal{L}/\mathcal{M}' \cong \mathcal{O}_K/\mathfrak{p}$.

Proof. By Proposition 3.4.13 we can assume $T = T_0$. Let δ be as defined in Lemma 3.4.15, and define the hermitian matrix $S_0 = \delta T_0$. By Lemma 3.4.19 there exists $\mathcal{N} \supseteq \mathcal{M}$ S_0-maximal with S_0-norm $\mu^{S_0}(\mathcal{N}) = \mu^{S_0}(\mathcal{M})$, which by Proposition 3.4.20 satisfies $\mu^{S_0}(\mathcal{M}) = \mathcal{O}_{K^+}$.

Since both $\mathcal{N}$ and $\mathcal{L}$ are S_0-maximal $\mathcal{O}_K$-lattices with S_0-norm $\mathcal{O}_{K^+}$, we have by Theorem 3.4.17 that they are in the same $\mathcal{G}(S_0)$-orbit. Therefore there exists $\gamma \in \mathcal{G}(S_0)$ such that $\gamma\mathcal{N} = \mathcal{L}$.

For $\mathcal{M}' = \gamma\mathcal{M}$ we have $(\mathcal{M}, S_0) \sim (\mathcal{M}', S_0)$, and $\mathcal{M}'$ satisfies $\mathcal{M}' \subseteq \mathcal{L}$ and $\mu^{S_0}(\mathcal{M}') = \mathcal{O}_{K^+}$. Next we prove $\mathcal{L}/\mathcal{M}' \cong \mathcal{O}_K/\mathfrak{p}$.

By Proposition 3.4.20 we have $\mu_0^S(\mathcal{L}) = \mathfrak{p}^{-1}$, which implies $\mathfrak{p}\mathcal{L} \subseteq \mathcal{M}'$, hence the quotient $\mathcal{L}/\mathcal{M}'$ is an $(\mathcal{O}_K/\mathfrak{p})$-module. Therefore, since $\mathfrak{p}$ is prime, it is enough to show $[\mathcal{L}/\mathcal{M}'] = \mathfrak{p}$ or, equivalently, $\mathrm{N}_{K/K^+}([\mathcal{L}/\mathcal{M}']) = \sqrt{5}\mathcal{O}_{K^+}$. We have

$$\mathrm{N}_{K/K^+}([\mathcal{L}/\mathcal{M}']) = \mathrm{N}_{K/K^+}([\mathcal{L}/\mathcal{O}_K^3])\,\mathrm{N}_{K/K^+}([\mathcal{O}_K^3/\mathcal{M}']),$$

and since $(\mathcal{M}', S_0)$ is principally polarized, by Proposition 3.4.9 we have $\mathrm{N}_{K/K^+}([\mathcal{O}_K^3/\mathcal{M}']) = \mathcal{O}_{K^+}$. The equality $\mathrm{N}_{K/K^+}([\mathcal{L}/\mathcal{O}_K^3]) = \sqrt{5}\mathcal{O}_{K^+}$ holds by Proposition 3.4.8.(2), since we have $\mathcal{L} = L\mathcal{O}_K^3$ for the matrix

$$L = \begin{pmatrix} -\frac{3}{5}\zeta_5^3 - \frac{1}{5}\zeta_5^2 + \frac{1}{5}\zeta_5 - \frac{2}{5} & -\frac{1}{5}\zeta_5^3 - \frac{2}{5}\zeta_5^2 + \frac{2}{5}\zeta_5 + \frac{1}{5} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we compute $\det L = \sqrt{5}$. This completes the proof. □

Using Script 1 in [46] we computed all $\mathcal{O}_K$-lattices $\mathcal{M}$ such that $\mathcal{L}/\mathcal{M}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}$, and we obtained 6 different $\mathcal{O}_K$-lattices.

By Lemma 3.4.10, for every $\mathcal{O}_K$-lattice $\mathcal{M}$ there exists $\gamma \in \mathrm{GL}_3(K)$ that satisfies $\mathcal{M} = \gamma\mathcal{O}_K$, so we computed the equivalent pair $\gamma^{-1}(\mathcal{M}, T_0) = (\mathcal{M}_0, T_{\mathcal{M}})$.

Then, for every $\mathcal{O}_K$-lattice that we obtained with Script 1 we managed to find $\alpha \in \mathrm{GL}_3(\mathcal{O}_K)$ that satisfies ${}^t\alpha T_{\mathcal{M}}\overline{\alpha} = T_0$. For the explicit computations see Script 2 in [46].

We conclude that all polarized $\mathcal{O}_K$-lattices $(\mathcal{M}, T_0)$ such that $\mathcal{L}/\mathcal{M}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}$ are equivalent to $(\mathcal{M}_0, T_0)$, so we can now prove the main theorem of this section.

Proof of Theorem 3.4.5. By Example 3.4.2 the pair $(\mathcal{M}_0, T_0)$ is equivalent to a pair $(\mathcal{M}_1, T_1) \in \Upsilon(\mathfrak{Z})$ that we obtained in Section 3.3 from a Riemann form with determinant 1.

Therefore, by Proposition 3.4.3, if $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ is equivalent to the pair $(\mathcal{M}_0, T_0) \sim (\mathcal{M}_1, T_1)$, then the polarized abelian varieties $A(Z, \mathcal{M}, T)$ for $Z \in \mathcal{H}_{\mathfrak{Z}}$ are principally polarized.

For the other implication let $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ such that $\zeta_5\mathcal{M} \subseteq \mathcal{M}$. Then the pair $(\mathcal{M}, T)$ is a polarized $\mathcal{O}_K$-lattice whose hermitian matrix T has signature $((3,2),(0,1))$. If $A(Z, \mathcal{M}, T)$ is principally polarized, then $(\mathcal{M}, T)$ is principally polarized as a polarized $\mathcal{O}_K$-lattice.

Therefore it follows from Proposition 3.4.21 that there exists an equivalent pair $(\mathcal{M}', T_0)$ with $\mathcal{M}' \subseteq \mathcal{L}$ and $\mathcal{L}/\mathcal{M}' \cong \mathcal{O}_K/\mathfrak{p}$. But we have seen that there are only 6 possibilities for such $\mathcal{M}'$ and they all satisfy $(\mathcal{M}', T_0) \sim (\mathcal{M}_0, T_0)$, hence the result follows. □

3.5 The Torelli locus of CPQ curves

In this section we solve the Riemann-Schottky problem for CPQ curves and give a result analogous to Proposition 1.4.1 for the family $\mathcal{S}$ of CPQ curves.

In Proposition 1.4.1 we focused on principally polarized abelian threefolds, which all are Jacobians of curves, so we only needed to prove that the curves were Picard curves. The main obstacle to obtain an analogous result for CPQ curves is that, since CPQ curves have genus 6, their Jacobians have dimension 6, but when considering 6-dimensional principally polarized abelian varieties, not all of them are Jacobians of curves.

However, we have seen in Proposition 3.3.1 that Jacobians of CPQ curves have 3-CM-type

$$\mathfrak{Z} = (\mathbb{Q}(\zeta_5), (\phi_1, \phi_2), (3,2), (0,1)) \text{ with } \phi_i : \mathbb{Q}(\zeta_5) \to \mathbb{C} \text{ given by } \phi_i(\zeta_5) = z_5^i. \tag{3.19}$$

Therefore we focus on the set of principally polarized abelian varieties with 3-CM-type $\mathfrak{Z}$ and order-5 automorphisms. Let $\mathcal{M}_0 = \mathcal{O}_K^3$ and consider T_0 as in Example 3.4.2. Let A_6 be the smooth algebraic variety as in [28], which has complex points

$$\mathsf{A}_6(\mathbb{C}) = \mathrm{Sp}_{12}(\mathbb{Z})\backslash\mathbf{H}_6,$$

and let $\mathsf{A}_{\mathfrak{Z}} \subseteq \mathsf{A}_6$ be the image of $\mathcal{H}_{\mathfrak{Z}}$ by the map

$$\begin{aligned} &\mathcal{H}_{\mathfrak{Z}} \to \mathrm{Sp}_{12}(\mathbb{Z})\backslash\mathbf{H}_6, \\ &\quad Z \mapsto (\text{the class of a period matrix } \Omega \text{ of } A(Z, \mathcal{M}_0, T_0)). \end{aligned}$$

Let M_6 be the moduli space of genus-6 curves. We define the *open Torelli locus* T_6° as the image $J(\mathsf{M}_6) \subseteq \mathsf{A}_6$ of M_6 by the Torelli map J, and we call its Zariski closure $\mathsf{T}_6 = \overline{\mathsf{T}_6^\circ}$ the *Torelli locus*. The points $X \in \mathsf{T}_6 \backslash \mathsf{T}_6^\circ$ correspond to decomposable principally polarized abelian varieties. For more details, see Section 1 in Moonen-Oort [28].

In order to prove our result, we need to assume the following conjecture.

Conjecture 3.5.1. The set $\mathsf{A}_{\mathfrak{Z}}$ is an algebraic subset of the variety A_6, that is, a Zariski-closed subset.

Remark 3.5.2. We are convinced that this follows from the basics of Shimura varieties. However, since we are not familiar enough with the theory and due to time restrictions we have not been able to prove the conjecture yet.

Theorem 3.5.3. Assume that Conjecture 3.5.1 holds and let X be a simple principally polarized abelian variety of dimension 6 over $\mathbb{C}$. The following are equivalent:

(1) The principally polarized abelian variety X has an automorphism φ of order 5 such that the eigenvalues of $\rho_a(\varphi)$ are z_5, z_5^2 and z_5^3 with multiplicity 3, 2 and 1 respectively.
(2) There exists a cyclic plane quintic curve C that satisfies $X \cong J(C)$ and for $\rho \in \mathrm{Aut}(C)$ given by $\rho(x, y) = (x, \zeta_5 y)$, we get $\varphi = \rho_*$.

For the last step of the proof we will need the following result:

Lemma 3.5.4. If C is a curve given by $y^5 = f(x)$ where the x-map $C \to \mathbb{P}_1$ has 5 ramification points, then C is isomorphic to a curve with one of the following forms:

(1) $y^5 = x(x-1)(x-\lambda)(x-\mu)$,
(2) $y^5 = x^3(x-1)(x-\lambda)(x-\mu)$, or
(3) $y^5 = x^2(x-1)^2(x-\lambda)(x-\mu)$.

Moreover if ρ is the automorphism of C given by $\rho(x, y) = (x, z_5 y)$, then the eigenvalues of $\rho_a(\rho_*)$ are in each case

(1) z_5, z_5^2 and z_5^3 with multiplicity 3, 2 and 1 respectively;
(2) z_5, z_5^2, z_5^3 and z_5^4 with multiplicity 2, 2, 1 and 1 respectively; or
(3) z_5, z_5^2, z_5^3 and z_5^4 with multiplicity 2, 1, 2 and 1 respectively.

