Curves of genus 2 with real multiplication by a square root of 5

John Wilson
Green College, Oxford

Trinity Term 1998

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Oxford

Curves of genus 2 with real multiplication by a square root of 5

John Wilson
Green College, Oxford

Trinity Term 1998

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Oxford

Abstract

Our aim in this work is to produce equations for curves of genus 2 whose Jacobians have real multiplication (RM) by $\mathbb{Q}(\sqrt{5})$, and to examine the conjecture that any abelian surface with RM by $\mathbb{Q}(\sqrt{5})$ is isogenous to a simple factor of the Jacobian of a modular curve $X_0(N)$ for some N.

To this end, we review previous work in this area, and are able to use a criterion due to Humbert in the last century to produce a family of curves of genus 2 with RM by $\mathbb{Q}(\sqrt{5})$ which parametrizes such curves which have a rational Weierstrass point.

We proceed to give a calculation of the ℓ-adic representations arising from abelian surfaces with RM, and use a special case of this to determine a criterion for the field of definition of RM by $\mathbb{Q}(\sqrt{5})$. We examine when a given polarized abelian surface A defined over a number field k with an action of an order R in a real field F, also defined over k, can be made principally polarized after k-isogeny, and prove, in particular, that this is possible when the conductor of R is odd and coprime to the degree of the given polarization.

We then give an explicit description of the moduli space of curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$. From this description, we are able to generate a fund of equations for these curves, employing a method due to Mestre.

Acknowledgements

There are many people without whose help this thesis would not be what it is (or simply would not be).

My thanks are due to Prof. Birch for his suggestion of the work contained herein, and his diligent supervision of its progress.

I should especially like to thank Peter Bending for useful discussions which set my ideas straight on many occasions (proposition 2.6.1 and lemma 4.5.6, in particular, are the fruit of such discussions). In a similar capacity, my thanks go to Frazer Jarvis and Steven Galbraith.

I owe a material debt to all British tax-payers for funding this work via the EPSRC.

Last, on a personal note, I should like to dedicate this thesis to Sarah because of her constant love and support.

> "Man puts an end to the darkness; he searches the farthest recesses for ore in the blackest darkness. ... He searches the sources of the rivers and brings hidden things to light. 'But where can wisdom be found? Where does understanding dwell?' ... God understands the way to it and he alone knows where it dwells, for he views the ends of the earth and sees everything under the heavens."
>
> Job 28:3, 11–12, 23–24

Contents

Chapter 1

Introduction

1.1 Motivation

This thesis is concerned with curves of genus 2 with real multiplication, and especially those with real multiplication by $\mathbb{Q}(\sqrt{5})$. Exact definitions are given in chapter 2, but for now let us note that these arise naturally when one considers the factors of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ classifying pairs of N-isogenous elliptic curves. Indeed, Shimura's construction of an abelian variety corresponding to a cusp form of weight 2 gives an abelian variety with real multiplication by the field generated by the Fourier coefficients of the form (see [Shi71, chapter 7]). More than this, we are motivated by the following conjecture; note that we shall call an abelian variety $A/\mathbb{Q}$ *modular* if A is $\mathbb{Q}$-isogenous to a factor of $J_0(N)$ for some N.

Conjecture 1.1.1 *Every simple abelian variety $A/\mathbb{Q}$ with real multiplication defined over $\mathbb{Q}$ is modular.*

The value of N for which we expect that A is isogenous to a factor of $J_0(N)$ is related to the Artin conductor of the ℓ-adic representations of the absolute Galois group of $\mathbb{Q}$ on the Tate modules of the abelian variety A—we say more about this in section 2.8.

It is worth noting that we deliberately state this conjecture in a strong form, in the sense that we do not refer to any polarization on the abelian variety A. Indeed it is

fairer to say that our work is motivated by the possibly weaker conjecture that every abelian variety over $\mathbb{Q}$ which has real multiplication and a principal polarization both defined over $\mathbb{Q}$ is modular. This weaker form of the conjecture extends immediately to all polarized abelian varieties over $\mathbb{Q}$ with real multiplication defined over $\mathbb{Q}$ which become principally polarized after $\mathbb{Q}$-isogeny. But it is not clear whether this includes all polarized abelian varieties.

In general, hardly any of conjecture 1.1.1 has been proven. In the case that A is an elliptic curve, however, the last few years have seen remarkable progress through the work of Wiles [Wil95], as completed by Taylor and Wiles [TW95], and extended by Diamond [Dia96]: but for a few technical conditions, (1.1.1) is a theorem for elliptic curves. (We should note that conjecture 1.1.1 for elliptic curves is generally known as the *Shimura–Taniyama Conjecture*.) Conjecture 1.1.1 has also been addressed (in a slightly different form) by Ribet [Rib92], who has shown that (1.1.1) would follow from Serre's conjecture on mod p Galois representations (see [Ser87]).

We consider the 2-dimensional case: abelian surfaces with real multiplication. Wiles' approach is via the ℓ-adic Galois representations associated with elliptic curves; these are 2-dimensional, and are already difficult to get to grips with. Passing to abelian surfaces gives us 4-dimensional Galois representations, and there seems little hope of understanding these at present. However, the presence of a real multiplication chops the size of these representations down again (as we shall see in chapter 4). Indeed, Taylor and Shepherd-Barron [SBT97, Theorem 4.2] have extended Wiles' result to give the following.

Theorem 1.1.2 *Suppose that $A/\mathbb{Q}$ is an abelian surface, $\lambda\colon A \to A^\vee$ is a principal polarization and $i\colon \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{5})\right] \to \mathrm{End}(A)$ is an embedding, all defined over $\mathbb{Q}$ and such that $\lambda \circ i(a) = i(a)^\vee \circ \lambda$ for all a. Suppose moreover that A has semi-stable reduction at 3 and 5 and that the representation of $G_{\mathbb{Q}(\sqrt{5})}$ on the $\sqrt{5}$-division points of A is irreducible. Then A is modular.*

It is worth remarking that the conditions on the reduction at 3 and 5 follow from the method of proof which applies Diamond's results [Dia96], but that the existence of

a principal polarization seems a real restriction. (Compare with our remarks following conjecture 1.1.1.)

We can actually get hold of principally polarized abelian surfaces because they are the Jacobians of curves of genus 2 (see section 2.4) and, further, we can obtain examples with real multiplication by $\mathbb{Q}(\sqrt{5})$ because of a rather beautiful criterion obtained by Humbert in the last century [Hum99] (see chapter 3). Indeed some of our motivation has been to re-discover some of this underlying classical geometry.

With all this in mind, we focus mainly on curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$, and our principal aim is to produce a fund of examples of these. This, among other things, provides a fund of icosahedral representations of $G_{\mathbb{Q}}$ (see chapter 4).

There is one subtle point here which it is worth making explicit at an early stage. We start from equations for curves of genus 2 and take their Jacobians as our examples of abelian surfaces. These surfaces are canonically principally polarized (see chapter 2). Now the Shimura factors of $J_0(N)$ have a natural polarization on them, too, but this need not be principal. Thus we can only hope to cover those factors of $J_0(N)$ which can be made principally polarized after an isogeny over $\mathbb{Q}$.

Now it is well known that any polarized abelian variety over an algebraically closed field is isogenous to a principally polarized abelian variety, but the same need not be true over non-algebraically closed fields (see [Mil86a, Remark 16.14]). However, to be more positive, we do have that the extra structure given by the presence of a real multiplication allows us to make the Shimura factors principally polarized most of the time (see chapter 4).

1.2 Outline

In the remainder of this chapter we offer a brief outline of the rest of this thesis, and give a short (but important) remark on notation.

In chapter 2 we review the theory underlying curves of genus 2 and abelian surfaces, including the link between them, and some information about reduction modulo

primes. We review some facts about the endomorphism structure of abelian surfaces, and finish with an account of Poncelet's theorem, a classical result in plane projective geometry of which we make use later.

In chapter 3 we restrict our attention to curves with real multiplication by $\mathbb{Q}(\sqrt{5})$, and review Humbert's criterion in more modern language. We then use this to determine an explicit description of a given real multiplication by $\mathbb{Q}(\sqrt{5})$, to establish a criterion for the field of definition of a real multiplication by $\mathbb{Q}(\sqrt{5})$, and to produce a family of curves with real multiplication by $\mathbb{Q}(\sqrt{5})$. This family of curves parametrizes such curves defined over $\mathbb{Q}$ which have a rational Weierstrass point. Examples of families of curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$ already exist in the literature—see [Mes91a] and [Bru95, equation 6.2] (there is also a brief report of Brumer's work in [CF96, chapter 15]). We note that both of these constructions are indirect, unlike ours.

In chapter 4 we return to the more general case, and examine the ℓ-adic Galois representations associated with abelian varieties with real multiplication, and more particularly to abelian surfaces with real multiplication. We also consider the question of when a polarized abelian surface with real multiplication is isogenous (over the ground field) to a principally polarized abelian surface.

In chapter 5 we describe the moduli spaces of principally polarized abelian surfaces, and of principally polarized abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{5})$. We discuss the question of "definition over k" for the various parts of the moduli problem, which leads us on to chapter 6, where we describe a construction due to Mestre [Mes91b] to produce equations for curves of genus 2 from their moduli, and then use this to calculate various examples. We also offer a brief diversion to discuss equations for curves with nontrivial automorphisms and real multiplication by $\mathbb{Q}(\sqrt{5})$. A necessary part of the method on chapter 6 for producing equations is to be able to find points on conics defined over $\mathbb{Q}$, and so we discuss some of the practical details involved in this.

We finish with an appendix giving various tables and remarks on the results contained in them.

1.3 A remark about notation

Notation, where not defined explicitly, is standard (for example, we use the traditional symbols $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{R}$ to denote the rational numbers, integers and real numbers). Note that we use $\overline{k}$ to denote the algebraic closure of a number field k, and G_k to denote the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of k. Also, the letter η only ever denotes the quantity $\frac{1}{2}(1+\sqrt{5})$ (so that $\mathbb{Z}[\eta]$ is the ring of integers of $\mathbb{Q}(\sqrt{5})$).

Chapter 2

Background material

2.1 Generalities on curves of genus 2

We begin by discussing some of the theory relating to curves of genus 2, assuming many of the basic notions but also trying to state explicitly those properties we shall use later in this thesis.

Let C be a curve of genus 2 over a field k. (We do not assume that k is algebraically closed.) Then, as we can calculate from the Riemann–Roch theorem [Har77, IV.1.3], the canonical linear system κ on C has degree 2 and dimension 1. But for any curve of genus greater than 1 the canonical linear system has no base points [Har77, IV.5.1], so we then have that κ defines a 2-1 morphism $C \to \mathbb{P}^1$ over the algebraic closure $\overline{k}$, the *canonical morphism*. A curve which admits such a morphism and which has genus greater than 1 is called a *hyperelliptic curve*. Any hyperelliptic curve carries a natural involution, called the *hyperelliptic involution*, which interchanges the branches of the map to $\mathbb{P}^1$. The canonical linear system on a curve C of genus 2 is the unique linear system of dimension 1 and degree 2 [Har77, IV.5.3], and so any two double covers $C \to \mathbb{P}^1$ differ only by an automorphism of $\mathbb{P}^1$, since they differ only by choosing different bases for κ.

For any 2-1 map $C \to \mathbb{P}^1$ we can use the Hurwitz genus formula [Har77, IV.2.4] to calculate that there are precisely six branch points, save in characteristic 2.

Now, in fact, κ has a basis of elements each defined over k (not just $\overline{k}$) as a

consequence of the following lemma [Sil86, II.5.8.1].

Lemma 2.1.1 *Let V be a $\overline{k}$-vector space with a continuous G_k-action compatible with the G_k-action on $\overline{k}$. Then V has a $\overline{k}$-basis which is fixed elementwise by G_k.*

Hence we can choose our canonical morphism $C \to \mathbb{P}^1$ to be a map defined over k, not just $\overline{k}$.

Thinking concretely, this gives us an affine equation for C of the shape

$$y^2 + g(x)y = h(x), \tag{2.1}$$

where g and h are polynomials over k. In all characteristics other than 2, we can complete the square and obtain an equation

$$y^2 = f(x), \tag{2.2}$$

with $f(x) = 4h(x) + g(x)^2$. The map $C \to \mathbb{P}^1$ is then essentially projection onto the x-coordinate, and the hyperelliptic involution changes the sign of the y-coordinate. Notice that we must have $\deg f$ equal to 5 or 6, as a consequence of Hurwitz's formula. When k has more than 5 elements then we may make a coordinate transformation of the form

$$(x, y) \mapsto \left(\frac{1}{x-a}, \frac{y}{(x-a)^3} \right)$$

and produce a new equation (2.2) with the degree of f equal to 6. (There are a few curves in small characteristic where this is not possible, for example the curve over $\mathbb{F}_5$ given by

$$y^2 = x(x-1)(x-2)(x-3)(x-4),$$

since then there is no suitable choice for a.)