Proof. Let C be given by

$$y^5 = f(x) := (x-a_1)^{e_1}(x-a_2)^{e_2}(x-a_3)^{e_3}(x-a_4)^{e_4}(x-a_5)^{e_5},$$

for $a_i \in \mathbb{C}$, $e_i \in \mathbb{Z}_{\geq 0}$ and $a_i \neq a_j$ if $i \neq j$.

Since the curve is ramified exactly at the points $(a_i, 0)$, we have

$$e_i \not\equiv 0 \pmod 5 \quad \text{and} \quad \sum_{i=1}^{5} e_i \equiv 0 \pmod 5.$$

Furthermore, we only need to consider the class $\overline{e_i} = (e_i \bmod 5)$, and the polynomials f^k with $k \not\equiv 0 \pmod 5$ all give the same curve, thus we can consider the vector $(\overline{e_1}, \overline{e_2}, \overline{e_3}, \overline{e_4}, \overline{e_5}) \in (\mathbb{Z}/5\mathbb{Z})^5$ up to multiplication by $(\mathbb{Z}/5\mathbb{Z})^\times$.

With these conditions we obtain three possible exponent vectors, which are precisely $(1,1,1,1,1)$, $(1,1,1,3,4)$ and $(1,1,2,2,4)$. We can then consider an isomorphic curve where the points with larger exponents are at $(1:0:0)$, $(0:0:1)$ and $(1:0:1)$, thus obtaining the models in the statement.

The first case corresponds to the family of CPQ curves, so we have already computed the eigenvalues of $\rho_a(\rho_*)$ in that case. For the remaining two cases

we computed a basis of differentials using the *algcurves* library [8] in Maple [27]. We obtained respectively the bases

$$\left(\frac{dx}{y}, \frac{xdx}{y^2}, \frac{xdx}{y^3}, \frac{x^2dx}{y^3}, \frac{x^2dx}{y^4}, \frac{x^3dx}{y^4}\right)$$

and

$$\left(\frac{dx}{y}, \frac{dx}{y^2}, \frac{xdx}{y^2}, \frac{x(x-1)dx}{y^3}, \frac{x(x-1)dx}{y^4}, \frac{x(x^2-1)dx}{y^4}\right).$$

Then we computed the eigenvalues of $\rho_a(\rho_*)$ by considering the action of ρ^* on the basis of $H^0(\omega_C)$ for each case, as we did for CPQ curves in Section 3.3. □

We prove now the main result of the chapter.

Proof of Theorem 3.5.3. That (2) implies (1) follows from Proposition 3.3.1. We will now prove the converse.

Suppose that X satisfies (1) and let $\mathfrak{Z}$ be the 3-CM-type defined in (3.19). We start by proving that X is in $\mathsf{A}_{\mathfrak{Z}}$. Then we show that $\mathsf{A}_{\mathfrak{Z}}$ is an irreducible subvariety of the Torelli locus, hence there exists $C \in \mathsf{M}_6$ whose Jacobian is isomorphic to X, and finally we prove that C is a CPQ curve.

Let λ be the principal polarization of X and consider the embedding $\iota : \mathbb{Q}(\zeta_5) \to \mathbb{C}$ given by $\iota(\zeta_5) = \varphi$. As φ is an automorphism of the principally polarized abelian variety X, it satisfies $\lambda = \widehat{\varphi} \circ \lambda \circ \varphi$. We obtain

$$\iota(\zeta_5)' = \varphi' = \lambda^{-1} \circ \widehat{\varphi} \circ \lambda = \varphi^{-1} = \iota(\zeta_5)^{-1} = \iota(\overline{\zeta_5}),$$

thus the Rosati involution on $\mathrm{End}(X) \otimes \mathbb{Q}$ with respect to the polarization λ extends the complex conjugation on K via ι.

Then the triple (X, λ, ι) has 3-CM-type $\mathfrak{Z}$, hence by Proposition 3.2.5 there exist $(\mathcal{M}, T) \in \Upsilon(\mathfrak{Z})$ and $Z \in \mathcal{H}_{\mathfrak{Z}}$ that satisfy $A(Z, \mathcal{M}, T) \cong (X, \lambda, \iota)$. Since we have $\iota(\zeta_5) = \varphi \in \mathrm{End}(X)$, the lattice $\mathcal{M}$ satisfies $\zeta_5\mathcal{M} \subseteq \mathcal{M}$.

By Theorem 3.4.5 the pair $(\mathcal{M}, T)$ is equivalent to $(\mathcal{M}_0, T_0)$, so it follows from Proposition 3.4.3 that there exists $Z' \in \mathcal{H}_{\mathfrak{Z}}$ such that $A(Z', \mathcal{M}_0, T_0)$ is isomorphic to $A(Z, \mathcal{M}, T) \cong (X, \lambda, \iota)$. We conclude that the class of X is in $\mathsf{A}_{\mathfrak{Z}}$.

Next we prove that $\mathsf{A}_{\mathfrak{Z}}$ is an irreducible subvariety of the Torelli locus. On the one hand, the complex manifold $\mathcal{H}_{\mathfrak{Z}} = \mathcal{H}_{3,0} \times \mathcal{H}_{2,1} \cong \mathcal{H}_{2,1}$ is irreducible and has dimension 2, hence if $\mathsf{A}_{\mathfrak{Z}}$ is an algebraic subset of A_6, then it is an irreducible closed subvariety of A_6. On the other hand, the family of CPQ curves $\mathcal{S} \subseteq \mathsf{M}_6$ also has dimension 2, as can be seen from the Legendre-Rosenhain equation $y^5 = x(x-1)(x-\lambda)(x-\mu)$. The closure S of its image $J(\mathcal{S})$ by the Torelli map is then a dimension-2 closed subvariety, and since by Proposition 3.3.1 we have $J(S) \subseteq \mathsf{A}_{\mathfrak{Z}}$, we get that S is also contained in $\mathsf{A}_{\mathfrak{Z}}$.

It follows that S is a closed irreducible subvariety of the irreducible variety A_3. Therefore, by definition of dimension (see Definition 2.48 in Milne [26]), we obtain $\mathsf{S} = \mathsf{A}_3$.

We conclude that the class of X is in $\mathsf{S} \subseteq \mathsf{T}_6$ and, as X is simple, it is in fact in T_6°, so there is a curve C that satisfies $J(C) \cong X$.

Finally we prove that C is a CPQ curve and $\varphi = \rho_*$.

By Torelli's Theorem 1.1.1, there is some non-trivial $\nu \in \mathrm{Aut}(C)$ such that $\varphi = \pm\nu_*$. Then the automorphism $\eta = \nu^6$ satisfies $\eta_* = (\nu^6)_* = (\pm\nu)_*^6 = \varphi^6 = \varphi$, hence by the uniqueness in Torelli's Theorem 1.1.1 we get that η has order 5.

It follows that the projection $\pi : C \to C/\langle\eta\rangle$ is a cyclic Galois covering map of degree 5, hence all the ramification indices of π are either 1 or 5. Therefore by the Riemann-Hurwitz formula one obtains that $C/\langle\eta\rangle$ has either genus 0 or 2. But X is simple, so the curve $C/\langle\eta\rangle$ is isomorphic to $\mathbb{P}^1$ and the map π has 5 ramification points.

Then $k(C)/k(C/\langle\eta\rangle)$ is a Kummer extension of degree 5, hence C is given by an equation of the form $y^5 = f(x)$, the x-map π has 5 ramification points, and η is a power of the automorphism ρ given by $(x, y) \mapsto (x, z_5 y)$. We conclude by Lemma 3.5.4 that, as the eigenvalues of $\rho_a(\varphi)$ are z_5, z_5^2 and z_5^3 with multiplicity 3, 2 and 1 respectively, the curve C is isomorphic to a curve of the form $y^5 = x(x-1)(x-\lambda)(x-\mu)$, that is, the curve C is a CPQ curve, and η is equal to ρ. □

It follows from Theorem 3.5.3 that if Conjecture 3.5.1 holds, then one can think of the input in Algorithm 2.2.6 as just a principally polarized abelian variety of dimension 6 with an order-5 automorphism whose analytic representation has the right eigenvalues.

CM cyclic plane quintic curves defined over $\mathbb{Q}$

4

In this chapter we give a complete list of CM-fields whose ring of integers occurs as the endomorphism ring over $\mathbb{C}$ of the Jacobian of a CPQ curve defined over $\mathbb{Q}$ with complex multiplication (CM). We do so by extending the methods for genus 2 and 3 due to Kılıçer [12], see also [15].

In Section 4.1 we define what a polarized abelian variety (or a curve) with complex multiplication is as a particular case of the polarized abelian varieties with m-CM-type that we defined in Chapter 3.

In Section 4.2 we define what the CM class number of a CM-field is, and its relation with the field of moduli of the polarized abelian variety. We also show as a direct consequence of Theorem 4.3.1 in Kılıçer [12] that the list of heuristic models of maximal CM Picard curves over $\mathbb{Q}$ in Section 1.5 is complete.

Finally, in Section 4.3 we focus on the case of CPQ curves, and prove that the fields appearing in the list in Section 2.3 are the only possible CM-fields by which a CPQ curve defined over $\mathbb{Q}$ can have maximal CM over $\mathbb{C}$.

4.1 CM-types

Let K be a CM-field. Throughout this chapter we refer to 1-CM-types as just *CM-types*, that is, sets $\Phi \subseteq \mathrm{Hom}(K, \mathbb{C})$ such that for every complex conjugate pair of homomorphisms $\phi, \overline{\phi}$, exactly one belongs to Φ. For details, see Shimura [42, Chapter II].

Definition 4.1.1. Let k be a proper CM-subfield of K with CM-type Φ_k. The CM-type of K *induced by* Φ_k is

$$\Phi = \{\phi \in \mathrm{Hom}(K, \mathbb{C}) : \phi|_k \in \Phi_k\}.$$

A CM-type Φ of K is *primitive* if it is not induced by any CM-type of any proper CM-subfield.

Definition 4.1.2. The *reflex field* K^r of a CM-type (K, Φ) is

$$K^r = \mathbb{Q}\left(\left\{\sum_{\phi\in\Phi} \phi(x) : x \in K\right\}\right) \subseteq \mathbb{C}.$$

Let now L be the normal closure of the extension $K/\mathbb{Q}$ and let Φ_0 be the CM-type of L induced by Φ. If we take $N \subseteq \mathbb{C}$ the unique subfield of $\mathbb{C}$ isomorphic to L, then we can see the elements in Φ_0 as homomorphisms (hence isomorphisms) from L to N. In this setting we define the *reflex CM-type*.

Definition 4.1.3. The *reflex CM-type* Φ^r of a CM-type (K, Φ) is

$$\Phi^r = \{\phi^{-1}|_{K^r} : \phi \in \Phi_0\}.$$

The CM-type (K^r, Φ^r) is called the *reflex* of (K, Φ).

Lemma 4.1.4 (Shimura, see [42, pg. 63])**.** Let (K, Φ) be a primitive CM-type. Then the reflex type of its reflex type (K^r, Φ^r) coincides with (K, Φ).

Definition 4.1.5. The *type norm* of a CM-type (K, Φ) is the multiplicative map

$$\begin{aligned} N_\Phi : K &\to K^r \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x). \end{aligned}$$

In this context, following Definition 3.1.1 we obtain that a *polarized abelian variety with complex multiplication* (CM) by (K, Φ) is a triple (X, λ, ι) where:

- ▷ X is an abelian variety over $\mathbb{C}$ of dimension g,
- ▷ λ is a polarization of X, and
- ▷ ι is a ring homomorphism $\iota : K \hookrightarrow \mathrm{End}(X) \otimes \mathbb{Q}$ such that:
  - the analytic representation $\rho_a \circ \iota$ is equivalent to the representation $\rho_\Phi = \mathrm{diag}(\phi_1, \ldots, \phi_g)$, and
  - the Rosati involution on $\mathrm{End}(X) \otimes \mathbb{Q}$ with respect to the polarization λ extends the complex conjugation on K via ι.

We say that it has *CM by an order* $\mathcal{O} \subseteq K$ if $\iota^{-1}(\mathrm{End}(X)) = \mathcal{O}$.

Lemma 4.1.6 (Theorem 1.3.5 in Lang [19])**.** A polarized abelian variety with CM-type (K, Φ) is absolutely simple if and only if Φ is primitive. □

In Sections 1.5 and 2.3 we defined a maximal CM Picard curve (respectively CPQ curve) to be a Picard curve (resp. CPQ curve) such that its Jacobian has endomorphism ring isomorphic to the maximal order of some sextic field K

(resp. a degree-12 field). The following result shows that then its Jacobian is a principally polarized abelian varieties with complex multiplication.

Proposition 4.1.7. If C is a maximal CM Picard curve (respectively CPQ curve), then there exist a primitive CM-type (K, Φ) and an embedding $\iota : K \to \mathrm{End}(J(C)) \otimes \mathbb{Q}$ such that $(J(C), \lambda_C, \iota)$ is a principally polarized abelian variety with CM by $\mathcal{O}_K$.

Proof. Assume C is a maximal CM Picard (respectively CPQ) curve. Then there exists a sextic (resp. degree-12) field K that satisfies $\mathrm{End}(J(C)) \cong \mathcal{O}_K$. In particular, the field K contains a primitive third root of unity $\zeta_3 \in K$ (resp. a primitive fifth root of unity $\zeta_5 \in K$), which corresponds via the isomorphism to the automorphism ρ_*.

We define $\iota : K \to \mathrm{End}(J(C) \otimes \mathbb{Q}$ to be the extension of the ring isomorphism $\mathcal{O}_K \to \mathrm{End}(J(C))$ and Φ to be a CM-type such that $\rho_a \circ \iota$ is equivalent to ρ_Φ.

As $J(C)$ is absolutely simple, by Lemma 4.1.6, the CM-type Φ is primitive. Moreover, the field K is a CM-field and the Rosati involution on $\mathrm{End}(J(C)) \otimes \mathbb{Q}$ with respect to λ_C extends the complex conjugation on K via ι, see for example Lemma 1.3.5.4 in Chai-Conrad-Oort [4]. □

In the case of (1-)CM-types, the moduli space $\mathcal{H}_{\mathbf{r},\mathbf{s}}$ contains only one point, thus one can find the corresponding period matrix following the construction due to Shimura that we gave in Section 3.2. For example, given a CM-type (K, Φ), Van Wamelen's method lists all pairs $(\mathcal{M}, T) \in \Upsilon(\Phi)$ as defined in Section 3.1 and then computes all the period matrices of principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ following the construction in Section 3.2, see [51] for details.

If we apply Van Wamelen's method to a primitive CM-type (K, Φ) where K is a sextic CM-field containing a primitive third root of unity $\zeta_3 \in K$, then we obtain a list of period matrices corresponding to principally polarized abelian threefolds with CM by $\mathcal{O}_K$ with a order-3 automorphism $\iota(\zeta_3)$. Hence by Proposition 1.4.1 they correspond to Jacobians of Picard curves. Obtaining the rational representation of $\iota(\zeta_3)$ with Van Wamelen's is then a matter of keeping track of the changes of basis throughout the algorithm.

4.2 The CM class number

In this section we introduce the concept of the *field of moduli* of a polarized abelian variety, which is closely related to the field of definition, and we see how it relates to the CM-field in the case of polarized abelian varieties with CM.

Theorem 4.2.1 (Shimura, see [41, pp. 130–131])**.** Let (X, λ) be a polarized abelian variety over $\mathbb{C}$, let K be a number field and let $\iota : \mathcal{O}_K \to \mathrm{End}(X)$ be an embedding. There exists a unique field $k \subseteq \mathbb{C}$ such that for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, the restriction of σ to k is the identity if and only if there exists an isomorphism $f : X \to {}^{\sigma}X$ that satisfies $f^{\vee} \circ {}^{\sigma}\lambda \circ f = \lambda$ and $f \circ \iota(a) = {}^{\sigma}\iota(a) \circ f$ for all $a \in \mathcal{O}_K$. □

The field k in Theorem 4.2.1 is called the *field of moduli* of (X, λ, ι).

In particular, if a polarized abelian variety (X, λ, ι) is defined over $\mathbb{Q}$, then its field of moduli is $\mathbb{Q}$. The following results give conditions on the field of moduli for polarized abelian varieties with CM.

Proposition 4.2.2 (Shimura [41, Proposition 5.17])**.** Let (K, Φ) and (K^r, Φ^r) be respectively a primitive CM-type and its reflex. Let (X, λ, ι) be a polarized abelian variety of CM-type (K, Φ). Let F be a subfield of K, $\iota|_F$ be the restriction of λ to F and M_F be the field of moduli of $(X, \lambda, \iota|_F)$. Then the following assertions hold:

(1) the field $M_F K^r$ is the field of moduli of (X, λ, ι),
(2) the reflex field K^r is normal over $M_F \cap K^r$,
(3) the field $M_F K^r$ is normal over M_F, and
(4) the group $\mathrm{Gal}(M_F K^r / M_F)$ is isomorphic to a subgroup of $\mathrm{Aut}(K/F)$.

Theorem 4.2.3 (Shimura-Taniyama [43, Main theorem 1])**.** Let (K, Φ) be a primitive CM-type and let (K^r, Φ^r) be its reflex CM-type. Let (X, λ, ι) be a polarized abelian variety of type (K, Φ) with CM by $\mathcal{O}_K$, and let M be the field of moduli of $(X, \lambda, \iota|_{\mathbb{Q}})$. Then MK^r is the unramified class field over K^r corresponding to the ideal group

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} : \exists \alpha \in K^{\times} \text{ such that } N_{\Phi^r}(\mathfrak{b}) = (\alpha),\ N_{K/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha}\}. \quad \square$$

Observe that if M is a subfield of K^r, then $I_{K^r}/I_0(\Phi^r)$ is trivial. In this context, the quotient $I_{K^r}/I_0(\Phi^r)$ is called the *CM class group* of (K, Φ) and when it is trivial we say that K has *CM class number one*.

Proposition 4.2.4. Let (X, λ) be an absolutely simple polarized abelian variety defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$. Then K has CM class number one and is normal over $\mathbb{Q}$.

Proof. Since (X, λ) is defined over $\mathbb{Q}$ we have $M_{\mathbb{Q}} = \mathbb{Q}$, by Proposition 4.2.2.(2), the field K^r is normal over $\mathbb{Q}$. We also have that, by Proposition 4.2.2.(4), the group $\mathrm{Gal}(K^r/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{Aut}(K/\mathbb{Q})$, hence we obtain

$$[K^r : \mathbb{Q}] = \#\,\mathrm{Gal}(K^r/\mathbb{Q}) \leq \#\,\mathrm{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}].$$

By Lemma 4.1.6, since X is absolutely simple we have that its CM-type Φ is primitive, so by Lemma 4.1.4 we get $K^{rr} = K$, and since K^r is normal we

	$p(x)$	h_K	h_K^*
(1)	$x^3 - 3x - 1$	1	1
(2)	$x^3 - x^2 - 2x + 1$	1	1
(3)	$x^3 - x^2 - 4x - 1$	1	1
(4)	$x^3 + x^2 - 10x - 8$	1	1
(5)	$x^3 - x^2 - 14x - 8$	1	1
(6)	$x^3 - 21x - 28$	3	1
(7)	$x^3 - 21x + 35$	3	1
(8)	$x^3 - 39x + 26$	3	1
(13)	$x^3 - 61x - 183$	4	4
(14)	$x^3 - x^2 - 22x - 5$	4	4

Table 4.1: List of CM class number one sextic CM-fields K containing a primitive third root of unity $\zeta_3 \in K$. We write $K = K_0(\zeta_3)$ for K_0 the splitting field of $p(x)$, and indicate the class number h_K of K and its relative class number $h_K^* := h_K/h_{K_0}$. The number in the first column indicates which curves in Section 1.5 are heuristic models for the Picard curves with maximal CM by K.

obtain that K^{rr} is isomorphic to a subfield of K^r. Altogether it gives us that K is isomorphic to K^r and therefore K is normal over $\mathbb{Q}$.

Lastly, by Proposition 4.2.2.(1) we have that the field of moduli of (X, λ, ι) is K^r, so it follows that K has CM class number one. □

Proposition 4.2.4 characterizes the CM-fields whose maximal order may occur as the endomorphism ring of a polarized abelian variety with CM.

Kılıçer studies in [12] the CM class number one fields that correspond to principally polarized abelian varieties of dimension 2 and 3. In particular, Table 3.1 in [12] includes a complete list of CM-fields whose ring of integers is the endomorphism ring of the Jacobian of a Picard curve.

Corollary 4.2.5 (See also Theorem 4.3.1 in Kılıçer [12])**.** Let C be a Picard curve defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$ for a sextic CM-field K. The field K is isomorphic to $K_0(\zeta_3)$, where ζ_3 is a primitive third root of unity and K_0 is the splitting field of a polynomial $p(x)$ from Table 4.1.

Proof. Let C be a Picard curve with CM by the ring of integers of a sextic CM-field K. Recall that C has an automorphism given by $\rho(x, y) = (x, z_3 y)$ that induces an automorphism ρ_* in the Jacobian. It follows that the field K contains a primitive third root of unity, and thus $k = \mathbb{Q}(\zeta_3)$ is a quadratic CM-subfield

whose discriminant has absolute value 3. The list in Table 4.1 contains all CM class number one cyclic sextic CM-fields of Table 3.1 in [12] with $d_k = 3$. □

It follows that the list in Section 1.5 contains heuristic models for all Picard curves with maximal CM that have a model over $\mathbb{Q}$. In the cases (13) and (14) we also list heuristic models defined over K_0 for three other Picard curves, which by Theorem 4.3.1 in Kılıçer [12] exist and have field of moduli K_0.