Suppose for the moment that the characteristic of k is not 2. If we try to complete the curve given by an equation as in (2.2) in a naïve manner, then we end up with a singular curve: there is a point of multiplicity $(\deg f - 2)$ at infinity. We can desingularize this by repeated blowing up (see [Har77, Proposition V.3.8]) and if we calculate the genus of the resulting curve by the formula in [Har77, Example V.3.9.2],

we do indeed obtain a curve of genus 2. A rather prettier way to proceed is presented in [CF96, chapter 1]. We replace the map $C \to \mathbb{P}^1$ by a map $C \to X$, where X is the image of the 3-uple embedding $\mathbb{P}^1 \hookrightarrow \mathbb{P}^3$ to obtain a model of the form

$$\begin{aligned} x_0x_2 = x_1^2,\ x_0x_3 = x_1x_2,\ x_1x_3 = x_2^2, \\ x_4^2 = f_0x_0^2 + f_1x_0x_1 + f_2x_1^2 + f_3x_1x_2 + f_4x_2^2 + f_5x_2x_3 + f_6x_3^2. \end{aligned}$$

in $\mathbb{P}^4$. This is clearly birational to the original curve but neatly replaces the singular point at infinity with two nonsingular points when $\deg f = 6$, and with one nonsingular point when $\deg f = 5$. As an alternative approach, one can complete the curve by gluing it to its image under a rational map which moves the point at infinity. In terms of equations, we use the rational map

$$(x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^3}\right)$$

and produce the set of equations

$$y^2 = f(x),\ xX = 1,\ x^3Y = 1,\ \text{and } Y^2 = F(X),$$

where $F(x) = x^6 f(1/x)$.

(As an aside, note that we can never find a nonsingular model for a curve of genus 2 as a complete intersection because the canonical map is not an embedding [Har77, Exercise IV.3.3].)

An important remark about equations of the form (2.2) for a curve C of genus 2 is that f on the right-hand side is determined up to fractional linear transformations

$$f(x) \mapsto (cx + d)^6 f\left(\frac{ax + b}{cx + d}\right),\ \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k).$$

(This follows from the remark earlier that the canonical morphism is defined up to an automorphism of $\mathbb{P}^1$.) As a result of this, we often think of C as being given, at least up to isomorphism, by the six branch points of $C \to \mathbb{P}^1$, that is, the roots of f along with ∞ in the case that f has degree 5. The points of C above these branch points are called the *Weierstrass points*.

Now we turn to the question of when an equation of the shape (2.1) or (2.2) gives a singular curve (with the aforementioned caveat about the point(s) at infinity). It is easy to calculate that in characteristics other than 2, this occurs exactly when $f(x) = 4h(x) + g(x)^2$ has a repeated root (in $\overline{k}$). In characteristic 2, things are a little different: in general we do not have an equation of shape (2.2), but only of the shape (2.1) and in this case we find that the affine curve is singular if and only if $g(x)$ and $t(x) := h'(x)^2 + g'(x)^2 h(x)$ have a common root (in $\overline{k}$).

Finally for this section, we discuss when an equation (2.1) gives a curve of genus 2. We do this by applying Hurwitz's genus formula to the canonical map π, which can be thought of as projection onto the x-coordinate in (2.1). Note that this map is separable whenever the characteristic of k is not 2, that it is separable in characteristic 2 when g is nonzero and is purely inseparable otherwise. Since genus is invariant under purely inseparable maps [Har77, Proposition IV.2.5], we first require that $\operatorname{char} k \neq 2$ or that $g \neq 0$.

In these remaining cases, we can apply Hurwitz's formula. When $\operatorname{char} k \neq 2$, the map π is tamely ramified, and branches above the roots of $f(x) = 4h(x) + g(x)^2$. Infinity is also a branch point precisely when $\deg f$ is odd. The ramification index at each ramification point is 2, and hence the curve has genus 2 exactly when $\deg f$ is 5 or 6.

When $\operatorname{char} k = 2$, the map π branches at the roots of g, and at infinity when $\deg(h) > 2\deg(g)$, and is wildly ramified at each ramification point. We can differentiate the equation (2.1) with respect to x to determine that

$$\frac{\mathrm{d}y}{\mathrm{d}x} = \frac{h'(x) + g'(x)y}{g(x)}.$$

It follows that $\mathrm{d}y/\mathrm{d}x$ has a double pole at each root of g. To examine the behaviour at infinity, we choose for local parameters at infinity $x_1 = 1/x$ on $\mathbb{P}^1$ and $y_1 = y/x^3$ on the curve. Then, in a similar fashion, $\mathrm{d}y_1/\mathrm{d}x_1$ has a pole at $x_1 = y_1 = 0$ if and only if $\deg(h) > 2\deg(g)$, and then the order of this pole is $2(r - \deg g)$ where r is the smallest integer no less than $\deg(h)/2$. Substituting this into Hurwitz's genus formula, one determines that the curve has genus 2 exactly when the larger of $\deg g$

and r is 3 (the same answer as in other characteristics).

2.2 The Jacobian of a curve of genus 2

An important object for the study of the arithmetic of a curve C is the *Jacobian* $\mathrm{Jac}(C)$. For a thorough account (which we do not hope to reproduce in all its generality) of the theory of Jacobians one might look at [Mil86b]. We aim now to present the properties that we need.

The first point is that $\mathrm{Jac}(C)$ is an abelian variety of dimension equal to the genus of C. It gives geometric structure to the group $\mathrm{Pic}^0(C)$ of divisors of degree 0 modulo linear equivalence, in the sense that $\mathrm{Pic}^0(C_{k'})$ is isomorphic to $\mathrm{Jac}(C)(k')$ for each extension k'/k such that $C(k') \neq \emptyset$.

When C has a k-point P, say, we can define a map $f^P\colon C(k) \to \mathrm{Jac}(C)(k)$ by mapping each point Q to the class of the divisor $Q - P$ (and identifying $\mathrm{Pic}^0(C)$ and $\mathrm{Jac}(C)(k)$). Then $\mathrm{Jac}(C)$ satisfies the following universal property [Mil86b, Proposition 6.1].

Proposition 2.2.1 *Suppose that A is an abelian variety over k and that $\varphi\colon C \to A$ is a map such that $\varphi(P) = 0$. Then there is a unique homomorphism $\psi\colon \mathrm{Jac}(C) \to A$ such that $\varphi = \psi \circ f^P$.*

In general, C need not have a k-point. But there will be some Galois extension k'/k such that $C(k') \neq \emptyset$; given $P \in C(k')$ we can define a map $F\colon C_{k'} \times C_{k'} \to \mathrm{Jac}(C)_{k'}$ by $(P_1, P_2) \mapsto f^P(P_1) - f^P(P_2)$. The map F is independent of the choice of the point P and so is defined over k. Notice also that it is zero on the diagonal. Then we also have the following universal property.

Proposition 2.2.2 *Let A be an abelian variety over k and $\varphi\colon C \times C \to A$ a map which is zero on the diagonal. Then there is a unique homomorphism $\psi\colon \mathrm{Jac}(C) \to A$ such that $\varphi = \psi \circ F$.*

In our case, the genus of C is 2, so $\mathrm{Jac}(C)$ is an abelian surface. Further, it is naturally principally polarized, and by an image of C [Mil86b, Theorem 6.6]. We

shall see in section 2.4 that any principally polarized abelian surface which is not a product is necessarily a Jacobian.

To be able to look at $\mathrm{Jac}(C)$ in a more concrete way, we recall that it is closely linked to the symmetric square $C^{(2)}$. The canonical class on C is of degree 2, and so addition of this class in $\mathrm{Pic}(C)$ gives an identification between $\mathrm{Pic}^0(C)$ and $\mathrm{Pic}^2(C)$. Of course there is a natural surjection $C^{(2)}(\overline{k}) \twoheadrightarrow \mathrm{Pic}^2(C_{\overline{k}})$: simply send the pair $\{P_1, P_2\}$ to the class of the divisor $P_1 + P_2$. So we can view $\mathrm{Jac}(C)$ as some sort of quotient of $C^{(2)}$.

We can be more precise about this. Let i denote the hyperelliptic involution on C. Then, given any point $P \in C(\overline{k})$ the canonical morphism sends P and $i(P)$ to the same point, so the divisor $P + i(P)$ must lie in the canonical class. Now suppose that D is any divisor on C of degree 2 and that K is some canonical divisor. Then $(K - D)$ has degree 0, so is linearly equivalent to an effective divisor exactly when it is equivalent to the empty divisor, that is when $K \sim D$. For any divisor D of degree 2 which is not in the canonical class, then, the Riemann–Roch theorem tells us that D is linearly equivalent to precisely one effective divisor. This allows us to identify each element of $\mathrm{Pic}^2(C)$ other than the canonical class with its unique effective element.

As a result, we can describe $\mathrm{Jac}(C)$ as the symmetric square $C^{(2)}$ with the line formed of pairs $\{P, i(P)\}$ blown down. If we are given an equation for C in the shape (2.2), then we can choose our canonical divisor to be $(\infty^+ + \infty^-)$, where $\infty^\pm$ are the points of a desingularized model for C which lie above the point at infinity on (2.2). So every point of $\mathrm{Jac}(C)$ is represented by a divisor of the form $(P_1 + P_2 - \infty^+ - \infty^-)$, and this form is unique except when $P_1 = i(P_2)$.

We also have that when we want to define a map of the Jacobian (as we shall do in chapter 3) it will be enough to define a map of the symmetric square which commutes with the hyperelliptic involution.

Even more explicitly than all this, E.V. Flynn has determined equations for an embedding into $\mathbb{P}^{15}$ of the Jacobian of a curve of genus 2 [CF96, Chapter2]. These equations are fairly complicated, and so we have not made much use of them here,

but see proposition 3.3.1 for an application.

2.3 Remarks about moduli spaces

Since much of what follows in this thesis is concerned with moduli problems, we offer a brief discussion of some of the generalities concerning these. The discussion that follows is heavily influenced by [Che96, §1.2], and by the account in [Cha86, §1] for the theory of the moduli of abelian varieties.

Let $\mathscr{A}$ be the set of pairs X/S, where X is an object of the type to be classified over the scheme S. Suppose further that $\mathscr{A}$ is closed under base extension. We are being deliberately vague here; to clarify matters we give a few examples. First, consider the problem of classifying principally polarized abelian surfaces with a level 2 structure (the precise definition of what we mean by this is given in section 5.1). Then we should let the objects X/S be triples $(A/S, \lambda, \mu)$ formed of an abelian scheme A/S of relative dimension 2, a principal polarization λ on A and a level 2 structure μ. The maps between these objects are the obvious ones. We also consider the problem of classifying curves of genus 2 up to isomorphism. Here X/S would be an S-scheme of relative dimension 1 and genus 2; again the maps are the obvious ones.

Now let $\mathscr{M}$ be the contravariant functor from schemes to sets given by

$$\mathscr{M}(S) = \{S\text{-isomorphism classes of } (X/S) \in \mathscr{A}\}.$$

We wish to represent $\mathscr{M}$ by a scheme $\mathbb{M}$ if at all possible, so that S-points of $\mathbb{M}$ correspond exactly to S-isomorphism classes of $(X/S) \in \mathscr{A}$.

Definition 2.3.1 *The scheme* $\mathbb{M}$ *is a* fine moduli space *(for our moduli problem) if* $\mathbb{M}$ *represents the functor* $\mathscr{M}$*. The* universal family $\mathscr{X}/\mathbb{M}$ *is then the object associated with the identity of* $\mathscr{M}(\mathbb{M}) = \mathrm{Hom}_{\mathrm{Sch}}(\mathbb{M}, \mathbb{M})$.

Clearly a fine moduli space is unique up to isomorphism if it exists. Also, the universal family does the job one expects: the isomorphism of functors $\mathscr{M}(-) = \mathrm{Hom}(-, \mathbb{M})$ gives us that for any $(X/S) \in \mathscr{A}$ there is a unique map of schemes

$\phi\colon S \to \mathbb{M}$ such that X/S is the pullback along ϕ of $\mathscr{X}/\mathbb{M}$. This gives us the first clue why fine moduli spaces do not, in general, exist: if X/S has nontrivial automorphisms then the map ϕ will no longer be unique. We can, however, still hope in many cases for a near approximation.

Definition 2.3.2 *The scheme $\mathbb{M}$ is a* coarse moduli space *if there is a natural transformation of functors $\alpha\colon \mathscr{M}(-) \to \mathrm{Hom}(-, \mathbb{M})$ and if the pair $(\mathbb{M}, \alpha)$ is universal among pairs $(\mathbb{M}', \alpha')$ of a scheme $\mathbb{M}'$ and a natural transformation $\alpha'\colon \mathscr{M}(-) \to \mathrm{Hom}(-, \mathbb{M}')$ with the property that α' is bijective on algebraically-closed fields.*

So a coarse moduli space is also unique up to isomorphism if it exists, and represents $\mathscr{M}$ "geometrically." Naturally enough, a fine moduli space is a coarse moduli space.

Now let k be a number field and $\overline{k}$ its algebraic closure. If $\mathbb{M}$ is a fine moduli space then it is immediate from the definition that k-points of $\mathbb{M}$ correspond to k-isomorphism classes of objects $(X/\operatorname{Spec} k) \in \mathscr{A}$. For a coarse moduli space this need not hold: an object $X/\operatorname{Spec} k$ still gives rise to a k-point of $\mathbb{M}$ (via α) but a k-point of $\mathbb{M}$ need not be associated with any object over k.

Suppose that we have an object $X/\operatorname{Spec} \overline{k}$ and an automorphism $\sigma \in \mathrm{Gal}(\overline{k}/k)$. We define ${}^{\sigma}X/\operatorname{Spec} \overline{k}$ to be the pullback along the induced map $\operatorname{Spec} \overline{k} \xrightarrow{\sigma} \operatorname{Spec} \overline{k}$ of $X/\operatorname{Spec} \overline{k}$. Now we have a commutative diagram

$$\begin{array}{ccc} \mathscr{M}(\operatorname{Spec} \overline{k}) & \xrightarrow{\alpha} & \mathrm{Hom}(\operatorname{Spec} \overline{k}, \mathbb{M}) \\ \Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle \sigma} \\ \mathscr{M}(\operatorname{Spec} \overline{k}) & \xrightarrow[\alpha]{} & \mathrm{Hom}(\operatorname{Spec} \overline{k}, \mathbb{M}) \end{array}$$

and so if $X/\operatorname{Spec} \overline{k}$ is associated with $x \in \mathbb{M}(\operatorname{Spec} \overline{k})$ then ${}^{\sigma}X/\operatorname{Spec} \overline{k}$ is associated with ${}^{\sigma}x$.