Remark 4.2.6. Park and Kwon [34, Table 3] give a complete list of all imaginary abelian sextic number fields K with class number $h_K \leq 11$. In particular, those with an imaginary quadratic subfield of conductor 3 contain a third root of unity, and thus occur as CM-fields of Picard curves.

Table 3 in [34] includes four fields with CM class number bigger than 1, for which we also applied Van Wamelen's method and obtained heuristic models for the corresponding Picard curves with maximal CM, see cases (9)–(12) in Section 1.5.

4.3 CM class number one fields for CPQ curves

The goal for this section is to give a result analogous to Corollary 4.2.5 in the case of CPQ curves, that is, we want to find all fields whose maximal order may occur as the endomorphism ring over $\mathbb{C}$ of the Jacobian of a CPQ curve with CM and defined over $\mathbb{Q}$.

By Proposition 4.2.4 we only need to look for CM class number one CM-fields that are Galois over $\mathbb{Q}$. We will prove the following result.

Theorem 4.3.1. Let C be a CPQ curve defined over $\mathbb{Q}$ with CM by the ring of integers of a degree-12 CM-field K. Then the field K is isomorphic to $K_0(\zeta_5)$, where ζ_5 is a primitive fifth root of unity and K_0 is the splitting field of a polynomial $p(x)$ from Table 4.2.

We start by listing the possible Galois groups of degree-12 Galois number fields containing a primitive fifth root of unity. Then we give a sufficient condition for such a field to have CM class number one and finally we study the necessary conditions for that to happen for each occurring Galois group.

Proposition 4.3.2. Let n be a positive integer, and consider the group given by the presentation

$$Q_{4n} = \langle s, t : s^{2n} = 1, s^n = t^2, sts = t \rangle.$$

The group Q_{4n} has order $4n$.

Proof. See pp. 347–348 in [36]. □

	$p(x)$	h_K	h_K^*
(1)	$x^3 - x^2 - 2x + 1$	1	1
(2)	$x^3 - 3x - 1$	1	1
(3)	$x^3 - x^2 - 4x - 1$	4	4
(4)	$x^3 - 12x - 14$	4	4

Table 4.2: List of CM class number one CM-fields K of degree 12 containing a primitive fifth root of unity $\zeta_5 \in K$. We write $K = F(\zeta_5)$ for F the splitting field of $p(x)$, and indicate the class number h_K of K and its relative class number $h_K^* := h_K/h_{K^+}$. The number in the first column indicates which curve in Section 2.3 is an heuristic model for the CPQ curve defined over $\mathbb{Q}$ with maximal CM by K over $\mathbb{C}$.

A group isomorphic to Q_{4n} as defined in Proposition 4.3.2 is called a *dicyclic group of order* $4n$.

Definition 4.3.3. Let N and H be two groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism. *The semidirect product* $N \rtimes H$ *of* N *and* H *with respect to* φ is the Cartesian product $N \times H$ together with the operation

$$(n, h)(n', h') = (n\varphi(h)(n'), hh').$$

Proposition 4.3.4. If K is a degree-12 Galois number field containing a quartic cyclic number field k, then the Galois group of K is a cyclic or dicyclic group of order 12.

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$, and let $H = \mathrm{Gal}(K/k)$, which has order 3. We have

$$G/H \simeq \mathrm{Gal}(k/\mathbb{Q}) = C_4,$$

and by the Schur-Zassenhaus theorem, we obtain

$$G = H \rtimes G/H \simeq C_3 \rtimes C_4.$$

Let g and h be generators of C_3 and C_4 respectively. Since C_3 has two possible automorphisms, the trivial one and the one given by $g \mapsto g^2$, the group homomorphisms in $\mathrm{Hom}(C_4, \mathrm{Aut}(C_3))$ are

$$\begin{aligned} \varphi_1 : C_4 &\to \mathrm{Aut}(C_3) \\ h &\mapsto (g \mapsto g), \end{aligned} \qquad \text{and} \qquad \begin{aligned} \varphi_2 : C_4 &\to \mathrm{Aut}(C_3) \\ h &\mapsto (g \mapsto g^2). \end{aligned}$$

We obtain that the semidirect product of C_4 and C_3 with respect to φ_1 is actually the direct product, and thus a cyclic group of order 12.

Consider now the semidirect product of C_4 and C_3 with respect to φ_2. Let $s = (g, h^2) \in C_3 \times C_4$ and $t = (1, h) \in C_3 \times C_4$. Note that $s^2 = (g^2, 1)$ has order 3 and t has order 4. Moreover they satisfy

$$s^3 = (g, h^2)(g, h^2)(g, h^2) = (g^2, 1)(g, h^2) = (1, h^2) = (1, h)(1, h) = t^2,$$

thus we obtain $s^6 = t^4 = 1$; and also

$$sts = (g, h^2)(1, h)(g, h^2) = (g, h^3)(g, h^2) = (1, h) = t.$$

We conclude that the semidirect product of C_4 and C_3 with respect to φ_2 is a dicyclic group of order 12. □

As we proved in Proposition 3.3.1, the Jacobians of CPQ curves have 3-CM-type $\mathfrak{Z} = (\mathbb{Q}(\zeta_5), (\phi_1, \phi_2), (3, 2), (0, 1))$, where $\phi_k : K \to \mathbb{C}$ maps ζ_5 to $z_5^k = \exp(2\pi ik/5)$. This has to be taken into account when considering possible CM-types for the Jacobian of a CPQ curve, since it introduces some restrictions.

Definition 4.3.5. Let k be a proper CM-subfield of a CM-field K. We say that a CM-type (K, Φ) *restricts to* an m-CM-type (k, Ψ) if the fields satisfy $m = [K : k]$ and for every $\psi \in \mathrm{Hom}(k, \mathbb{C})$ we have

$$\mathrm{mult}_\Psi(\psi) = \#\{\phi \in \Phi : \phi|_k = \psi\}.$$

Definition 4.3.6. We say that a CM-type (K, Φ) is *CPQ-compatible* if K is a degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$ such that Φ restricts to the m-CM-type $\mathfrak{Z}$ on the subfield $\mathbb{Q}(\zeta_5) \subseteq K$.

Corollary 4.3.7. If K Galois over $\mathbb{Q}$ and (K, Φ) is a CPQ-compatible CM-type, then the CM-type Φ is primitive.

Proof. If (K, Φ) is a CPQ-compatible CM-type, then K contains a fifth root of unity $\zeta_5 \in K$. It follows that the subfield $k = \mathbb{Q}(\zeta_5) \subseteq K$ is a cyclic quartic number field and since by assumption K is Galois over $\mathbb{Q}$, it follows that it is cyclic or dicyclic. In particular, in either case the only proper CM-subfield of K is $k = \mathbb{Q}(\zeta_5)$, see Figures 4.1 and 4.2. If Φ was induced, its restriction to k without multiplicity would be a CM-type of k. However, since (K, Φ) is CPQ-compatible, the restriction of Φ to k is the 3-CM-type $\mathfrak{Z}$, which is not a CM-type when considered without multiplicity. □

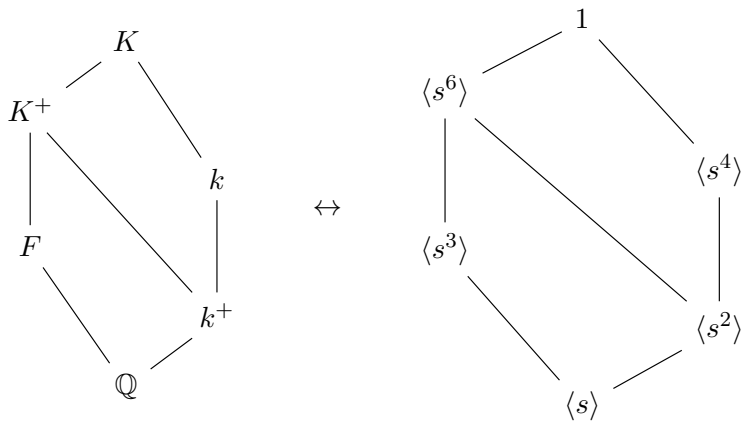


Figure 4.1: Lattices of subfields and subgroups for a cyclic field K of degree 12.

4.3.1 Sufficient condition for CM class number one

Let K be a CM-field with maximal totally real subfield K^+. In this section we give a sufficient condition for a CPQ-compatible CM-type (K, Φ) to have CM class number one. We denote the *class number* of K by h_K and define its *relative class number* $h_K^* := h_K/h_{K^+}$.

We will prove the following result.

Proposition 4.3.8. Let K be a Galois degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be its maximal totally real subfield and let Φ be a primitive CM-type. Let t_K be the number of primes in K^+ that ramify in K.

If the relative class number of K is $h_K^* = 2^{t_K-1}$, then K has CM class number one.

To prove this proposition we start with a result by Kılıçer that given a CM-field K with group of roots of unity W_K and *Hasse unit index* $Q_K := [\mathcal{O}_K^\times : W_K\mathcal{O}_{K^+}^\times] = 1$, writes the relative class number h_K^* in terms of t_K and the index $[I_K : I_K^H P_K]$ for $H = \mathrm{Gal}(K/K^+)$. Then we prove that this applies to our case because our CM-fields have $Q_K = 1$, and finally we prove that if we have $I_K = I_K^H P_K$, then the CM-field has CM class number one.

Lemma 4.3.9 (Lemma 2.2.2 in Kılıçer [12])**.** Let K be a CM-field with maximal totally real subfield K^+, and let t_K be the number of primes in K^+ that ramify in K. If the Hasse unit index Q_K of K is one, then we have

$$h_K^* = 2^{t_K-1}[I_K : I_K^H P_K].$$

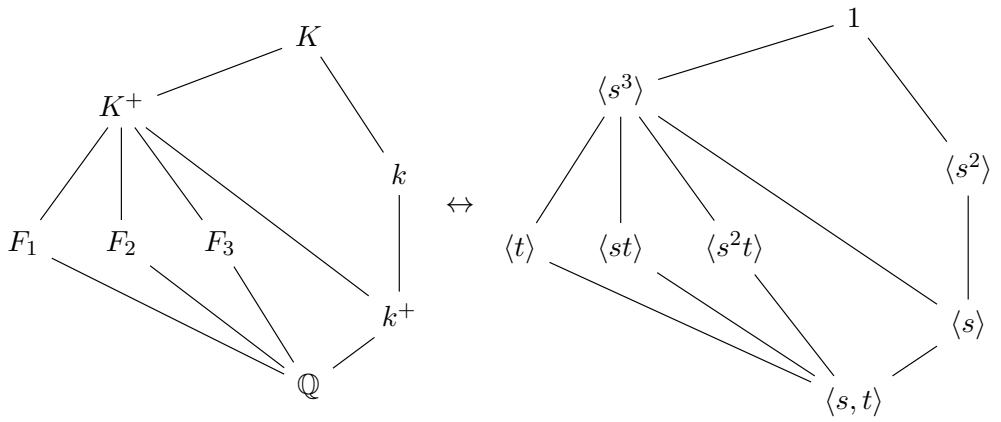


Figure 4.2: Lattices of subfields and subgroups for a dicyclic field K of degree 12.

□

Lemma 4.3.10. Let K be a degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be its maximal totally real subfield and let t_K be the number of primes in K^+ that ramify in K. The relative class number of K is

$$h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K].$$

Proof. Louboutin, Okazaki and Olivier [22] state in Theorem 5(i) that two CM-fields $k \subseteq K$ for which $[K : k]$ is odd have the same Hasse unit index.

In the case at hand, we have by assumption $\mathbb{Q}(\zeta_5) \subseteq K$ with $[K : \mathbb{Q}(\zeta_5)] = 3$, and thus we obtain $Q_K = Q_{\mathbb{Q}(\zeta_5)}$. One computes that the Hasse unit index for $\mathbb{Q}(\zeta_5)$ is $Q_{\mathbb{Q}(\zeta_5)} = 1$. Then the result follows from Lemma 4.3.9. □

Proof of Proposition 4.3.8. Since K is Galois over $\mathbb{Q}$ and the CM-type is primitive, we identify the CM-field K with its reflex field K^r via an isomorphism and assume $h_K^* = 2^{t_K - 1}$. By Lemma 4.3.10 we have that $I_K = I_K^H P_K$.

For any $\mathfrak{b} \in I_{K^+}$ we have $N_{\Phi^r}(\mathfrak{b}) = (N_{K^+/\mathbb{Q}}(\mathfrak{b}))$, where $N_{K^+/\mathbb{Q}}(\mathfrak{b}) \in \mathbb{Q}^\times$, hence we obtain the inclusion $I_{K^+} P_K \subseteq I_0(\Phi^r)$. Considering the exact sequence

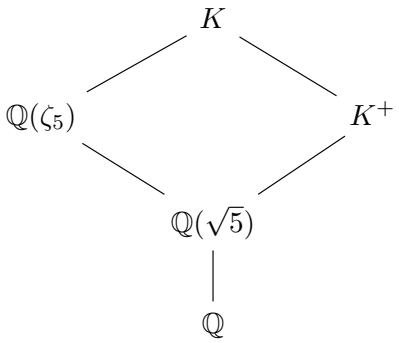
$$1 \to I_{K^+} \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } K^+} \mathbb{Z}/e_{K/K^+}(\mathfrak{p})\mathbb{Z} \to 1$$

we see that the elements in I_K^H / I_{K^+} are represented by the products of primes in K that are ramified in K/K^+. For any such prime $\mathfrak{P}$, let $\mathfrak{p} = \mathfrak{P} \cap K^+$ and

$p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Q}$. We obtain

$$N_{\Phi^r}(\mathfrak{P})^2 = N_{\Phi^r}(\mathfrak{p}\mathcal{O}_K) = N_{K^+/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K, \tag{4.1}$$

where $N_{K^+/\mathbb{Q}}(\mathfrak{p}) = p^{f_{K^+/\mathbb{Q}}(\mathfrak{p})}$. We have the subfield lattice



hence the rational prime p over which $\mathfrak{P}$ lies is ramified in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ (see also Proposition 4.8(ii) in [20, II]), so we conclude that $p = 5$ and by (4.1) we get

$$N_{\Phi^r}(\mathfrak{P}) = \sqrt{N_{K^+/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K} = (\pi), \text{ where } \pi = \begin{cases} \sqrt{5} & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 1, \\ 5 & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 2, \\ 5\sqrt{5} & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 3, \\ 5^3 & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 6, \end{cases}$$

where indeed in all cases we have $N_{K/\mathbb{Q}}(\mathfrak{P}) = \pi\overline{\pi}$. We conclude

$$I_K = I_K^H P_K \subseteq I_0(\Phi^r)$$

and the statement follows. □

In the following sections we prove the converse result for the different Galois group possibilities.

4.3.2 Cyclic degree-12 CM-fields

Throughout this section, we assume K to be a cyclic degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$ and denote its maximal totally real subfield by K^+.

We will prove that if K has CM class number one, then its relative class number h_K^* is $2^{t_K - 1}$. To do so we show that there is a unique CPQ-compatible CM-type up to the choice of an isomorphism between K and its reflex field K^r. That way we can use a concrete CM-type to prove that we have $I_K = I_K^H P_K$ using the type norm (see Definition 4.1.5).

Proposition 4.3.11. Let (K, Φ) be a cyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$ and let s be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that maps ζ_5 to ζ_5^2. There is an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that if we identify K with its reflex field K^r via σ, then Φ is $\{\mathrm{id}, s, s^3, s^4, s^5, s^8\}$. The reflex CM-type Φ^r is $\{\mathrm{id}, s^4, s^7, s^8, s^9, s^{11}\}$.

Proof. Let s be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that satisfies $s(\zeta_5) = \zeta_5^2$. The image of ζ_5 by the k-th power of s is $\zeta_5^{2^k}$ and thus it only depends on the class of k modulo 4.

If we consider an embedding $\sigma : K \to \mathbb{C}$ that satisfies $\sigma(\zeta_5) = z_5$, then there is a set $N \subseteq \mathbb{Z}/12\mathbb{Z}$ such that the CM-type consists of embeddings of the form $\sigma \circ s^k$ for $k \in N$. Since Φ restricts to the 3-CM-type $\mathfrak{Z}$, the subset N contains all $k \in \mathbb{Z}/12\mathbb{Z}$ that satisfy $k \equiv 0 \pmod 4$, one that satisfies $k \equiv 3 \pmod 4$ and two that satisfy $k \equiv 1 \pmod 4$.

Moreover, by definition, the CM-type Φ does not contain a complex conjugate pair, so the value $k \in N$ with $k \equiv 3 \pmod 4$ determines the those with $k \equiv 1 \pmod 4$. Therefore there are three possible index sets:

$$N_i = \{0, 4, 8, 3 + 4i, 1 + 4i, 5 + 4i\}, \quad i \in \{0, 1, 2\}.$$

It follows that, if we identify K with its reflex field K^r with the embedding $\sigma \circ s^{-4i}$, then we get Φ as in the statement of the proposition. Finally, since K is normal and Φ is primitive, the reflex CM-type is therefore $\Phi^r = \{\mathrm{id}, s^4, s^7, s^8, s^9, s^{11}\}$. □

Notation 4.3.12. For an arbitrary field F, an ideal $\mathfrak{b} \subseteq F$ and g an automorphism of F, we denote by ${}^g\mathfrak{b}$ the image by g of $\mathfrak{b}$, so we have ${}^{gr}\mathfrak{b} = {}^g({}^r\mathfrak{b})$. We extend this notation to the group ring $\mathbb{Z}[\mathrm{Aut}(F)]$.

Proposition 4.3.13. Let (K, Φ) be a cyclic CPQ-compatible CM-type, let K^+ be the maximal totally real subfield of K and let t_K be the number of primes in K^+ that ramify in K. If K has CM class number one, then the relative class number of K is $h_K^* = 2^{t_K - 1}$.

Proof. Let (K, Φ) be a cyclic CPQ-compatible CM-type. It follows from Lemma 4.3.10 that the relative class number is $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$, so we only need to prove $[I_K : I_K^H P_K] = 1$ when K has CM class number one, that is, when we have $I_0(\Phi^r) = I_{K^r}$.

We will start by proving that for any $\mathfrak{b} \in I_K$ the fractional ideal ${}^{1-s^6}\mathfrak{b}$ is principal and generated by an element $\alpha \in K^\times$ that satisfies $\alpha\overline{\alpha} = 1$. Then we will use Hilbert's Theorem 90 to prove that the ideal $\mathfrak{b}$ is in $I_K^H P_K$.

Let $\zeta_5 \in K$ be the primitive fifth root of unity for which the CM-type (K, Φ) is CPQ-compatible, and let $k = \mathbb{Q}(\zeta_5)$. Identify K with its reflex field K^r via

the embedding given in Proposition 4.3.11, so we have $\Phi = \{\mathrm{id}, s, s^3, s^4, s^5, s^8\}$ for s a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that maps ζ_5 to ζ_5^2. For any $\mathfrak{b} \in I_K$ we can check by writing it out that we obtain

$$N_{\Phi^r}({}^{-1+s+s^5-s^6}\mathfrak{b})/N_{K/k}({}^{s-s^3}\mathfrak{b}) = {}^{1-s^6}\mathfrak{b}.$$

By assumption we have $I_0(\Phi^r) = I_{K^r}$, so the ideal $N_{\Phi^r}({}^{-1+s+s^5-s^6}\mathfrak{b})$ is generated by an element $\beta \in K^\times$ with $\beta\overline{\beta} = N_{K/\mathbb{Q}}({}^{-1+s+s^5-s^6}\mathfrak{b}) = 1$.

The ideal $N_{K/k}({}^{s-s^3}\mathfrak{b}) \in I_k$ is also principal, since it is a fractional ideal of the class number one field k. Choose a generator $\gamma \in k^\times$. By cancellation, it satisfies

$$(\gamma\overline{\gamma}) = N_{K/k}({}^{s-s^3}\mathfrak{b})\overline{N_{K/k}({}^{s-s^3}\mathfrak{b})} = (1).$$

But since we have seen that all totally positive units in k^+ are norms of elements of $\mathcal{O}_k^\times$ (see Lemma 3.4.14), we change γ so that it satisfies $\gamma\overline{\gamma} = 1$.

Altogether we have that ${}^{1-s^6}\mathfrak{b}$ is a principal ideal generated by an element $\alpha = (\beta/\gamma)$ such that $\alpha\overline{\alpha} = 1$. It follows from Hilbert's Theorem 90 [10] that there exists an element $\delta \in K^\times$ with $\alpha = \overline{\delta}\delta^{-1}$. In consequence, we obtain $\delta\mathfrak{b} = \overline{\delta\mathfrak{b}} \in I_K^H$ so we write $\mathfrak{b} = \overline{\delta\mathfrak{b}}\left(\frac{1}{\delta}\right) \in I_K^H P_K$ and thus we obtain the equality $I_K = I_K^H P_K$. □

4.3.3 Dicyclic degree-12 CM-fields

In this section we consider the remaining case, that is, we assume that K is a degree-12 CM-field containing a fifth root of unity and whose Galois group is a dicyclic group of order 12. In particular there are elements $s, t \in \mathrm{Gal}(K/\mathbb{Q})$ that satisfy $\mathrm{Gal}(K/\mathbb{Q}) = \langle s, t : s^6 = 1, s^3 = t^2, sts = t\rangle$.