We also have a commutative diagram

$$\begin{array}{ccc} \mathscr{M}(\operatorname{Spec} k) & \xrightarrow{\alpha} & \operatorname{Hom}(\operatorname{Spec} k, \mathbb{M}) \\ \downarrow & & \downarrow \\ \mathscr{M}(\operatorname{Spec} \overline{k}) & \xrightarrow[\alpha]{} & \operatorname{Hom}(\operatorname{Spec} \overline{k}, \mathbb{M}) \end{array}$$

with the lower horizontal arrow being a bijection, so to any $x \in \mathbb{M}(k)$ we can certainly associate a $\overline{k}$-isomorphism class. But further, for each $X/\operatorname{Spec}\overline{k}$ in this class and for each $\sigma \in \operatorname{Gal}(\overline{k}/k)$, we must have that ${}^{\sigma}X/\operatorname{Spec}\overline{k}$ is isomorphic to $X/\operatorname{Spec}\overline{k}$ since it, too, will be associated with the point $x = {}^{\sigma}x$.

Thus we have that the k-points of a coarse moduli space $\mathbb{M}$ correspond to the $\overline{k}$-isomorphism classes which contain an object $X/\operatorname{Spec}\overline{k}$ such that ${}^{\sigma}X/\operatorname{Spec}\overline{k}$ is isomorphic to $X/\operatorname{Spec}\overline{k}$ for each $\sigma \in G_k$.

If we further assume that $X/\operatorname{Spec}\overline{k}$ has no nontrivial automorphisms then for each $\sigma \in G_k$ there will be a unique isomorphism $\phi(\sigma)\colon {}^{\sigma}X/\operatorname{Spec}\overline{k} \to X/\operatorname{Spec}\overline{k}$, and ϕ then satisfies the cocycle identity

$$\phi(\sigma\tau) = {}^{\sigma}\phi(\tau) \circ \phi(\sigma).$$

One generally tries to make sure that the objects of $\mathscr{A}$ have enough structure that, at least generically, they have no nontrivial automorphisms. If no object of $\mathscr{A}$ has nontrivial automorphisms then we call the moduli problem *rigid*.

Our principal motivation is to study the moduli space of curves of genus 2. A fundamental problem here is that the moduli problem is not rigid, and so there is at best a coarse moduli space. However, in this case we can view ϕ as a 1-cocycle valued in $\operatorname{Aut}(\mathbb{P}^1/\overline{k}) = \operatorname{PGL}_2(\overline{k})$. Then $X/\operatorname{Spec}\overline{k}$ has a model over k, that is to say it is the pullback of some $X_k/\operatorname{Spec} k$ exactly when ϕ is a 1-coboundary. But we return to this point in detail in chapter 5, and so do not discuss it further here.

2.4 A classification of abelian surfaces

If E_1 and E_2 are elliptic curves, then $E_1 \times E_2$ is an abelian surface with canonical polarization given by the divisor $(E_1 \times \{0\}) + (\{0\} \times E_2)$. If C is a curve of genus 2, then $\mathrm{Jac}(C)$ is an abelian surface with canonical polarization given by an image of C on $\mathrm{Jac}(C)$. We now prove that, up to isomorphism, these are the only examples of principally polarized abelian surfaces. (The proof we give is basically an annotated version of that in [Gon94, §§4.10–4.13]; the result is due to Weil [Wei57]).

First, we prove the following lemma.

Lemma 2.4.1 *For any effective divisor D on an abelian surface A, the arithmetic genus is given by*

$$p_a(D) = \frac{1}{2}(D^2) + 1.$$

Proof The Riemann–Roch theorem for A [Mum70, §16] states that $\chi(\mathscr{L}(D)) = \frac{1}{2}(D^2)$, where χ is the Euler characteristic, and $\mathscr{L}(D)$ is the invertible sheaf associated with D.

Further, we have a short exact sequence

$$0 \to \mathcal{O}_A \to \mathscr{L}(D) \to \mathscr{L}(D) \otimes \mathcal{O}_D \to 0,$$

because of [Har77, II.6.18] after tensoring with $\mathscr{L}(D)$, and the Euler characteristic is additive on short exact sequences, so

$$\chi(\mathscr{L}(D)) = \chi(\mathcal{O}_A) + \chi(\mathscr{L}(D) \otimes \mathcal{O}_D).$$

But now [Mum70, §13, page 129] gives $h^0(A, \mathcal{O}_A) = h^2(A, \mathcal{O}_A) = 1$, $h^1(A, \mathcal{O}_A) = 2$ and $h^i(A, \mathcal{O}_A) = 0$ for $i > 2$, and so $\chi(\mathcal{O}_A) = 0$.

The Riemann–Roch theorem for curves [Har77, IV.1.3] applied to D gives

$$\chi(\mathscr{L}(D) \otimes \mathcal{O}_D) = \deg_D(\mathscr{L}(D) \otimes \mathcal{O}_D) + 1 - p_a(D) = \left(D^2\right) + 1 - p_a(D),$$

so the result follows. □

Theorem 2.4.2 *Let A be a principally polarized abelian surface defined over an algebraically closed field k. Then A is isomorphic over k to (exactly) one of* $\mathrm{Jac}(C)$ *for a curve C of genus 2 and a product $E_1 \times E_2$ of elliptic curves.*

Proof Let D be an ample effective divisor on A giving the polarization. Then from [Mum70, §16], we deduce that $\chi(\mathscr{L}(D)) = 1$, $(D^2) = 2$ and $p_a(D) = 2$.

First suppose that D is irreducible. $(D^2) = 2$, which is squarefree, and so D is also reduced. Let C be the normalization of D, so we have a map $C \to A$. The curve C cannot be rational (there are no non-constant maps from rational varieties to abelian varieties [Mil86a, corollary 3.9]); suppose C is elliptic. Then the map $C \to A$ is, up to translation, a homomorphism, and so the image, namely D, is nonsingular which implies that $p_a(D) = p_a(C) = 1$, a contradiction. Hence C must be a curve of genus 2.

The map $C \to A$ induces a map $\pi\colon \mathrm{Jac}(C) \to A$ such that $\pi(C) = D$. On $\mathrm{Jac}(C)$ we have $(C^2) = 2$ (as for D on A), but we also have that $(\pi^*(D) \cdot C) = (D \cdot \pi_*(C)) = (D^2) = 2$. If $\deg(\pi) > 1$ then $\pi^*(D) = C + C'$ for some nonzero divisor C', and thus $(\pi^*(D) \cdot C) = (C^2) + (C' \cdot C) > 2$ since C is ample on $\mathrm{Jac}(C)$. Hence $\pi\colon \mathrm{Jac}(C) \xrightarrow{\sim} A$ as principally polarized abelian surfaces.

Now suppose that D is reducible. D is ample, so $(D \cdot D') > 0$ for any effective divisor D' on A; hence $(D^2) = 2$ forces $D = D_1 + D_2$, where the D_i are reduced and irreducible, and $(D_i^2) = 0$, $(D_1 \cdot D_2) = 1$. That is, D is the union of two curves of arithmetic genus 1 which meet in one point. Let C_i be the normalization of D_i $(i = 1, 2)$.

Again, C_1 and C_2 cannot be rational, so must be elliptic. Then the maps $C_1, C_2 \to A$ give rise to a map $\pi\colon C_1 \times C_2 \to A$ of abelian surfaces such that $\pi(C_1 \times \{0\}) = D_1$ and $\pi(\{0\} \times C_2) = D_2$. But now we can calculate as before that $\deg(\pi) = 1$. □

2.5 Endomorphism structure of an abelian surface

Let (A, λ) be a polarized abelian surface defined over a number field k, and write $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$. Let $\alpha \in \mathrm{End}(A)$. Then α induces an endomorphism $\alpha^\vee \in \mathrm{End}(A^\vee)$ by functoriality; $\alpha^\vee$ acts on geometric points by taking the preimage: $\alpha^\vee(D) = \alpha^* D$.

The *Rosati involution* on $\mathrm{End}^0(A)$ associated with the polarization λ is defined by

$$\dagger \colon \alpha \mapsto \lambda' \circ \alpha^\vee \circ \lambda,$$

where $\lambda' \in \mathrm{Hom}(A^\vee, A) \otimes \mathbb{Q}$ is an inverse for $\lambda \in \mathrm{Hom}(A, A^\vee)$. This is a positive involution, that is, the trace of $\alpha\alpha^\dagger$ is always positive. (See, for example, [Mil86a, Theorem 17.3].)

Notice that $\dagger$ preserves the subalgebra $\mathrm{End}_k^0(A)$ of endomorphisms defined over k.

Shimura [Shi63] classifies the possibilities for $\mathrm{End}^0(A)$. Suppose that A is geometrically simple. Then (with reference to §§1,4 of [Shi63]), $\mathrm{End}^0(A)$ must be one of the following:

(a) $\mathbb{Q}$;

(b) a totally real quadratic field $F/\mathbb{Q}$;

(c) a totally indefinite quaternion algebra $B/\mathbb{Q}$;

(d) a quartic CM field $K/\mathbb{Q}$.

We note that $\mathrm{End}^0(A) = \mathrm{End}^0(B)$ when A and B are isogenous abelian varieties. Also, if $A = \prod_{i=1}^{n} A_i^{r_i}$, where the A_i are simple abelian varieties which are not isogenous, then $\mathrm{End}^0(A) = \bigoplus_{i=1}^{n} \mathrm{M}_{r_i}\left(\mathrm{End}^0(A_i)\right)$.

If an abelian variety A admits an embedding $F \hookrightarrow \mathrm{End}^0(A)$ for a totally real field F, we shall say that A *has real multiplication by* F. If further $\mathrm{End}(A)$ contains the maximal order of F then we shall say A *has maximal real multiplication by* F.

We shall also use the terms *quaternionic multiplication* and *complex multiplication* analogously, and may abbreviate these three terms to RM, QM and CM from time to time.

One also knows the possibilities for the automorphism group of a curve of genus 2, the classification being due to Bolza [Bol88]. A curve C of genus 2 always carries a hyperelliptic involution; the *reduced automorphism group* $\mathrm{Aut}(C)^{\mathrm{red}}$ is the automorphism group modulo the hyperelliptic involution. This then embeds in $\mathrm{Aut}(\mathbb{P}^1)$ via the canonical map $C \to \mathbb{P}^1$, and is finite. Since the finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$ are known, this leaves us in good shape to proceed to a classification of $\mathrm{Aut}(C)^{\mathrm{red}}$.

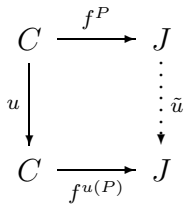
The reduced automorphism group is generically trivial; Bolza's classification of those cases where $\mathrm{Aut}(C)^{\mathrm{red}}$ is nontrivial is as follows. The second column gives a binary sextic form $f(x_1, x_2)$ such that if C is a curve of the relevant type then $y^2 = f(x, 1)$ gives an affine equation for C, for some choice of the parameters $\alpha, \beta \in \overline{k}$.

Type	$f(x_1, x_2)$	$\mathrm{Aut}(C)^{\mathrm{red}}$
I	$x_1^6 + \alpha x_1^4 x_2^2 + \beta x_1^2 x_2^4 + x_2^6$	C_2
II	$x_1(x_1^5 + x_2^5)$	C_5
III	$x_1 x_2(x_1^4 + \alpha x_1^2 x_2^2 + x_2^4)$	D_4
IV	$x_1^6 + \alpha x_1^3 x_2^3 + x_2^6$	D_6
V	$x_1^6 + x_2^6$	D_{12}
VI	$x_1 x_2(x_1^4 + x_2^4)$	S_4

It is possible to rewrite this, dividing into only two cases, the first being when $\mathrm{Aut}(C)^{\mathrm{red}}$ contains an involution and the second being case II as above; cases I and III–VI are then specializations of this new first case.

Fix a point $P \in C(\overline{k})$ and let $f^P : C \to J$ be the map defined in section 2.2. We shall define an embedding $\mathrm{Aut}(C) \hookrightarrow \mathrm{End}(J) : u \mapsto \tilde{u}$. For each $u \in \mathrm{Aut}(C)$, let $\tilde{u}$ be the endomorphism of J which fits in the following diagram. Then $\tilde{u}$ is unique and well-defined by proposition 2.2.1, and one may readily check that $u \mapsto \tilde{u}$ is independent

of the choice of P.



Now we can see that when C is of type II, then J has CM by $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive 5th root of 1, and in particular that J is simple. For type I and types III–VI, on the other hand, the group structure implies that $\mathrm{End}(J)$ is not a division ring, since $\mathrm{Aut}(C)$ contains more than two square roots of 1. Hence, in these cases, J must be isogenous to the product of two elliptic curves. This is also clear from the equations in the table above, since one can quotient C by one of the extra involutions and obtain a nonconstant map onto an elliptic curve E; an application of proposition 2.2.1 shows that this extends to a surjection $J \to E$.

Further, we can determine the effect of the canonical Rosati involution on the image of $\mathrm{Aut}(C)$ in $\mathrm{End}(J)$.

Lemma 2.5.1 *Let $u \in \mathrm{Aut}(C)$. Then $\tilde{u}^\dagger = \tilde{u}^{-1}$.*

Proof Let $P \in C(\overline{k})$ be a fixed point for u. Then let D be the image of $f^P\colon C \to J$. Then the canonical principal polarization on J is

$$\varphi_D\colon a \mapsto [t_a^* D - D],$$

where $t_a\colon J \to J$ is translation by a.