We will prove also in this case that if the field K has relative class number $h_K^* = 2^{t_K - 1}$, then it also has CM class number one.

To do so we follow the same strategy as in Section 4.3.2. First we determine the unique CPQ-compatible CM-type Φ up to the choice of an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and then we use that to prove $I_K = I_K^H P_K$ using the type norm of the reflex type Φ^r.

Lemma 4.3.14. If (K, Φ) is a dicyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$, then there exist generators s and t of $\mathrm{Gal}(K/\mathbb{Q})$ that map ζ_5 to ζ_5^4 and ζ_5^2 respectively, and satisfy the relations $ts = s^5t$, $t^2 = s^3$ and $s^6 = 1$.

Proof. Let $s, t \in \mathrm{Gal}(K/\mathbb{Q})$ satisfy $\mathrm{Gal}(K/\mathbb{Q}) = \langle s, t : s^6 = 1, s^3 = t^2, sts = t\rangle$.

The automorphism s maps ζ_5 to ζ_5^4 because it has order 2 in $\langle s, t\rangle/\langle s^2\rangle$ (see Figure 4.2) and the map given by $\zeta_5 \mapsto \zeta_5^4$ is the only order-2 element in $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.

Analogously, the automorphism t has order 4 in $\langle s,t\rangle/\langle s^2\rangle$ so, changing t to t^{-1} if necessary, we get that it maps ζ_5 to ζ_5^2. □

Proposition 4.3.15. Let (K,Φ) be a dicyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$ and let s and t be generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. Then there is an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that if we identify K with its reflex field K^r via σ, then Φ is $\{\mathrm{id}, s^2, s^4, t, st, s^2t\}$. Moreover, the reflex CM-type Φ^r is $\{\mathrm{id}, s^2, s^4, s^3t, s^4t, s^5t\}$.

Proof. Let s and t be generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. We can write the Galois group of K as

$$\mathrm{Gal}(K/\mathbb{Q}) = \{s^it^j : 0 \le i \le 5, j \in \{0,1\}\}$$

together with the relations $ts = s^5t$, $t^2 = s^3$ and $s^6 = 1$.

If we consider an embedding $\sigma : K \to \mathbb{C}$ that satisfies $\sigma(\zeta_5) = z_5$, then there exists a subset $P \subseteq \mathrm{Gal}(K/\mathbb{Q})$ such that the CM-type consists of embeddings of the form $\sigma \circ s^it^j$ for $s^it^j \in P$. Since Φ restricts to the 3-CM-type $\mathfrak{Z}$, the subset P contains all automorphism that map ζ_5 to itself, one that maps ζ_5 to ζ_5^3 and two that map ζ_5 to ζ_5^2.

Moreover, by definition, the CM-type does not contain a complex conjugate pair, so the automorphism in P mapping ζ_5 to ζ_5^3 determines those mapping ζ_5 to ζ_5^2.

Since the group $\langle s^2\rangle$ fixes $\mathbb{Q}(\zeta_5)$ (see Figure 4.2) we get $\langle s^2\rangle \subseteq P$. Furthermore, the automorphism t maps ζ_5 to ζ_5^2 and s^3 is the complex conjugation in K, hence only one automorphism in the subgroup $\langle s^2\rangle s^3t = \langle s^2\rangle st$ is in P, and it determines the remaining two automorphisms.

Altogether, we obtain that there are 3 possible subsets $P \subseteq \mathrm{Gal}(K/\mathbb{Q})$:

$$P_i = \{\mathrm{id}, s^2, s^4, s^{2i}t, s^{1+2i}t, s^{2+2i}t\}, \quad i \in \{0,1,2\}.$$

It follows that, if we identify K with its reflex field K^r via the embedding $\sigma \circ s^{-2i}$, then we get that Φ is P_0. Lastly, since K is normal and Φ is primitive by Remark 4.3.7, we can compute the reflex CM-type $\Phi^r = \{\mathrm{id}, s^2, s^4, s^3t, s^4t, s^5t\}$. □

Proposition 4.3.16. Let (K,Φ) be a dicyclic CPQ-compatible CM-type, let K^+ be its maximal totally real subfield and let t_K be the number of primes in K^+ that ramify in K. If K has CM class number one, then the relative class number of K is $h_K^* = 2^{t_K-1}$.

Proof. Let (K,Φ) be a dicyclic CPQ-compatible CM-type. It follows from Lemma 4.3.10 that the relative class number is $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$, so

we only need to prove $[I_K : I_K^H P_K] = 1$ when the CM-field K has CM class number one, that is, when we have $I_0(\Phi^r) = I_{K^r}$.

We will start by proving that for any $\mathfrak{b} \in I_K$ the fractional ideal ${}^{1-s^3}\mathfrak{b}$ is principal and generated by an element $\alpha \in K^\times$ that satisfies $\alpha\overline{\alpha} = 1$. Then we can use Hilbert's Theorem 90 to prove that the ideal $\mathfrak{b}$ is in $I_K^H P_K$.

Let $\zeta_5 \in K$ be the primitive fifth root of unity for which (K, Φ) is CPQ-compatible, and let $k = \mathbb{Q}(\zeta_5)$. Identify K with its reflex field K^r via the embedding given in Proposition 4.3.15, so we have $\Phi = \{\mathrm{id}, s^2, s^4, t, st, s^2t\}$ for s and t generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. For any ideal $\mathfrak{b} \in I_K$ we can check by writing it out that we obtain

$$N_{\Phi^r}({}^{t-s^5t}\mathfrak{b})/N_{K/k}({}^{t-st}\mathfrak{b}) = {}^{1-s^3}\mathfrak{b}.$$

By an argument analogous to the one in the proof of Proposition 4.3.13, there exists $\alpha \in K^\times$ that satisfies ${}^{1-s^3}\mathfrak{b} = (\alpha)$ and $\alpha\overline{\alpha} = 1$, hence, by Hilbert's Theorem 90 [10], there exists an element $\delta \in K^\times$ with $\alpha = \overline{\delta}\delta^{-1}$. In consequence, $\mathfrak{b} = \overline{\delta\mathfrak{b}}\left(\frac{1}{\delta}\right) \in I_K^H P_K$ and thus $I_K = I_K^H P_K$. □

4.3.4 Final results

The following theorem summarizes all the results above.

Theorem 4.3.17. Let (K, Φ) be a Galois CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be the maximal totally real subfield of K and let Φ be a primitive CM-type. Let t_K be the number of primes in K^+ that ramify in K. The relative class number h_K^* of K is 2^{t_K-1} if and only if K has CM class number one.

Proof. One implication corresponds to Proposition 4.3.8. For the converse, note that by Proposition 4.3.4 the field K has a cyclic or dicyclic Galois group. Then, Propositions 4.3.13 and 4.3.16 are enough to prove the statement. □

With this result we can now prove Theorem 4.3.1.

Proof of Theorem 4.3.1. By Theorem 4.3.17, the field K has CM class number one if and only if its relative class number is $h_K^* = 2^{t_K-1}$ where t_K is the number of primes in the maximal totally real subfield K^+ that ramify in K. But since $\sqrt{5}$ is the only ramified prime in $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$, all ramified primes in K/K^+ lie above 5 (see Proposition 4.8(ii) in [20, II]) and we get $t_K \leq 3$, hence we obtain $h_K^* \leq 4$.

Recall that by Proposition 4.3.4 the field K has a cyclic or dicyclic Galois group, so we look at each case separately.

On the one hand, Chang and Kwon [5] list all imaginary cyclic number fields of even degree with relative class number (with respect to their maximal totally

real subfields) less than or equal to 4, see [5, Table I]. In particular, we are interested in those that are degree-12 CM-fields containing a quartic field with conductor 5, that is, containing $\mathbb{Q}(\zeta_5)$, which are the fields (1)–(3) in Table 4.2.

On the other hand, Louboutin and Park [23] prove that the minimum relative class number of dicyclic CM-fields is 4, and list all such CM-fields (see Theorem 1 in [23]). In particular, we are again interested in those degree-12 CM-fields containing a quartic field with conductor 5, that is, containing $\mathbb{Q}(\zeta_5)$, which is exactly case (4) in Table 4.2. □

Using the methods due to Kılıçer [12, Chapter 4] and Theorem 3.5.3, one can prove that if Conjecture 3.5.1 holds, then for every field K in Table 4.2 there exists a unique CPQ curve with maximal CM by K and defined over $\mathbb{Q}$.

The curves in Section 2.3 are heuristic models for those curves, which we obtained by applying Algorithm 2.2.6 to the period matrices obtained through Van Wamelen's method, see Section 4.1 for details.

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. – Cited on pages 7, 8, 99, 100, 101, and 102.

[2] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004. – Cited on pages 10, 13, 15, 23, 24, 41, 49, 51, 52, 53, 54, 55, and 61.

[3] 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). – Cited on page 44.

[4] C.L. Chai, B. Conrad, and F. Oort. *Complex Multiplication and Lifting Problems*. Mathematical Surveys and Monographs. American Mathematical Society, 2013. – Cited on page 77.

[5] K.-Y. Chang and S.-H. Kwon. Class number problem for imaginary cyclic number fields. *J. Number Theory*, 73(2):318–338, 1998. – Cited on pages 89 and 90.

[6] A. Clebsch. Zur Theorie der binären algebraischen Formen. *Math. Ann.*, 3(2):265–267, 1870. – Cited on page 47.

[7] 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. – Cited on page 46.

[8] B. Deconinck and M.S. Patterson. Computing with plane algebraic curves and riemann surfaces: The algorithms of the maple package "algcurves". In Alexander I. Bobenko and Christian Klein, editors, *Computational Approach to Riemann Surfaces*, pages 67–123. Springer Berlin Heidelberg, 2011. – Cited on pages 37, 38, and 73.

[9] J. Guàrdia. On the Torelli problem and Jacobian Nullwerte in genus three. *Michigan Math. J.*, 60(1):51–65, 2011. – Cited on pages 7, 99, and 101.

[10] D. Hilbert. *The Theory of Algebraic Number Fields*. Springer Berlin Heidelberg, 1998. – Cited on pages 87 and 89.

[11] R.-P. Holzapfel. *The ball and some Hilbert problems*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1995. Appendix I by J. Estrada Sarlabous. – Cited on pages 9, 29, and 30.

[12] P. Kılıçer. *The CM class number one problem for curves*. PhD thesis, Leiden University, 2016. – Cited on pages 8, 75, 79, 80, 83, 90, 100, and 102.

[13] P. Kilicer, 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. – Cited on pages 8, 100, and 102.

[14] P. Kılıçer and M. Streng. LLL reduction of period matrices of genus 3, 2016. Available at `https://bitbucket.org/pkilicer/period-matrices-for-genus-3-cm-curves/`. – Cited on page 32.

[15] P. Kilicer and M. Streng. The CM class number one problem for curves of genus 2. *arXiv:1511.04869*, 2016. – Cited on page 75.