Then we can calculate

$$\tilde{u}^\vee \circ \varphi_D : a \mapsto [\tilde{u}^* t_a^* D - \tilde{u}^* D] = [\tilde{u}^* t_a^* D - D]$$
$$\text{and } \varphi_D \circ \tilde{u}^{-1} : a \mapsto [t^*_{\tilde{u}^{-1}(a)} D - D].$$

But $\tilde{u}\left(t^*_{\tilde{u}^{-1}(a)} D\right) = t_a^*\left(\tilde{u}(D)\right) = t_a^* D$, so $\varphi_D \circ \tilde{u}^{-1} = \tilde{u}^\vee \circ \varphi_D$. □

Given a curve C with RM by a real quadratic field F, we shall often make the hypothesis that the action of F is fixed by the Rosati involution. At first sight, one might suppose that this is always true because of the following well-known result.

Lemma 2.5.2 *Let F be a totally real number field, and let $\dagger$ be a positive involution on F. Then $\dagger$ is the identity.*

Proof Let $\alpha \in F$, and consider $\beta = \alpha - \alpha^\dagger$. We have that $\beta^\dagger = -\beta$, and so

$$0 \leqslant \mathrm{Tr}_{F/\mathbb{Q}}(\beta\beta^\dagger) = -\mathrm{Tr}_{F/\mathbb{Q}}(\beta^2) \leqslant 0,$$

using that $\dagger$ is positive and that F is totally real. Thus $\beta = 0$; that is, $\alpha = \alpha^\dagger$. □

The reason we may not be able to apply this result is that the endomorphism algebra of $\mathrm{Jac}(C)$ may contain more than one copy of F, these being permuted by the Rosati involution.

In fact, we often also assume that "everything in sight" is defined over k, and moreover are most interested in the case $k = \mathbb{Q}$. A sensible hypothesis, which would ensure that the RM by F is fixed by the Rosati involution, is to assume that the part of the endomorphism algebra defined over k is exactly equal to F; under this hypothesis, the Rosati involution would preserve F since it must preserve the property of definition over k. Indeed, when $k = \mathbb{Q}$ and we take the abelian surface A to be a Shimura factor associated with a modular form f with the field of real multiplication F equal to the field generated by the Fourier coefficients of f, then this hypothesis is true [Rib80, corollary 4.2].

For simple Jacobians, we can characterize when a real multiplication is fixed by the involution $\dagger$.

Proposition 2.5.3 *Let C be a curve of genus 2 and write $J = \mathrm{Jac}(C)$. Suppose that J is simple and that there is an embedding $i\colon \mathbb{Q}(\alpha) \hookrightarrow \mathrm{End}^0(J)$, where $\alpha^2 \in \mathbb{Q}_{>0}$. Then $\mathrm{im}(i) \subseteq \mathrm{End}^0(J)^{\dagger=1}$ if and only if one of the following is satisfied:*

(i) $\mathrm{End}^0(J)$ *is commutative;*

(ii) $\mathrm{End}^0(J)$ *is quaternionic and* $(C \cdot i(\alpha)^*C) = 2\alpha^2$.

Proof If (i) holds then $\dagger$ induces a positive involution on $i(\mathbb{Q}(\alpha))$ because $\mathrm{End}^0(J)$ contains only two roots of the minimal polynomial of α. But $\mathbb{Q}(\alpha)$ is totally real and so the induced involution must be the identity by lemma 2.5.2.

If (i) fails and J is simple then $\mathrm{End}^0(J)$ must be quaternionic, and $\dagger\colon \alpha \mapsto \delta^{-1}\overline{\alpha}\delta$ for some δ such that $\delta^2 \in \mathbb{Q}_{<0}$, where the bar denotes the canonical involution. (See [Shi63, §1].)

Now [Mil86a, Theorem 17.3] gives that $(C \cdot i(\alpha)^* C) = \mathrm{Tr}(\alpha\alpha^\dagger)$, where Tr denotes the reduced trace over $\mathbb{Q}$, and so we wish to show that $\alpha = \alpha^\dagger$ if and only if $\mathrm{Tr}(\alpha\alpha^\dagger) = 2\alpha^2$. (One implication is easy, of course.)

Note that $\alpha^2 \in \mathbb{Q}$ implies that $\overline{\alpha} = -\alpha$; likewise for δ. Hence

$$\begin{aligned} \alpha\alpha^\dagger &= \alpha\delta^{-1}\overline{\alpha}\delta \\ &= -\frac{1}{\delta^2}\alpha\delta\alpha\delta \\ \text{and } \mathrm{Tr}(\alpha\alpha^\dagger) &= -\frac{1}{\delta^2}(\alpha\delta\alpha\delta + \delta\alpha\delta\alpha). \end{aligned}$$

But $(\alpha\delta\alpha\delta + \delta\alpha\delta\alpha) = (\alpha\delta + \delta\alpha)^2 - 2\alpha^2\delta^2$, so that $\mathrm{Tr}(\alpha\alpha^\dagger) = 2\alpha^2$ if and only if $(\alpha\delta + \delta\alpha) = 0$. Finally, $\alpha - \alpha^\dagger = \alpha + \delta^{-1}\alpha\delta = \delta^{-1}(\delta\alpha + \alpha\delta)$, whence the result. □

Lastly for this section, we show that, up to isogeny, we may suppose that a given real multiplication is maximal. This justifies us in looking only for curves with an action of the full ring of integers $\mathbb{Z}[\eta] \subset \mathbb{Q}(\sqrt{5})$.

Proposition 2.5.4 *Let F be a number field, and let R and R' be orders in F. Let A/k be an abelian variety with an embedding $i\colon R \hookrightarrow \mathrm{End}_k(A)$. Then there is an abelian variety B/k and an isogeny $\pi\colon A \to B$ defined over k such that $R' \hookrightarrow \mathrm{End}_k(B)$.*

Proof Let $n = [R' : R]$, so that $nR' \subseteq R \subseteq R'$. We shall take $B = A/G$, where G is the finite subgroup $(nR') \cdot A[n^2]$ of A, and let $\pi\colon A \to B$ be the associated isogeny. Now for any $\varepsilon \in R'$, we can attempt to define an action of ε on B by fitting the missing arrow to the square

$$\begin{array}{ccc} A & \xrightarrow{n\varepsilon} & A \\ {\scriptstyle n\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ B & \overset{\varepsilon}{\cdots\cdots\rightarrow} & B \end{array}$$

such that the resulting diagram commutes.

To check that this is well-defined, we need to show that $a \in \ker(n\pi)$ implies $(n\varepsilon) \cdot a \in \ker \pi$. So, let $a \in \ker(n\pi)$, and put $x = (n\varepsilon) \cdot a$. Then

$$nx = (n\varepsilon) \cdot na \in (n\varepsilon) \cdot G \subseteq n \cdot G$$

$$\implies x \in G + A[n] = G + n \cdot A[n^2] = G.$$

The subgroup G is defined over k since the action of R on A is defined over k, and so B and π are defined over k. Given $\varepsilon \in R'$ and $\sigma \in G_k$, one can readily check that ε and ${}^{\sigma}\varepsilon$ agree on $B(\overline{k})$. Hence the action of R' on B is defined over k. □

Our claim that a given real multiplication may be made maximal after isogeny follows as an immediate corollary from this proposition.

Notice that if A were naturally principally polarized (a Jacobian, for example) it is not clear whether this process gives us a principal polarization on B as well. We return to this question in chapter 4, where we prove that if A is a principally polarized abelian *surface* and if $n = [R' : R]$ is odd, then B can indeed also be taken to be principally polarized.

2.6 Fields of definition for endomorphisms

Suppose A is a simple abelian surface defined over a number field k. Then, certainly, the action of $\mathbb{Z}$ on A is always defined over k. We shall also see that there are examples where A has real multiplication defined over k even if $k = \mathbb{Q}$; our aim in this section is to show that when $k = \mathbb{Q}$ then $\mathrm{End}^0_{\mathbb{Q}}(A)$ is always either $\mathbb{Q}$ or a quadratic field (although the full endomorphism algebra $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A)$ may well be larger than this). We do not claim that $\mathrm{End}^0_{\mathbb{Q}}(A)$ is always a *real* field. Cardona *et al.* have found examples with $\mathrm{End}^0_{\mathbb{Q}}(A) = \mathbb{Q}(\sqrt{-3})$ [CGLR98]; these examples are isogenous to the square of an elliptic curve over $\overline{\mathbb{Q}}$, but it may be possible to construct examples with $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A)$ equal to a quaternion algebra and $\mathrm{End}^0_{\mathbb{Q}}(A)$ equal to a quadratic imaginary field.

Proposition 2.6.1 *Let A be an abelian variety of dimension g defined over a number field k. Then there is an embedding $\mathrm{End}^0_k(A) \hookrightarrow \mathrm{M}_g(k)$.*

Proof It is sufficient to prove this for k-simple abelian varieties, for if A is isogenous over k to a product $\prod_{i=1}^{n} A_i^{r_i}$ of abelian varieties A_i defined over k then $\mathrm{End}_k^0(A) \cong \bigoplus_{i=1}^{n} \mathrm{M}_{r_i}\left(\mathrm{End}_k^0(A_i)\right)$. Thus we may assume that all nonzero endomorphisms of A defined over k are isogenies.

Let $\alpha \in \mathrm{End}_k(A)$. Then α induces a k-linear map α^* on the invariant differentials defined over k. These form a g-dimensional vector space dual to the tangent space at 0 [Sha74, chapter III §5.2]. Further, α^* is an embedding when α is nonzero [Sha74, chapter III §5.1]. Thus we have an embedding $\mathrm{End}_k(A) \hookrightarrow \mathrm{M}_g(k)\colon \alpha \mapsto \alpha^*$. This extends to an embedding of $\mathrm{End}_k^0(A)$ since $\mathrm{End}_k(A)$ is a free $\mathbb{Z}$-module [Mil86a, theorem 12.5]. □

Corollary 2.6.2 *For a simple abelian surface A defined over $\mathbb{Q}$, the algebra $\mathrm{End}_{\mathbb{Q}}^0(A)$ is either $\mathbb{Q}$ or a quadratic field.*

Proof The only other choices for $\mathrm{End}_{\mathbb{Q}}^0(A)$ are a quaternion algebra or a quartic CM field (see section 2.5). However it follows from the proposition that $\dim_{\mathbb{Q}}\left(\mathrm{End}_{\mathbb{Q}}^0(A)\right) = 4$ if and only if $\mathrm{End}_{\mathbb{Q}}^0(A) = \mathrm{M}_2(\mathbb{Q})$. □

For an elliptic curve $E/\mathbb{Q}$, the corresponding corollary is that $\mathrm{End}_{\mathbb{Q}}^0(E) = \mathbb{Q}$ (compare with [Sil94, theorem II.2.2(a)]).

2.7 Reduction at a prime

In this section we look at the reduction modulo a prime of a curve of genus 2 and its Jacobian. We make a few definitions to start.

Let p be a prime, let K be a finite extension of $\mathbb{Q}_p$ and let R be the ring of integers of K. We say that a variety X over K has *good reduction* if it extends to a smooth R-scheme $\mathscr{X}$. The variety is said to have *bad reduction* otherwise. In the case that X is defined over a number field K, with ring of integers R, we say that X

has good reduction at a prime π of R if $X \otimes_K K_\pi$ has good reduction, where K_π is the completion of K at π.

Let us from now on suppose that K is a number field and that R is the ring of integers of K. In the case of a curve C/K then we can find a proper regular R-model $\mathscr{C}$ for C, and indeed one with the following property: whenever $\mathscr{C}'$ is a proper regular R-model for C then the K-isomorphism $\mathscr{C}' \otimes_R K \to C$ extends to an R-isomorphism $\mathscr{C}' \to \mathscr{C}$. Such a model is called a *minimal model* for C. It can be constructed from a proper regular model by contracting all exceptional divisors, that is, divisors which have arithmetic genus 0, self-intersection -1 and which lie in a fibre over a closed point. (See [Chi86] for the details.)

In the case of an abelian variety X/K, a nice R-model is given by the *Néron model* $\mathscr{N}(X)/R$, which is defined by the following universal property: if $\mathscr{X}$ is a smooth R-scheme and $\phi\colon \mathscr{X} \otimes_R K \to X$ is a rational map of K-schemes, then ϕ extends uniquely to a morphism $\phi_R\colon \mathscr{X} \to \mathscr{N}(X)$ of R-schemes. Essentially, a Néron model must be large enough so that every K-point of X extends to an R-point of $\mathscr{N}(X)$, but small enough that the group structure on X extends to a group structure on $\mathscr{N}(X)$. That Néron models exist is a theorem of Néron himself [Nér64], and a construction in scheme language can be found in [Art86]; the most complete account is the book by Bosch, Lütkebohmert and Raynaud [BLR90], and Silverman gives a very readable account for the case of elliptic curves in [Sil94].

For an elliptic curve E, we can observe that the minimal model $\mathscr{E}$, regarding E as a curve, and the Néron model $\mathscr{N}(E)$, regarding E as an abelian variety, are linked in a simple way: $\mathscr{N}(E) = \mathscr{E}^0$, the smooth locus of $\mathscr{E}$ [Sil94, Theorem IV.6.1]. Similar, but rather more complicated, connexions exist between the minimal model of a curve C of higher genus and the Néron model of the Jacobian of C. We elucidate one such below.

We are, of course, primarily interested in these concepts applied to a curve of genus 2 and to its Jacobian. For an elliptic curve, the configuration of the special fibre of a minimal model is well known (see, for example [Sil94, table 4.1, page 365]). For the

case of a curve of genus 2, Ogg [Ogg66] has classified the possible configurations on the special fibre of a minimal model using a numerical argument. This classification was completed, using more geometrical arguments, by Namikawa and Ueno [Nam73], who list more than 100 cases. More recently, Liu [Liu94] has determined an algorithm to give the type of the special fibre when the residue characteristic is greater than 2.

If a curve C has good reduction at a prime π, then it follows that the Jacobian $J(C)$ also has good reduction because the generalized Jacobian $\mathscr{J}$ of a smooth integral model $\mathscr{C}$ has generic fibre J and is smooth—see [Mil86b, Corollary 12.3]. The converse is not true, however. It is known that Jacobians are never isomorphic to products of principally polarized abelian varieties although they may be *isogenous* to such a product (this is remarked, for instance, in [Maz77, proof of proposition 10.6]), so if J has good reduction as a product of abelian varieties, then we expect that the associated curve should reduce badly, but in a controlled fashion. The result for curves of genus 2 is the following.

Proposition 2.7.1 *Let R be the ring of integers of a number field K, and let π be a prime of R; write k for the finite field R/π. Let C be a curve of genus 2 over K, and let $J = \mathrm{Jac}(C)$. Then J has good reduction at π if and only if the curve has an R-model $\mathscr{C}$ such that the reduction $\mathscr{C}_\pi$ is of one of the following types:*

(i) *a smooth curve of genus 2 over k, or*

(ii) *the union of two elliptic curves E_1, E_2 and m rational curves (where $m \geqslant 0$) with configuration as in figure 2.1, where all the components appear with multiplicity 1 and the intersection multiplicities are 1 or 0.*

Proof From the definition of good reduction, we may replace K with K_π and R with the ring of integers of K_π.

If C has good reduction, then let $\mathscr{C}/R$ be a smooth model, and let $\mathscr{J}$ be the generalized Jacobian as defined in [Mil86b, §8]. Then, as remarked above, $\mathscr{J}$ is an abelian scheme over R with generic fibre J, and so J has good reduction.

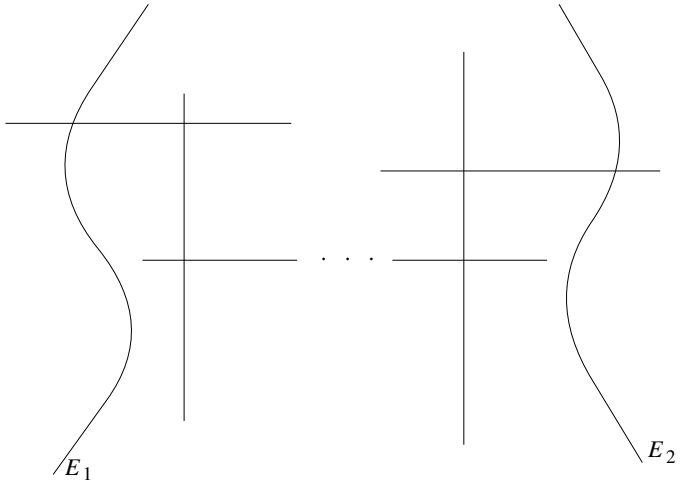


Figure 2.1: A configuration on the special fibre of a curve of genus 2 (refer to proposition 2.7.1). The components appear with multiplicity 1 and all intersection multiplicities are 1 or 0.

If C has an R-model $\mathscr{C}$ where the special fibre $\mathscr{C}_\pi$ is as in (ii), then we can still conclude that $\mathrm{Pic}^0(\mathscr{C}/R)$ is the identity component of a Néron model for J, because each component of $\mathscr{C}_\pi$ appears with multiplicity 1 [BLR90, §9.5, Theorem 4]. Further, the group of connected components $\mathscr{N}(J)/\mathscr{N}(J)^0$ of the Néron model of J is trivial by [BLR90, §9.6, Proposition 10], and so we have $\mathscr{N}(J) = \mathrm{Pic}^0(\mathscr{C})$. Hence the special fibre of $\mathscr{N}(J)$ is $\mathrm{Pic}^0(\mathscr{C}_\pi) \cong E_1 \times E_2$, and we conclude that J has good reduction (as a product of elliptic curves).

The converse takes a little more care. Let us suppose that J has good reduction. Then any smooth proper R-model for J is a Néron model for J—this follows from the valuative criterion for properness and the fact that rational maps from nonsingular varieties to abelian varieties are everywhere defined. Let $\mathscr{C}$ denote a minimal model for C. In what follows, we shall make use of several arguments from [Ogg66].

The arithmetic genus of the special fibre $\mathscr{C}_\pi$ is given by the formula $p_a(\mathscr{C}_\pi) = 1 + \frac{1}{2}\Big((\mathscr{C}_\pi^2) + (\mathscr{C}_\pi \cdot \kappa)\Big)$, where κ is a canonical divisor on $\mathscr{C}$, and this is equal to 2. But $\mathscr{C}_\pi$ is algebraically equivalent to the generic fibre C, and so $(\mathscr{C}_\pi \cdot \Gamma) = 0$ for any divisor Γ on $\mathscr{C}$ contained in $\mathscr{C}_\pi$. Hence $(\mathscr{C}_\pi \cdot \kappa) = 2$.

Suppose that $\mathscr{C}_\pi$ were nonreduced: $\mathscr{C}_\pi = n\Gamma$, say, with $n > 1$. Then we would have that $(\Gamma \cdot \kappa) = 2/n$ and so $p_a(\Gamma) = 1 + (1/n)$, which is not an integer. Hence $\mathscr{C}_\pi$ is reduced. We can conclude that $\mathrm{Pic}^0(\mathscr{C}) = \mathscr{N}(J)^0$, by [BLR90, §9.5, Theorem 4]. Further, $\mathscr{C}_\pi$ has smooth components and the configuration of the geometric components is tree-like by [BLR90, §9.2, Corollary 12].

Let Γ be a component of $\mathscr{C}_\pi$. Note that there is a map $\mathscr{N}(J)_\pi \to \mathrm{Pic}^0(\Gamma)$ by functoriality, and so we must have $p_a(\Gamma) \leqslant 2$.

Now write $\mathscr{C}_\pi = \Gamma + D$, where D is an effective divisor such that Γ does not appear in D. (We allow $D = 0$.) Since the special fibre is connected, we have $(D \cdot \Gamma) \geqslant 0$ with equality if and only if $D = 0$. Therefore $(\Gamma^2) \leqslant (\mathscr{C}_\pi \cdot \Gamma) = 0$, with equality exactly when $D = 0$. We also have $(\Gamma \cdot \kappa) = 2p_a(\Gamma) - 2 - (\Gamma^2)$; if $D \neq 0$ then this gives $(\Gamma \cdot \kappa) \geqslant -1$. Recall that $\mathscr{C}$ is a minimal model, and has no exceptional divisors. Thus we conclude that for every component Γ of $\mathscr{C}_\pi$ we have $(\Gamma \cdot \kappa) \geqslant 0$.

Suppose now that $\mathscr{C}_\pi = \Gamma + D$ as before, and that $p_a(\Gamma) = 2$. Then $(\mathscr{C}_\pi \cdot \kappa) = 2 = (\Gamma \cdot \kappa)$, and so $(D \cdot \kappa) = 0$, whence $D = 0$ by the previous paragraph. Thus we can conclude that if any component of the special fibre has genus 2, then the special fibre is irreducible, and is a smooth curve of genus 2.

From now on suppose that all components of $\mathscr{C}_\pi$ have genus 0 or 1. In order that $p_a(\mathscr{C}_\pi) = 2$ and that $\mathrm{Pic}^0(\mathscr{C}_\pi)$ is 2-dimensional, we can use similar arguments to conclude that $\mathscr{C}_\pi = \sum_{i=1}^{m+2} \Gamma_i$, with

$$(\Gamma_1^2) = (\Gamma_2^2) = -1,\ (\Gamma_1 \cdot \kappa) = (\Gamma_2 \cdot \kappa) = 1,\ p_a(\Gamma_1) = p_a(\Gamma_2) = 1$$

$$\text{and } (\Gamma_i^2) = -2,\ (\Gamma_i \cdot \kappa) = 0,\ p_a(\Gamma_i) = 0 \text{ for } i \geqslant 3.$$

(In Ogg's notation, we have two distinct components of type A and every other component is of type E.)

Put $D = \sum_{i=3}^{m+2} \Gamma_i$. (When $m = 0$ this means $D = 0$.) Note that $(\mathscr{C}_\pi \cdot D) = 0$ and that $(\mathscr{C}_\pi^2) = 0$, and so

$$(\Gamma_1 \cdot D) + (\Gamma_2 \cdot D) + 2(\Gamma_1 \cdot \Gamma_2) = 2.$$

Now, using that $\mathscr{C}_\pi$ is connected and that the configuration of the components is tree-like it is straightforward to see that $\mathscr{C}_\pi$ must be as in case (ii) of the statement. □

The configuration in (ii) of the proposition is type 13 in [Ogg66], and type [I_0-I_0-m] (page 158) in [Nam73].

2.8 The conductor of an abelian variety

Now we come to the definition of an important invariant of an abelian variety, namely the *conductor*. There are several different equivalent definitions in use: the one we give is taken from [LRS93]; the first definition in this generality was given by Serre and Tate [ST68].

Let p be a prime, let $K/\mathbb{Q}_p$ be a finite extension, and let A/K be an abelian variety. Fix an auxiliary prime ℓ distinct from p and from 2, and set $L = K\left(A[\ell]\right)$. Denote by G_i the ith inertia group of L/K, that is

$$G_i = \{\sigma \in \mathrm{Gal}(L/K) \mid v\left({}^\sigma\pi - \pi\right) \geqslant i+1\},$$

where π is a uniformizer for L and $v\colon L^\times \to \mathbb{Z}$ is the normalized valuation on L; write g_i for the order of G_i.

Then the *exponent of the conductor of* A/K is defined to be

$$f(A/K) = \sum_{i\geqslant 0} \frac{g_i}{g_0} \dim_{\mathbb{F}_\ell}\left(A[\ell]/A[\ell]^{G_i}\right).$$

We note that although this is not clear *a priori*, $f(A/K)$ is an integer, and independent of the choice of ℓ.

If A is an abelian variety over a number field k, we shall define the conductor of A/k to be the product of local factors

$$\prod_{\text{primes } \mathfrak{p}} \mathfrak{p}^{f_\mathfrak{p}}, \text{ where } f_\mathfrak{p} = f\left(A \otimes k_\mathfrak{p}/k_\mathfrak{p}\right).$$

Also, if C/k is a curve, then we shall define the conductor of C to be the conductor of the abelian variety $\mathrm{Jac}(C)/k$.

A few remarks are in order. First, when A/K is an elliptic curve, then the exponent $f(A/K)$ has a well-known simple description (see, for example [Sil94, theorem IV.10.2]). Indeed, in any dimension, the exponent $f(A/K) = 0$ if and only if A/K has good reduction.

Secondly, the definition of the conductor does not lend itself to direct calculation. To be able to calculate it, one must relate the definition more nearly to the geometric situation. Tate's algorithm will do this for elliptic curves (see, for example, [Sil94, chapter IV, §9]), and Liu [Liu94] has produced an algorithm which will compute the odd part of the conductor of a curve of genus 2; he has encoded this as the program `genus2reduction`.

It is also worth noting that when $A/\mathbb{Q}$ is an abelian variety of dimension g with RM defined over $\mathbb{Q}$, then the conductor of A is a gth power. Further, if A is a modular abelian variety, associated with a newform of level N, then it is known by work of Deligne, Langlands and Carayol that the conductor of A is N^g (see [Car86, theorem A]).

As a last remark, we observe that the problem of computing the conductor of a curve of genus 2 at the prime 2 still seems not to be completely solved. We can at least check (in an *ad hoc* manner) whether a curve has good reduction at 2. It is sometimes also possible to check the criterion of proposition 2.7.1 for good reduction of the Jacobian at 2, that is to say, to check whether the curve has an odd conductor.

2.9 Poncelet's theorem

The theorem of this section is a rather beautiful classical result in projective geometry. What is of use to us is the method of proof given by Griffiths and Harris [GH77].

Consider the following. Let Q and R be (distinct) plane conics. For simplicity, we shall assume that Q and R meet in four distinct points; the theorem below is still true without this assumption. Then the first step is to define a correspondence

on Q by taking tangents to R. To be precise, let P be a point of Q; then there are (generically) two tangents to R which pass through P. We shall denote the residual points of intersection of these tangents with Q by P_+ and P_- (refer to figure 2.2). Notice that there is an implicit choice of a positive direction here: this is arbitrary, but will need to be consistent in what follows.

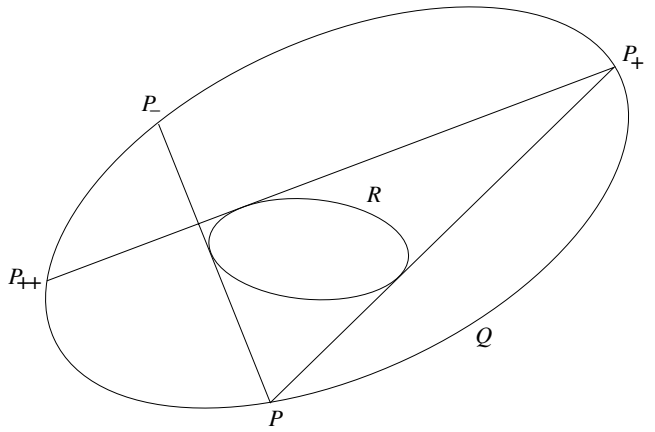


Figure 2.2: The correspondence $P \mapsto \{P_+, P_-\}$

Now for any point P on Q we can construct a sequence of points (P_n) by

$$P_0 := P \text{ and } P_{n+1} = (P_n)_+ \text{ for each } n \geqslant 0.$$

With this notation, we can state the result as follows.