[16] K. Koike and A. Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518, 2005. – Cited on pages 7, 8, 9, 21, 23, 26, 27, 29, 30, 33, 99, 100, 101, and 102.

[17] H. Labrande. *Explicit computation of the Abel-Jacobi map and its inverse*. PhD thesis, Université de Lorraine, 2016. – Cited on page 32.

[18] H. Labrande and E. Thomé. Computing theta functions in quasi-linear time in genus two and above. *LMS J. Comput. Math.*, 19(suppl. A):163–177, 2016. – Cited on page 32.

[19] S. Lang. *Complex Multiplication*. Grundleheren der math. Wiss, 255. Springer, 1983. – Cited on pages 10, 11, and 76.

[20] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994. – Cited on pages 85 and 89.

[21] J.-C. Lario and A. Somoza. A note on Picard curves of CM-type. *arXiv:1611.02582*, 2016. – Cited on pages 7, 8, 10, 99, 100, 101, and 102.

[22] S. Louboutin, R. Okazaki, and M. Olivier. The class number one problem for some non-abelian normal CM-fields. *Trans. Amer. Math. Soc.*, 349(9):3657–3678, 1997. – Cited on page 84.

[23] S. Louboutin and Y.-H. Park. Class number problems for dicyclic CM-fields. *Publ. Math. Debrecen*, 57(3-4):283–295, 2000. – Cited on page 90.

[24] J. S. Milne. Abelian varieties. In Gary Cornell and Joseph H. Silverman, editors, *Arithmetic Geometry*, pages 103–150. Springer New York, 1986. – Cited on page 10.

[25] J. S. Milne. Jacobian varieties. In Gary Cornell and Joseph H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer New York, 1986. – Cited on pages 10 and 14.

[26] J.S. Milne. Algebraic geometry. Version 6.02, 2017. Available at `www.jmilne.org/math/`. – Cited on page 74.

[27] M.B. Monagan, K.O. Geddes, K. M. Heal, G. Labahn, S.M. Vorkoetter, J. McCarron, and P. DeMarco. *Maple 2016 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005-2016. – Cited on page 73.

[28] B. Moonen and F. Oort. The torelli locus and special subvarieties. In G. Farkas and I. Morrisson, editors, *Handbook of Moduli*, volume 2, pages 549–594. International Press, 2013. – Cited on page 71.

[29] D. Mumford. *Tata lectures on theta. I.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. – Cited on pages 16 and 19.

[30] D. Mumford. *Abelian Varieties*. Studies in mathematics. Hindustan Book Agency, 2008. – Cited on pages 10 and 11.

[31] J. Noordsij. Master's thesis, Leiden University, the Netherlands, 2008. To appear at `https://www.universiteitleiden.nl/en/science/mathematics/education/theses`. – Cited on page 47.

[32] J. Noordsij. Invariants and reconstruction of quintic binary forms, 2018. See SageMath trac tickets at `https://trac.sagemath.org/query?reporter=jnoordsij`. – Cited on page 47.

[33] F. Oort and K. Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:377–381, 1973. – Cited on page 29.

[34] Y.-H. Park and S.-H. Kwon. Determination of all imaginary abelian sextic number fields with class number ≤ 11. *Acta Arith.*, 82(1):27–43, 1997. – Cited on page 80.

[35] E. Picard. Sur des fonctions de deux variables indépendantes analogues aux fonctions modulaires. *Acta Math.*, 2(1):114–135, 1883. – Cited on page 23.

[36] S. Roman. *Fundamentals of Group Theory: An Advanced Approach*. SpringerLink : Bücher. Birkhäuser Boston, 2011. – Cited on page 80.

[37] G. Rosenhain, H. Weber, and A. Witting. *Abhandlung über die functionen zweier variabler mit vier perioden: welche die inversen sind der ultraelliptischen integrale erster klasse*. Ostwalds Klassiker der exakten Wissenschaften. W. Engelmann, 1895. – Cited on pages 7, 99, and 101.

[38] H. Shiga. On the representation of the Picard modular function by θ constants. I, II. *Publ. Res. Inst. Math. Sci.*, 24(3):311–360, 1988. – Cited on page 23.

[39] G. Shimura. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)*, 78:149–192, 1963. – Cited on pages 8, 49, 51, 55, 56, 62, 100, and 102.

[40] G. Shimura. Arithmetic of unitary groups. *Ann. of Math. (2)*, 79:369–409, 1964. – Cited on pages 63, 64, 66, 67, and 68.

[41] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Kanô memorial lectures. Princeton University Press, 1971. – Cited on page 78.

[42] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. – Cited on pages 75 and 76.

[43] G. Shimura and Y. Taniyama. *Complex multiplication of Abelian varieties and its applications to number theory*. Publications of the Mathematical Society of Japan. Mathematical Society of Japan, 1961. – Cited on page 78.

[44] C.L. Siegel. *Topics in complex function theory. Vol. II*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1988. – Cited on pages 17 and 37.

[45] A. Somoza Henares. Inverse Jacobian algorithms for Picard and CPQ curves, 2018. Available at `https://github.com/anna-somoza/inverse-jacobian-alg/`. – Cited on page 30.

[46] A. Somoza Henares. Scripts for *Inverse Jacobian and related topics for certain superelliptic curves*, 2018. Available at `https://github.com/anna-somoza/scripts-thesis/`. – Cited on page 70.

[47] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. – Cited on pages 8, 100, and 102.

[48] 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. – Cited on pages 7, 99, and 101.

[49] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018. `http://www.sagemath.org`. – Cited on pages 27, 66, and 69.

[50] J. Thomae. Beitrag zur Bestimmung von $\vartheta(0, 0, \ldots 0)$ durch die Klassenmoduln algebraischer Functionen. *J. Reine Angew. Math.*, 71:201–222, 1870. – Cited on pages 7, 99, and 101.

[51] P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999. – Cited on pages 8, 77, 100, and 102.

[52] H. Weber. Theorie der abel'schen functionen vom geschlecht 3. 1876. – Cited on pages 7, 8, 99, 100, 101, and 102.

[53] A. Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001. – Cited on pages 7, 8, 99, 100, 101, and 102.

Index

Abel-Jacobi map, **14**, 15
abelian variety, 10
    absolutely simple, 10
    Picard group, 10
analytic representation, 12

CM, *see* complex multiplication
CM class number one, 78
    CPQ case, **81**, 89
    Picard case, 79
CM-field, 50
CM-type, 75
    CPQ-compatible, 82
    generalized, *see* m-CM-type
    induced, 75
    primitive, **76**
    restricts to an m-CM-type, 82
    type norm, 76
complex torus polarizable 11
CPQ curve, *see* cyclic plane quintic curve
cyclic plane quintic curve, **35**
    basis of regular differentials, 38
    branch points, **35**, 42
    invariants, 47
    Legendre-Rosenhain equation, 35
    with maximal CM, **47**, 77

dicyclic group, 81
dual variety, 11

field of moduli, 78

homomorphism
    of complex tori, 12
    of abelian variety, 10

inverse Jacobian algorithm, 15
    for CPQ curves, 45
    for Picard curves, 27
inverse Jacobian problem, 7
isogeny, 10
isomorphism
    of polarized abelian varieties, 11
      with m-CM-type, **50**, 62

Jacobian of a curve, 7, **14**, 15
    over $\mathbb{C}$, 15

m-CM-type, 50

non-special divisor, *see* special divisor

$\mathcal{O}_K$-lattice, 63
    ideal index, 64
    polarized, 63
    principally polarized, **63**
    S-maximal, 67
    S-norm, 67
    S-scale, 67
    trace dual, 63

period matrix, 12
    big, 12
Picard curve, 7, **9**
    affine branch points, **9**, 18, 25

invariants, 33
Legendre-Rosenhain equation, 9
with maximal CM, **33**, 77
polarization, 11
principal, 11
polarized abelian variety, *see also* polarization
over $\mathbb{C}$, 11
with m-CM-type, 50
with CM, 76

rational representation, 12
reflex
CM-type, 76
field, 76
relative class number, 83
Riemann
constant, 16
form, 11
associated hermitian form, 11
of a principal polarization, 11
with respect to bases, 12
theta constant, 18
implementation, 30
quasi-periodicity, 19
symmetry, 19
theta function, 16
with characteristic, 18
Vanishing Theorem, 16
Riemann-Schottky problem, 7, **14**, 71
Rosati involution, 11

signature
of a hermitian matrix, 66
of an antihermitian matrix, 51
special divisor, 17
superelliptic curve, 7
basis of regular differentials, 37
$(1-\rho_*)$-torsion, 40
symplectic
basis, 12
group, 13
matrix, *see* symplectic group

Torelli locus, 71
open, 71
Torelli map, 14
Torelli's Theorem, 14

Samenvatting

Voor elke *elliptische kromme* E over $\mathbb{C}$ bestaat er een *rooster* $\Lambda \subseteq \mathbb{C}$, zodanig dat de groep $E(\mathbb{C})$ van complexe punten op E isomorf is met de complex analytische groep $\mathbb{C}/\Lambda$. Dit verband tussen elliptische krommen en één-dimensionale complexe tori heet de Uniformisatiestelling, en de constructie in omgekeerde richting (van roosters naar krommen) kan expliciet worden beschreven met de *Weierstrass $\wp$-functie*, zijn afgeleide, en de *Eisenstein-reeksen*.

Algemener kennen we aan een algebraïsche kromme C van geslacht g een *hoofdgepolariseerde abelse variëteit* $J(C)$ toe, de *Jacobiaan van C*. Over $\mathbb{C}$ is de Jacobiaan $J(C)$ isomorf met een g-dimensionale complexe torus $\mathbb{C}^g/\Lambda$ voor een rooster Λ van volledige rang in $\mathbb{C}^g$.

Dit bepaalt een afbeelding J van de verzameling M_g van isomorfieklassen van algebraïsche krommen van geslacht g naar de verzameling A_g van g-dimensionale hoofdgepolariseerde abelse variëteiten. We kunnen ons afvragen of er een expliciete inverse afbeelding bestaat, zoals het geval is voor elliptische krommen. Dit is het *inverse-Jacobiaan-probleem*.

Dit probleem is opgelost voor krommen van geslacht 2 [37, 50] en geslacht 3 [1, 9, 16, 21, 48, 52, 53]. Voor geslacht ≥ 4 is er echter de extra obstructie dat niet alle hoofdgepolariseerde abelse variëteiten Jacobianen van krommen zijn, dus om het inverse-Jacobiaan-probleem op te lossen moeten we in dit geval het beeld van M_g in A_g onder J bestuderen. Het beschrijven van $J(\mathsf{M}_g)$ staat bekend als het *Riemann-Schottky-probleem*.