Theorem 2.9.1 (Poncelet's theorem) *Suppose that $n \geqslant 3$ is an integer such that for some point P of Q we have $P_n = P$. Then $P_n = P$ for* every *point P on Q.*

In words, if there is one n-gon inscribed to Q and circumscribed to R, then for every point P on Q there is such an n-gon with a vertex at P.

Now we summarize the proof in [GH77]. The key step is to introduce the *incidence relation* E between Q and the projective dual R^*, that is,

$$E = \{(P, L) \in Q \times R^* \mid P \text{ lies on } L\}.$$

Both Q and R^* are (geometrically) isomorphic to $\mathbb{P}^1$, and the condition defining E gives one algebraic equation, so E is an algebraic curve in $\mathbb{P}^1 \times \mathbb{P}^1$. There are two natural 2–1 maps $\pi_1 \colon E \to Q$ and $\pi_2 \colon E \to R^*$; the map π_1 branches over the intersection points of Q and R and the map π_2 branches over $Q^* \cap R^*$. Any point of E which is not a ramification point for π_1 is nonsingular, and the same holds for π_2. But the assumption that Q and R meet in four distinct points ensures that π_1 and π_2 have no common ramification points, and we conclude that E is nonsingular.

The curve E has genus 1 by the Hurwitz genus formula, so we are able to use some of the theory of elliptic curves. There are two natural involutions ι_1 and ι_2 on E, given by exchanging the branches of the maps π_1 and π_2. Consider the lifiting of ι_1 and ι_2 to the universal cover of E. Each of the involutions ι_1 and ι_2 is the composition of a homomorphism with a translation; since neither of these maps is the identity, but each has fixed points, each one is of the form $P \mapsto -P + Q$ (for some Q). The composition $\iota_1 \circ \iota_2$ is then translation by a fixed point T, say, of E.

If the point $P \in Q$ lies under the point $\tilde{P} \in E$, then P_+ lies under $\tilde{P} + T$. Indeed, for each n, the point P_n lies under $\tilde{P} + nT$. Since we know $P_n = P$ for some $n \geqslant 3$, this forces $nT = 0$ on E. But the value of T is independent of the choice of P, and so the result follows immediately.

Chapter 3

Humbert's criterion

In [Hum99], the author describes the relations satisfied by the period matrix of an abelian surface with real multiplication by $\mathbb{Q}(\sqrt{d})$, and gives a geometric description of when these relations are satisfied. A translation to more modern language can be found in [vdG88, ch. IX]. We offer a proof of Humbert's geometric criterion for real multiplication in $\mathbb{Q}(\sqrt{5})$ following van der Geer [vdG88, *loc. cit.*] and Jakob [Jak94].

3.1 Humbert's criterion for RM by $\mathbb{Q}(\sqrt{5})$

Throughout the sequel, suppose C is a curve of genus 2 (defined over some algebraically closed field k of characteristic 0), write $J = \mathrm{Jac}(C)$ and K for the *Kummer surface* $J/\langle -1 \rangle$. Then J has a canonical principal polarization λ. We denote by $\dagger$ the associated Rosati involution on $\mathrm{End}(J)$ and write $\mathrm{End}(J)^{\dagger=1}$ for the subring fixed by $\dagger$. Further, choose an image D of C on J (so that D is an ample effective divisor giving the polarization λ) which is symmetric, that is, $(-1)^*D = D$. The Riemann–Roch theorem implies that $(D^2) = 2$.

The following proposition collects together several classical results about the geometry of the Kummer surface K, proofs of which can be found in [Gon94]. (The classic reference for this material is [Hud05].)

Proposition 3.1.1 *The map defined by the linear system $|2D|$ on J factors through*

the projection $J \to K$ and defines an embedding of K into $\mathbb{P}^3$ as a quartic hypersurface with sixteen nodes as its only singularities. These nodes are the images of $J[2]$.

There are sixteen planes termed the singular planes *such that each singular plane contains six of the nodes of K and each node is contained in six of the singular planes; furthermore the six singular planes containing a node are tangent to K at their other points of intersection with K, and cut out sixteen conics on K, termed the* singular conics*, which are the images of translates of D by points of $J[2]$.*

The surface K is projectively self-dual, and under this duality, the singular planes and singular conics are dual to one another. □

Now we do a little preparation for a proof of Humbert's criterion.

Proposition 3.1.2 *Let d be a squarefree integer such that $d \equiv 5 \pmod 8$. Write $d = 8t + 5$ and let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Then there is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(J)^{\dagger=1}$ if and only if there is a curve E on K of genus $2t(t+1)$ and degree $4t+3$ which passes through six of the nodes on K.*

Proof Suppose first that $\varepsilon \in \mathrm{End}(J)^{\dagger=1}$ satisfies $\varepsilon^2 + \varepsilon - (2t+1) = 0$, and put $H = \varepsilon^* D$. Then $(H^2) = \deg(\varepsilon)(D^2) = 2(2t+1)^2$, and so $p_a(H) = (2t+1)^2 + 1$.

Let E be the image of H on K. The endomorphism ε acts as an isomorphism on $J[2]$, so $\#(H \cap J[2]) = \#(D \cap J[2]) = 6$, and hence E passes through six of the nodes on K. Moreover, the Hurwitz genus formula implies that E has genus $2t(t+1)$.

The degree of E is given by the intersection number $(D \cdot H)$ on J (since the map $J \to K$ is defined by $|2D|$ and is a degree 2 map). But by [Mil86a, Theorem 17.3], $(D \cdot H) = \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\varepsilon^2) = 4t + 3$. This concludes the "only if" part.

Conversely, suppose that E is a curve on K as in the statement, and let H be the preimage of E on J. Then $(H^2) = 2(2t+1)^2$, and $(D \cdot H) = 4t + 3$.

Put $\varepsilon = \lambda^{-1} \circ \phi_{\mathscr{L}(H)} \in \mathrm{End}(J)^{\dagger=1}$ (cf. [Mil86a, proposition 17.2]). Then $\varepsilon^\dagger = \varepsilon$, and so, by [Lan86, lemma 2.3], ε satisfies the equation

$$\varepsilon^2 - (D \cdot H)\varepsilon + \frac{1}{2}(H^2) = 0.$$

Thus $\frac{1}{2}(1+\sqrt{d}) \mapsto \varepsilon - (2t+1)$ defines an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(J)^{\dagger=1}$. □

Now the last step is to convert the criterion of proposition 3.1.2 into something more appealing, as in the following.

Theorem 3.1.3 (Humbert's criterion) *Suppose that π is a map of C onto a plane conic Q with branch points P_1, P_2, P_3, P_4, P_5 and P_6. Then there is an embedding $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$ if and only if for some ordering of the branch locus there is a plane conic R passing through P_6 which is tangent to each of the edges of the pentagon $P_1P_2P_3P_4P_5$.*

Proof Suppose first that there is an embedding i as in the statement. Then proposition 3.1.2 tells us that there is a rational cubic curve E on K which passes through six of the nodes of K. Label these nodes P_0, P_1, P_2, P_3, P_4 and P_5, and project through P_0 to $\mathbb{P}^2$.

The image of E is a plane conic which is tangent to each of the six lines which are the intersections of the singular planes through P_0 with $\mathbb{P}^2$. This conic also passes through the five points which are the intersections of the lines P_0P_i with $\mathbb{P}^2$.

Taking the projective dual gives the configuration of the statement.

Given the configuration of the statement, Jakob [Jak94, §1] shows how to recover the Kummer surface K and Jacobian J. We let $\psi\colon X \to \mathbb{P}^2$ be the double cyclic cover branched over the lines $P_1P_2, P_2P_3, P_3P_4, P_4P_5, P_5P_1$ and the tangent to R at P_6. Then Jakob proves that $\psi^{-1}(R)$ splits into two smooth rational curves on X and that the Kummer surface can be recovered by a map $\xi\colon X \to K$ which blows down one component of $\psi^{-1}(R)$. This gives a rational curve E on K; let H be the preimage of E on J. Jakob further proves that $(H \cdot D) = 3$ and H has genus 2 so E is a curve as in (3.1.2). □

In the sequel, by an *Humbert configuration* we shall mean a configuration as in theorem 3.1.3, that is a tuple $(Q, R; P_1, \ldots, P_6)$ consisting of two plane conics Q and

R and six points $P_1, \ldots, P_6$ on Q such that R passes through P_6 and is tangent to the edges of the pentagon $P_1P_2P_3P_4P_5$. If we say that an Humbert configuration $(Q, R; P_1, \ldots, P_6)$ is an *Humbert configuration for the curve* C, we mean that C is a double cover of Q branched over $P_1, \ldots, P_6$.

It is not immediate on a first reading of theorem 3.1.3 and its proof that the real multiplication constructed from the Humbert configuration is necessarily the same as that which gives rise to the Humbert configuration. This is the case, as we can check from the following proposition, which gives us a criterion we also use later on. As before, we choose some image D of C on J which induces the canonical principal polarization.

Proposition 3.1.4 *Suppose that* $\varepsilon, \theta \in \mathrm{End}^0(J)$ *both satisfy* $f(T) = T^2 - \sigma_1 T + 1 = 0$, *where* $\sigma_1 \in \mathbb{Q} \setminus \{0\}$ *and* f *is irreducible, and that* $\varepsilon^\dagger = \varepsilon$.

Then $\varepsilon^* D = \theta^* D$ *implies that* $\varepsilon = \theta$.

Proof Recall the definition of the embedding $\mathrm{Aut}(C) \to \mathrm{End}(J) \colon u \mapsto \tilde{u}$ given before lemma 2.5.1.

Note that ε and θ are invertible. Then, certainly $\varepsilon^* D = \theta^* D$ implies that $\theta = \varepsilon\tilde{u}$ for some $u \in \mathrm{Aut}(C)$. We now make use of the classification of $\mathrm{Aut}(C)$ given in section 2.5. In particular, we know that u has finite order.

If $\mathrm{Aut}(C)^{\mathrm{red}}$ is trivial then the result is clear.

If $\mathrm{Aut}(C)^{\mathrm{red}} \cong \mathrm{C}_5$ then $\mathrm{End}^0(J) = \mathbb{Q}(\zeta_5)$ (where ζ_5 is a primitive 5^{th} root of 1), so ε and θ are elements of the unique quadratic subfield $\mathbb{Q}(\eta) \subset \mathbb{Q}(\zeta_5)$. Hence u is a fifth root of unity in $\mathbb{Q}(\eta)$ and thus $u = 1$.

In all other cases, J is isogenous to a product of elliptic curves. Indeed, J must be isogenous to the square of an elliptic curve E, for suppose otherwise that J is isogenous to $E_1 \times E_2$, where E_1 and E_2 are not isogenous. Then $\mathrm{End}^0(J) = \mathrm{End}^0(E_1) \oplus \mathrm{End}^0(E_2)$ and so each of $\mathrm{End}^0(E_1)$ and $\mathrm{End}^0(E_2)$ must contain roots of $f(T)$ (since $\mathrm{End}^0(E_i)$ is contained in $\overline{\mathbb{Q}}$). Hence (if this is possible) E_1 and E_2 both have CM by the same quadratic field, so are isogenous, contradicting the assumption.

There is, then, an isomorphism $\mathrm{End}^0(J) \cong \mathrm{M}_2(K)$, where $K = \mathrm{End}^0(E)$, such that the Rosati involution becomes

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\dagger = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix},$$

where $\overline{\ }$ denotes complex conjugation.

Under this isomorphism, write $\tilde{u} = (u_{ij})$ and $\varepsilon = (\varepsilon_{ij})$. Then we need to satisfy:

(i) $\det(\varepsilon\tilde{u}) = \det(\varepsilon)$, that is $\det(\tilde{u}) = 1$;

(ii) $\mathrm{Tr}(\varepsilon\tilde{u}) = \mathrm{Tr}(\varepsilon) = \sigma_1$;

(iii) $\tilde{u}^\dagger = \tilde{u}^{-1}$ (because of lemma 2.5.1);

(iv) $\varepsilon^\dagger = \varepsilon$.

Conditions (i) and (iii) together give the equations $\overline{u}_{11} = u_{22}$, $\overline{u}_{12} = -u_{21}$ and $u_{11}\overline{u}_{11} + u_{12}\overline{u}_{12} = 1$. Given these, and condition (iv), we can write

$$\mathrm{Tr}(\varepsilon\tilde{u}) = \mathrm{Tr}(\varepsilon)u_{11} + (\overline{\varepsilon}_{12}u_{12} - \varepsilon_{12}\overline{u}_{12}) + \varepsilon_{22}(\overline{u}_{11} - u_{11}).$$

If we apply $\overline{\ }$ to this equation and add, then use condition (ii), we find that $2\sigma_1 = \sigma_1(u_{11} + \overline{u}_{11})$, so that $u_{11} + \overline{u}_{11} = 2$ (since $\sigma_1 \neq 0$).

Since $\overline{\ }$ is just complex conjugation, $u_{11} + \overline{u}_{11} = 2$ and $u_{11}\overline{u}_{11} + u_{12}\overline{u}_{12} = 1$ together imply $u_{11} = 1$ and $u_{12} = 0$.