In dit proefschrift behandelen we deze twee problemen voor twee families van *superelliptische krommen*, dat wil zeggen, krommen gegeven door $y^k = \prod_{i=1}^{l}(x - \alpha_i)$. We richten ons op de familie van *Picard-krommen*, met $(k, l) = (3, 4)$ en van geslacht 3, waarvoor we het inverse-Jacobiaan-probleem oplossen en de familie van *cyclische vlakke vijfdegraads krommen* (CPQ-krommen), met $(k, l) = (5, 5)$ en van geslacht 6, waarvoor we beide problemen oplossen.

In Hoofdstuk 1 introduceren we eerst achtergrondkennis over abelse varieteiten, Jacobianen van krommen en Riemann theta constanten. Daarna geven we een inverse-Jacobiaan-algoritme voor Picard-krommen. Merk op dat

Picard-krommen geslacht 3 hebben, en er dus geen obstructie voor het inverse-Jacobiaan-probleem is.

Picard-krommen zijn een speciaal geval van vlakke vierdegraads krommen, dus het inverse-Jacobiaan-probleem voor Picard-krommen kan worden opgelost met behulp van de formules voor vlakke vierdegraads krommen gegeven in [52], maar de beperking tot een kleinere familie van krommen zorgt ervoor dat we een efficiëntere oplossing voor deze familie kunnen geven.

Dit is oorspronkelijk gedaan door Koike en Weng in [16], maar hun uiteenzetting bevat een aantal fouten die we hier aankaarten en corrigeren. Dit hoofdstuk is gebaseerd op gezamenlijk werk met Joan-Carles Lario, zie ook [21].

In Hoofdstuk 2 geven we een inverse-Jacobiaan-algoritme voor CPQ-krommen. We volgen een strategie analoog aan die in Hoofdstuk 1 voor het geval van Picard-krommen.

In Hoofdstuk 3 pakken we het Riemann-Schottky-probleem voor CPQ-krommen aan, dat wil zeggen dat we de hoofdgepolariseerde abelse variëteiten die Jacobianen van CPQ-krommen zijn classificeren. Eerst gebruiken we Shimura's algemene vorm van de theorie van *complexe vermenigvuldiging*, zie [39], om te bestuderen hoe het bestaan van het automorfisme $(x, y) \mapsto (x, z_5 y)$ met $z_5 = \exp(2\pi i/5)$ van een CPQ-kromme de structuur van de Jacobiaan beïnvloedt. Vervolgens lossen we een klassengetal-één-probleem voor hogerdimensionale Hermitese roosters over $\mathbb{Z}[\zeta_5]$ op, wat cruciaal is voor het oplossen van het Riemann-Schottky-probleem voor CPQ-krommen.

Tot slot geven we in Hoofdstuk 4 een toepassing van bovenstaande algoritmes: het construeren van krommen waarvan de Jacobianen complexe vermenigvuldiging toestaan. Dit is eerder gedaan voor geslacht 2 [51, 47] en geslacht 3 [1, 13, 16, 21, 53]. Hier breiden we methoden van Kılıçer [12] uit om een complete lijst van CM-lichamen te bepalen waarvan de ringen van gehelen voorkomen als endomorfismering over $\mathbb{C}$ van de Jacobiaan van een CPQ-kromme over $\mathbb{Q}$.

In het bijzonder geeft dit ons de mogelijkheid om een lijst te geven met vermoedelijke modellen voor alle CPQ-krommen over $\mathbb{Q}$ waarvan de Jacobianen de maximale orde van een CM lichaam van graad 12 als endomorfismering over $\mathbb{C}$ hebben. Onze lijst bevat het juiste aantal krommen, die gedefinieerd zijn over $\mathbb{Q}$ en numeriek correct met hoge nauwkeurigheid.

Resumen

Dada una *curva elíptica* E sobre $\mathbb{C}$, existe una *red* $\Lambda \subseteq \mathbb{C}$ tal que el grupo $E(\mathbb{C})$ de puntos complejos en E es isomorfo al grupo analítico complejo $\mathbb{C}/\Lambda$. Esta connexión entre curvas elípticas y toros de dimensión 1 se conoce como el Teorema de la Uniformización de Riemann, y es posible encontrar de forma explícita la curva correspondiente a una cierta red mediante la *función $\wp$ de Weierstrass*, su derivada, y las *series de Eisenstein*.

De forma similar, dada una curva algebraica C de género g, podemos definir una *variedad abeliana principalmente polarizada* $J(C)$, la *Jacobiana de* C. Sobre $\mathbb{C}$, la Jacobiana $J(C)$ es isomórfa a un toro complejo g-dimensional $\mathbb{C}^g/\Lambda$ para una red Λ de rango completo en $\mathbb{C}^g$.

Esto determina una función J del conjunto M_g de clases de isomorfismo de curvas algebraicas de género g al conjunto A_g de variedades abelianas principalmente polarizadas de dimensión g, y nos preguntamos si existe una función inversa explícita, como en el caso de las curvas elípticas. Se trata del *problema de la Jacobiana inversa*.

Este problema ha sido resuelto para curvas de género 2 [37, 50] y género 3 [1, 9, 16, 21, 48, 52, 53]. Sin embargo, para género $g \geq 4$, tenemos el obstáculo añadido de que no todas las variedades abelianas principalmente polarizadas son Jacobianas de curvas, por lo que para resolver el problema de la Jacobiana inversa tenemos que estudiar la imagen vía J de M_g en A_g. El problema de describir $J(\mathsf{M}_g)$ se conoce como el *problema de Riemann-Schottky*.

En esta tesis tratamos estos dos problemas para dos familias de curvas superelípticas, es decir, curvas de la forma $y^k = \prod_{i=1}^{l}(x-\alpha_i)$. Nos centramos en la familia de curvas de Picard, con $(k,l) = (3,4)$ y género 3, donde solucionamos el problema de la Jacobiana inversa, y la família de las curvas cíclicas quínticas planas (curvas CPQ), con $(k,l) = (5,5)$ y género 6, para la que resolvemos ambos problemas.

En el Capítulo 1 introducimos algunos preliminares de variedades abelianas, Jacobianas de curvas y constantes teta de Riemann, y a continuación presentamos un algoritmo de Jacobiana inversa para las curvas de Picard. Dado que las curvas de Picard tienen género 3, no hay obstrucción al problema de la Jacobiana inversa.

Dado que las curvas de Picard son curvas cuárticas planas, el problema de la Jacobiana inversa se resolvería con las ideas para el problema de la Jacobiana inversa para cuárticas planas que encontramos en [52]. Sin embargo, concentrarnos en una familia más reducida de curvas nos permite presentar una solución más eficiente para la familia en cuestión.

Esto lo hicieron originalmente Koike y Weng en [16], pero su exposición presenta algunos errores que corregimos aquí. El capítulo está basado en una colaboración con Joan-Carles Lario, véase también [21].

En el Capítulo 2 presentamos un algoritmo de la Jacobiana inversa para las curvas CPQ. Seguimos una estrategia análoga a la del Capítulo 1 para el caso de curvas de Picard.

En el Capítulo 3 lidiamos con en el problema de Riemann-Schottky para curvas CPQ, es decir, caracterizamos las variedades abelianas principalmente polarizadas que son Jacobianas de curvas CPQ. Primero usamos una generalización de la teoría clásica de multiplicación compleja de Shimura [39] para estudiar cómo la existencia del automorfismo de curvas CPQ $(x, y) \mapsto (x, \exp(2\pi i/5)y)$ afecta la estructura de las Jacobianas. A continuación resolvemos un problema de número de clases 1 para redes hermíticas de dimensión superior sobre $\mathbb{Z}[\zeta_5]$.

Finalmente, en el Capítulo 4 presentamos una aplicación de los algoritmos anteriores: construir curvas cuyas Jacobianas tengan multiplicación compleja (CM). Esto se ha hecho anteriormente para género 2 [51, 47] y género 3 [1, 13, 16, 21, 53]. Aquí extendemos los métodos de Kılıçer [12] para determinar una lista completa de cuerpos CM cuyo anillo de enteros se da como el anillo de endomorfismos sobre $\mathbb{C}$ de la Jacobiana de una curva CPQ sobre $\mathbb{Q}$.

En particular, ésto nos permite listar modelos conjeturales para todas las curvas CPQ sobre $\mathbb{Q}$ cuyas Jacobianas tienen el orden maximal de un cuerpo CM de grado 12 como anillo de endomorfismos sobre $\mathbb{C}$. Nuestra lista contiene el número previsto de curvas, y éstas están definidas sobre $\mathbb{Q}$ y son numéricamente correctas hasta un cierto grado de precisión.

Acknowledgements

I would like to take this opportunity to thank all the people that have accompanied me during these years.

First and foremost, I would like to thank my supervisors.

Joan-Carles, I discovered what research means by your side, when in the early days of this project, with a different title and a different goal, we waited with excitement for the results of our computations only to get unexpected results over and over again. Little did we know back then that those weird results where the first hints of what this thesis would become. Thank you for infecting me with your enthusiasm and curiosity about mathematics.

Marco, thank you for your patience and guidance. You have taught me how to see the bigger picture mathematically, greatly influencing both my talks and the exposition of this same thesis. Your thoroughness and kindness has helped me grow both as a mathematician and as a person.

And to my promotor, Peter, thank you for always having your door open for me.

Thanks to all current and former members of the MI for welcoming me to Leiden and making the department such a lovely place to work. A special thank-you goes to Rosa, for the translation of the *Samenvatting*.

I would also like to thank Pili, my former officemate in Barcelona and friend, for making me realize that my feelings and worries during my studies were the norm, and not the exception. I look forward to our celebratory trip to Mexico after you graduate.

Thanks also to the members of the committee for your feedback on the thesis.

A la meva artista Vanessa, gràcies per fer possible aquesta portada i per tota la resta, que no sé posar per escrit.

A mis padres Manuel y Begoña y mi hermana Maite, gracias de todo corazón por apoyarme siempre en todo lo que hago, incluso cuando no lo entendéis.

Y por último, gracias Jose por los preciosos dibujos que llenan la portada, pero sobretodo por estar a mi lado a cada paso, incluso cuando el camino llevaba a un nuevo país, y por todos los pasos que están por venir.

Curriculum vitae

Anna Somoza Henares was born in L'Hospitalet del Llobregat on 10th December 1991.

In 2009 se obtained her secondary school diploma at Escola Mestral, in Sant Feliu del Llobregat. Afterwards, she started her Mathematics degree at Universitat Politècnica de Catalunya, Barcelona, and she obtained her diploma in 2013.

In 2014 she graduated from the Master in Applied Mathematics and Mathematical Engineering, also at Universitat Politècnica de Catalunya, after defending her masters' thesis *The Sato-Tate conjecture for a Picard curve with Complex Multiplication* under the supervision of Joan-Carles Lario.

In 2015 she started her PhD studies between Universitat Politècnica de Catalunya and Universiteit Leiden under the supervision of Joan-Carles Lario, Peter Stevenhagen and Marco Streng, which lead to the thesis you are now reading.

She has been working as a postdoc at Max Planck Instiute für Mathematik since September 2018.