This proves that $\tilde{u} = 1$ in $\mathrm{M}_2(K)$, and so $\theta = \varepsilon$. □

3.2 Humbert's criterion revisited

We can copy Humbert [Hum99] and make explicit the geometric criterion of theorem 3.1.3. Let us fix a little notation. We let C be a curve of genus 2 over a number field k. Suppose that C admits an Humbert configuration $(Q, R; P_1, \ldots, P_6)$, say, and then choose coordinates $(X : Y : Z)$ on $\mathbb{P}^2$ so that the conic Q which is covered by C has equation

$$Y^2 = XZ$$

(the image of the 2-uple embedding $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$). Suppose that the branch points $P_1, \ldots, P_6$ are given by $P_i = (a_i^2 : a_i : 1)$.

Notice that there is only one conic R which is tangent to the five lines P_1P_2, P_2P_3, P_3P_4, P_4P_5, P_5P_1, and so the condition is that this conic passes through P_6. In fact it is no difficult matter to write down the equation of the projective dual R^* (Maple V has a function for this task). If we take coordinates $(l : m : n)$ on the projective dual $\mathbb{P}^{2*}$ so that R^* has an equation

$$al^2 + bm^2 + cn^2 + 2dmn + 2enl + 2flm = 0$$

then the coefficients are

$$\begin{aligned}
a &= a_1a_2^2a_5^2(a_4^2 - a_3^2) + \cdots + a_5a_1^2a_4^2(a_3^2 - a_2^2),\\
b &= a_1^2a_2a_5(a_3 - a_4) + \cdots + a_5^2a_1a_4(a_2 - a_3),\\
c &= a_1^2(a_3 - a_4) + \cdots + a_5^2(a_2 - a_3),\\
2d &= a_1^2(a_2 + a_5)(a_3 - a_4) + \cdots + a_5^2(a_1 + a_4)(a_2 - a_3),\\
2e &= a_1^2(a_2^2 + a_5^2)(a_4^2 - a_3^2) + \cdots + a_5^2(a_1^2 + a_4^2)(a_3^2 - a_2^2),\\
2f &= a_1^2\left[a_3a_4(a_2^2 + a_5^2) + a_2a_5(a_3^2 - a_4^2)\right] + \cdots + a_5^2\left[a_2a_3(a_1^2 + a_4^2) + a_1a_4(a_2^2 - a_3^2)\right],
\end{aligned}$$

where on each line the missing terms are produced by cycling the suffices by the 5-cycle (1 2 3 4 5).

To obtain the condition that R passes through P_6 it is slightly more elegant to first consider the case when $P_6 = (1 : 0 : 0)$, in which case the condition is simply $bc = d^2$, and then to generalize by making the substitution $a_i \mapsto \dfrac{1}{a_i - a_6}$. We shall denote this condition by $H(a_1, \ldots, a_6)$.

An important fact from our point of view is that, while the group of permutations of the a_i which fix R is the symmetry group of the pentagon $P_1P_2P_3P_4P_5$ (that is $\mathrm{D}_{10} = \langle (1\ 2\ 3\ 4\ 5), (1\ 2)(3\ 4)\rangle$), the group of permutations in S_6 which fix H is rather larger. This subgroup is precisely the transitive copy of A_5 which is generated by (1 2 3 4 5) and (1 6)(2 5). We call this subgroup $\mathrm{A}_5^{\mathrm{tr}}$. This means that for each choice of branch point P_i, there is some conic R_i which passes through P_i and is tangent

to the pentagon formed by taking the other branch points in a specific order. (The equation above defines R_6.) We can retrieve this ordering because we know that for each $i = 1, \ldots, 6$ the group of symmetries of the pentagon formed by the branch points other than P_i is just the intersection of $\mathrm{A}_5^{\mathrm{tr}}$ with the stabilizer in S_6 of i.

We are now in a position to verify the following, which makes life a little simpler later on.

Lemma 3.2.1 *Let C be a curve of genus 2 which admits the Humbert configuration $(Q, R, \{P_i\})$. Then, after reordering the P_i, we may suppose that Q and R meet transversally in four points.*

Proof Our proof is a straightforward, if rather tedious, calculation, which was performed with the aid of Maple. As a point of notation, if p_1 and p_2 are multivariate polynomials we shall denote by $\mathrm{Res}(p_1, p_2; x)$ the resultant of p_1 and p_2 with respect to the variable x.

We may suppose up to isomorphism that Q has the equation $Y^2 = XZ$, and that the branch points of $C \to Q$ are $P_1 = (0 : 0 : 1)$, $P_2 = (1 : 1 : 1)$, $P_3 = (\lambda^2 : \lambda : 1)$, $P_4 = (\mu^2 : \mu : 1)$, $P_5 = (\nu^2 : \nu : 1)$ and $P_6 = (1 : 0 : 0)$, for some λ, μ and ν such that 0, 1, λ, μ and ν are all distinct.

The condition that Q and R both pass through P_6 can be calculated as above, and gives a single condition $H(\lambda, \mu, \nu) = 0$, say. We can also determine the condition $D_1(\lambda, \mu, \nu)$ that Q and R meet in fewer than four points: D_1 is the discriminant (with respect to t) of the quartic equation satisfied by those points $(t^2 : t : 1)$ lying on R.

From the discussion above, we note that the curve C admits three further Humbert configurations $(Q, R_2; P_1, P_4, P_6, P_2, P_5, P_3)$, $(Q, R_3; P_1, P_2, P_5, P_6, P_3, P_4)$ and $(Q, R_4; P_4, P_2, P_3, P_1, P_6, P_5)$, say; let the condition that Q meets R_i in fewer than four points be $D_i(\lambda, \mu, \nu)$ for $i = 2, 3, 4$.

We define $p_1(\nu) = \mathrm{Res}\Big(\mathrm{Res}(D_3, D_4; \lambda), D_2; \mu\Big)$ (a polynomial of degree 64), and let $p_2(\nu) = \mathrm{Res}\Big(\mathrm{Res}(H, D_1; \lambda), D_2; \mu\Big)$ (which has degree 32). After factorizing and clearing the factors of ν and $(\nu - 1)$, Maple gives the following forms for these poly-

nomials:

$$\begin{aligned} p_1(\nu) = {} & (\nu+1)^4(4\nu^4+36\nu^3-66\nu^2+26\nu-1)(\nu^4-26\nu^3+66\nu^2-36\nu-4)\times \\ & (31\nu^{12}-403\nu^{11}+5921\nu^{10}-47555\nu^9+244720\nu^8-440323\nu^7+ \\ & 475219\nu^6-440323\nu^5+244720\nu^4-47555\nu^3+5921\nu^2-403\nu+31)\times \\ & (11\nu^2-13\nu+1)^2(\nu^2-13\nu+11)^2(11\nu^4+9\nu^3+111\nu^2-11\nu+1)^2\times \\ & (\nu^4-11\nu^3+111\nu^2+9\nu+11)^2(11\nu^4-31\nu^3+41\nu^2-31\nu+11)^4 \\ \text{and } p_2(\nu) = {} & (\nu^2+2\nu-4)^4(16\nu^4+244\nu^3+51\nu^2-66\nu+11)\times \\ & (16\nu^4-116\nu^3+321\nu^2-396\nu+176)(\nu^4-21\nu^3+21\nu^2+9\nu-9)^2\times \\ & (\nu^4-96\nu^3+771\nu^2-666\nu-9)^2 \end{aligned}$$

These are coprime, and so we conclude that at least one the conics R, R_2, R_3 and R_4 must meet Q in four distinct points. □

3.3 An explicit $\sqrt{5}$-multiplication

Now we start from the configuration of theorem 3.1.3 and construct an explicit embedding $j\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$. This is mainly useful because it allows us to give a criterion for the multiplication being defined over $\mathbb{Q}$.

Let C be a curve of genus 2 which admits an Humbert configuration $(Q, R; \{P_i\})$, say. Let us fix a geometric isomorphism $\phi\colon Q \xrightarrow{\sim} \mathbb{P}^1$ such that $\phi(P_6) = \infty$. This gives an equation for C of the form

$$C : Y^2 = f(X) = \prod_{i=1}^{5}(X - a_i), \tag{3.1}$$

where $a_i = \phi(P_i)$ for $i = 1, 2, 3, 4, 5$.

By lemma 3.2.1, we may assume at first that Q and R meet transversally in four distinct points. As in section 2.9, define E to be the incidence relation between Q and the projective dual R^*, that is

$$E = \{(P, L) \in Q \times R^* \mid P \text{ lies on } L\}.$$

From the discussion in section 2.9, E is a nonsingular curve of genus 1. Further, there is a fixed point T on E of order 5 such that the coset $\widetilde{P_1} + \langle T \rangle$ on E projects to the set $\{P_1, \ldots, P_5\}$ on Q, where $\widetilde{P_1}$ is a point of E lying above P_1.

Now, following Mestre [Mes91a], let x be a function on E with double pole at 0, let $f\colon E \to E$ be the isogeny associated to the subgroup $\langle T \rangle$ and let u be the *abscissa equation*, that is, the function which makes the following square commute.

$$\begin{array}{ccc} E & \xrightarrow{f} & E \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow[u]{} & \mathbb{P}^1 \end{array}$$

Define the curve C' by the equation

$$C' : Y^2 = u(X) - u(a_1).$$

Then C' is a double cover of $\mathbb{P}^1$ branched over $a_1, \ldots, a_5$ and ∞, so is geometrically isomorphic to C. The poles of u are the x-coordinates of points of $\ker f$, so u has double poles at $x(T)$ and $x(2T)$, and no other poles. Write $\nu(x)$ for the function $(x - x(T))(x - x(2T))$, which we can regard as a function on E, C or C'. The isomorphism $C' \xrightarrow{\sim} C$ can then be written $(x', y') \mapsto (x', y'\nu(x'))$.

Now suppose (x, y) is a generic point of C (in the coordinates given by (3.1)). There are two tangents to R passing through $\phi^{-1}(x) \in Q$; label the residual points of intersection of these lines with Q as $\phi^{-1}(x_+)$ and $\phi^{-1}(x_-)$ such that if $x = x(P)$ for some $P \in E$ then $x_\pm = x(P \pm T)$. By the definitions, $\left(x_\pm, y \cdot \frac{1}{\nu(x)}\right)$ both lie on C' and so we have a well-defined pair of points $\left(x_+, y \cdot \frac{\nu(x_+)}{\nu(x)}\right)$ and $\left(x_-, y \cdot \frac{\nu(x_-)}{\nu(x)}\right)$ on C and can define a morphism θ from C to the second symmetric power $C^{(2)}$ by

$$\theta\colon (x, y) \mapsto \left\{ \left(x_+, y \cdot \frac{\nu(x_+)}{\nu(x)}\right), \left(x_-, y \cdot \frac{\nu(x_-)}{\nu(x)}\right) \right\}. \tag{3.2}$$

It follows that θ induces an endomorphism of $J = \mathrm{Jac}(C)$ since θ commutes with the hyperelliptic involution on C. Further, if we embed C in J by mapping (x, y) to the class of the divisor $(x, y) - \infty$ (where ∞ denotes the point of C above P_6) then, as can readily be verified, $(\theta^2 + \theta - 1)$ maps $[(x, y) - \infty]$ to the class of the divisor of the function $Y - \frac{y}{\nu(x)}\nu(X)$, that is $\theta^2 + \theta - 1 = 0$ on J.

Hence $j(\eta) = \theta + 1$ defines an embedding $j\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$.

We started this section by supposing that C admits an Humbert configuration. Of course, by theorem 3.1.3, this is equivalent to assuming that there is an embedding $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$. We have been careful thus far not to assert that our explicit RM by $\mathbb{Q}(\sqrt{5})$ is the same as this "original" RM, but we now prove the following proposition which states that these two actions of $\mathbb{Z}[\eta]$ are indeed the same.

Proposition 3.3.1 *Let C be a curve of genus 2, write $J = \mathrm{Jac}(C)$ and suppose given an embedding $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$. Let $(Q, R; \{P_i\})$ be an Humbert configuration for C (as given by theorem 3.1.3) and let $j\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$ be the embedding constructed as above with respect to $(Q, R; \{P_i\})$. Then $i = j$; that is to say that the procedure above gives an explicit description of the RM by $\mathbb{Q}(\sqrt{5})$.*

Proof We shall make use of the explicit description given by Cassels and Flynn [CF96, chapter 3] of the Kummer surface K associated to C.

Fix a model for C in the form

$$C : Y^2 = f(X) = \prod_{i=1}^{6} (X - a_i). \tag{3.3}$$

Now choose a point of J: this is represented by a point $\{(x, y), (u, v)\}$, say, on $C^{(2)}$. Then, from [CF96, equation 3.1.3], the image of this point on the Kummer surface K is $(1 : x + u : xu : \beta_0(x, u, y, v))$, where the exact form of β_0 will not worry us.

The node on K under the zero of J is at $N_0 = (0 : 0 : 0 : 1)$. From [CF96, equation 3.1.9], the image of the tangent cone at N_0 under projection through N_0 into the plane $(l : m : n : 0)$ has equation $l^2 = 4mn$. Considering the proof of theorem 3.1.3, this is the dual of Q. Hence we identify the plane $(l : m : n : 0)$ with $(\mathbb{P}^2)^*$, and then Q has equation $Y^2 = XZ$.

From the description of the singular planes in [CF96, chapter 3, section 7] (where they are called *tropes*) we see that the branch locus of $C \to Q$ is the set of points $\{(a_i^2 : -a_i : 1) \mid i = 1, \ldots, 6\}$. Thus the image of a point (x, y) under $C \to Q$ is

$(x^2 : -x : 1)$. Further, the image of $\{(x, y), (u, v)\}$ under the composition $C^{(2)} \to J \to K \to (\mathbb{P}^2)^*$ is the point representing the chord joining $(x^2 : -x : 1)$ and $(u^2 : -u : 1)$.

Now let $\varepsilon = i(\eta - 1)$ and let $\theta = j(\eta - 1)$ (as defined in equation 3.2). Considering the proofs of proposition 3.1.2 and theorem 3.1.3, the image of $\varepsilon^* D$ under $J \to K \to (\mathbb{P}^2)^*$ is the conic R^*. By the definition of θ, and by the previous paragraph, a pair $\{(x, y), (u, v)\}$ represents a point of $\theta^* D$ precisely when the chord joining $(x^2 : -x : 1)$ and $(u^2 : -u : 1)$ is tangent to R, that is when the projection of this point to $(\mathbb{P}^2)^*$ lies on R^*. Thus $\varepsilon^* D$ and $\theta^* D$ have the same projection to $(\mathbb{P}^2)^*$.

Since R^* is birational to its preimage on K, and since each of $\varepsilon^* D$ and $\theta^* D$ is fixed by multiplication by (-1) (recall that D was chosen to be symmetric), we can conclude that $\varepsilon^* D = \theta^* D$. An application of proposition 3.1.4 gives $\varepsilon = \theta$, and so $i = j$ as claimed. □

Note further that this shows (indirectly) that the image of our explicit embedding j is fixed by the Rosati involution.

Suppose the curve C is defined over a number field k, and take a model of the form (3.3) over k. We now give a criterion for when the real multiplication by $\mathbb{Q}(\sqrt{5})$ is defined over the field k. Observe that the set $\{a_1, \ldots, a_6\}$ is stable under the action of Galois and so we can regard $\mathrm{Gal}\,(k(a_1, \ldots, a_6))$ as a subgroup of S_6. Recall that $\mathrm{A}_5^{\mathrm{tr}} = \langle (1\ 2\ 3\ 4\ 5), (1\ 6)(2\ 5) \rangle$.

Theorem 3.3.2 *The embedding j has image contained in $\mathrm{End}_k(J)$ if and only if $\mathrm{Gal}\,(k(a_1, \ldots, a_6)/k)$ is contained in $\mathrm{A}_5^{\mathrm{tr}}$ up to S_6-conjugacy.*

Proof Any permutation $\sigma \in \mathrm{S}_6$ acts on $\{a_1, \ldots, a_6\}$, and so produces a (possibly different) configuration as in Humbert's criterion (3.1.3). Hence σ gives a new map ${}^{\sigma}\theta$, where $\theta = j(\eta - 1)$ is as defined in equation 3.2.

Let G be the subgroup

$$G = \{\sigma \in \mathrm{S}_6 \mid {}^{\sigma}\theta = \theta\},$$

and let H_i denote the stabilizer in S_6 of each $i = 1, \ldots, 6$.

Now $\sigma \in G \cap H_i$ if and only if the action of σ preserves the conic R_i, which in turn is defined by the pentagon formed by the branch points other than P_i. Hence $G \cap H_i$ is naturally the group of symmetries of that pentagon, that is, $G \cap H_i = \mathrm{A}_5^{\mathrm{tr}} \cap H_i$.

This forces $G = \mathrm{A}_5^{\mathrm{tr}}$, and so the result is immediate. □

3.4 A family of curves from Humbert's criterion

We can now use theorem 3.1.3 to produce our first examples of curves of genus 2 with maximal real multiplication by $\mathbb{Q}(\sqrt{5})$.

We shall take the same notation as before, that is, we take homogeneous coordinates $(X : Y : Z)$ for $\mathbb{P}^2$ and let Q be the plane conic

$$Q : Y^2 = XZ.$$

Further, we assume that there are points $P_1, \ldots, P_5$ on Q such that the conic R which is tangent to the edges of the pentagon $P_1P_2P_3P_4P_5$ passes through $(1 : 0 : 0)$.

Again, recall from section 3.3 that going from a point P of Q to the point P_+ is given by addition of a fixed 5-torsion point T on the curve $E = \{(P, L) \mid P \text{ lies on } L\}$. In particular, let us consider what happens if P is a point of intersection of Q and R. Then there is only one tangent to R passing through P and this meets Q in one further point P_+, say. With reference to Poncelet's theorem, the other tangent to R through P_+ meets Q in a third point P_{++} which lies on a line tangent to both Q and R—see figure 3.1.

Taking $(l : m : n)$ as homogeneous coordinates for $\mathbb{P}^{2*}$, we have an equation for R^* (the dual curve to R) of the form

$$R^* : al^2 + (bm + cn)^2 + 2eln + 2flm = 0$$

since R passes through $(1 : 0 : 0)$.

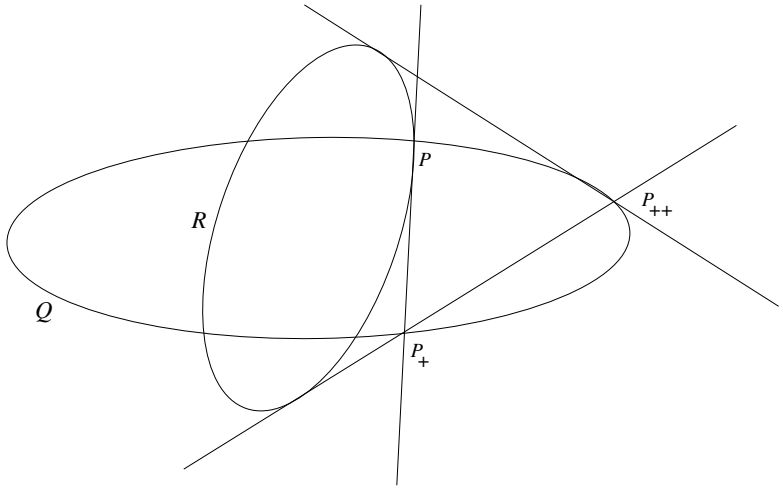


Figure 3.1: A "degenerate pentagon"

Now, to simplify things, we shall assume that the other vertices of the "degenerate pentagon" with a vertex at $(1:0:0)$ are $(t^2:t:1)$ and $(0:0:1)$, where the latter is the point of contact with Q of a common tangent to Q and R. Then, since the tangent to Q at $(0:0:1)$ is the line $(l:m:n)=(1:0:0)$, this gives $a=0$.

Now the tangent to R at $(1:0:0)$ is $(0:-c:b)\in R^*$, and this meets Q again at $(b^2:bc:c^2)$, so the condition that this degenerate pentagon exists is that the chord joining $(0:0:1)$ and $(b^2:bc:c^2)$ should be tangent to R, that is $(c:-b:0)\in R^*$.

This gives $b(b^3-2cf)=0$, but $b=0$ would actually mean that we only had a degenerate *triangle*, so the condition we require is $b^3=2cf$.

The next step is to start from a point of Q and find the pentagon passing through that point which is inscribed to Q and circumscribed to R. From the above, we write

$$\begin{aligned} Q &: Y^2 = XZ \\ R^* &: (m+\lambda n)^2 + 2\mu ln + \frac{1}{\lambda} lm = 0. \end{aligned}$$

(We are taking $\lambda = c/b$ and $\mu = e/b^2$; note that b is nonzero for nonsingular R.)

Using a little hindsight, we suppose that the first vertex of the pentagon is at $P=(1:\lambda t:\lambda^2 t^2)\in Q$, and write $P_+=(1:\lambda u_1:\lambda^2 u_1^2)$, $P_-=(1:\lambda u_2:\lambda^2 u_2^2)$, $P_{++}=(1:\lambda s_1:\lambda^2 s_1^2)$ and $P_{--}=(1:\lambda s_2:\lambda^2 s_2^2)$.

Suppose that the two tangents to R passing through the point $(1 : \lambda t : \lambda^2 t^2)$ are $(l_1 : m_1 : n_1)$, $(l_2 : m_2 : n_2) \in R^*$. Then the ratios (m_1/n_1) and (m_2/n_2) are the roots of the quadratic polynomial

$$\lambda^2(1 - 2\mu t^2) + \lambda(2 - 2\mu t - t^2)T + (1 - t)T^2.$$

The line $l_i X + m_i Y + n_i Z = 0$ meets Q at those points $(1 : u : u^2)$ satisfying $n_i u^2 + m_i u + l_i = 0$, and thus $\lambda(u_i + t) = -(m_i/n_i)$ for $i = 1, 2$. This gives

$$u_1 + u_2 = \frac{2 - 2\mu t - 2t + t^2}{1 - t} \text{ and } u_1 u_2 = 1 - t.$$

But now the same calculation gives $s_i t = 1 - u_i$ for $i = 1, 2$ and so we have

$$s_1 + s_2 = \frac{2\mu - t}{1 - t} \text{ and } s_1 s_2 = \frac{2\mu - 1}{t(1 - t)}.$$

The associated family of hyperelliptic curves is

$$Y^2 = X(X - t)(X^2 - [u_1 + u_2]X + u_1 u_2)(X^2 - [s_1 + s_2]X + s_1 s_2),$$

with the two parameters t and μ; observe that the choice of λ does not affect the isomorphism class of the associated curve of genus 2.

We shall next make the transformation which puts the point $X = Y = 0$ at infinity, and thereby obtain an equation of the form

$$\begin{aligned} Y^2 &= (1 - tX)(u_1 u_2 X^2 - [u_1 + u_2]X + 1)(s_1 s_2 X^2 - [s_1 + s_2]X + 1) \\ &= -\sigma_5 X^5 + \sigma_4 X^4 - \sigma_3 X^3 + \sigma_2 X^2 - \sigma_1 X + 1, \end{aligned}$$

where the σ_i are the elementary symmetric functions in t, u_1, u_2, s_1, and s_2.

In terms of t and μ, the σ_i are

$$\begin{aligned} \sigma_1 &= 2(1 + \mu), \\ \sigma_2 &= \frac{-t^5 + 2(1 + \mu)t^4 - (3 + 2\mu + 4\mu^2)t^2 + 2(1 + \mu)t + 1 + 2\mu}{t(1 - t)^2}, \\ \sigma_3 &= \frac{-2t^5 + 4(1 + \mu)t^4 - (3 + 2\mu + 4\mu^2)t^3 - (1 - 2\mu - 4\mu^2)t - 2 + 4\mu}{t(1 - t)^2}, \\ \sigma_4 &= \frac{-t^5 + 2(1 + \mu)t^4 - 2(1 + \mu)t^3 + (1 + 2\mu - 4\mu^2)t^2 - 1 + 2\mu}{t(1 - t)^2} \end{aligned}$$

and $\sigma_5 = 2\mu - 1$.

Thus if we choose the two parameters

$$A = 1 - 2\mu \text{ and } B = \sigma_2 \tag{3.4}$$

then we obtain equations for the family of curves of genus 2 in the following shape:

$$\mathscr{C}_{AB} : Y^2 = AX^5+(A+B-3)X^4+(5-3A+A^2-2B)X^3+BX^2+(A-3)X+1. \tag{3.5}$$

Note that the discriminant of $\mathscr{C}_{AB}$ is

$$D_{AB} = A^2\Big(4A^5 - 29A^4 + (106-26B)A^3 - (223-112B+B^2)A^2 + (338-240B+42B^2)A - (117-114B+37B^2-4B^3)\Big)^2.$$

Let S be the locus in the affine plane where D_{AB} does not vanish, and consider the family of curves $\pi\colon \mathscr{C} \to S$ where $\pi^{-1}(A,B) = \mathscr{C}_{AB}$. This gives a parametrization of all triples (X, i, P) defined over $\mathbb{Q}$, where X is a curve of genus 2, i is an action of $\mathbb{Z}[\eta]$ on $\mathrm{Jac}(X)$ which commutes with the Rosati involution, and P is a Weierstrass point on X. More precisely we have the following.

Proposition 3.4.1 *Let k be a number field. Then each k-rational section to the map $\pi\colon \mathscr{C} \to S$ gives a triple (X, i, P) where X, $i(\eta)$ and P are all defined over k. Conversely, when k does not contain $\mathbb{Q}(\sqrt{5})$, every nonsingular curve X/k which has a k-rational Weierstrass point P and maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over k arises in this fashion.*

Proof First suppose we choose $A, B \in k$. Then it is clear that $\mathscr{C}_{AB}$ is defined over k and has a k-rational Weierstrass point (at infinity). The choice of A and B (3.4) ensures that there is an Humbert configuration $(Q, R; P_1, \ldots, P_6)$ for $\mathscr{C}_{AB}$ where the conic R^* is defined over k. But then any Galois automorphism $\sigma \in \mathrm{Gal}(\overline{k}/k)$ acts on the configuration $(Q, R; P_1, \ldots, P_6)$ and commutes with the correspondence $P \mapsto \{P_+, P_-\}$ on Q, and so σ commutes with the induced action of $\mathbb{Z}[\eta]$ on $\mathrm{Jac}(\mathscr{C}_{AB})$.

Conversely, suppose we have a triple (X, i, P) where each of X, $i(\eta)$, and P is defined over k. Then we can choose an Humbert configuration $(Q, R; P_1, \ldots, P_6)$ for

X such that P_6 is the image of P on Q, and is a k-rational point. The conic R is defined over k, since $i(\eta)$ is defined over k (see the proof of theorem 3.3.2). Further, the "degenerate pentagon" with a vertex at P_6 must also be preserved by any Galois automorphism (since it is determined by R). Since one vertex is k-rational, and the other two occur with multiplicity 2, every vertex must be rational over k. Hence we can choose an Humbert configuration for X such that the pair of conics Q and R assume the forms at the start of this section (and so X will be isomorphic to $\mathscr{C}_{AB}$ for some $(A, B) \in S$) providing that the conics Q and R meet transversally at P_6. It remains to show that this is true when k does not contain $\mathbb{Q}(\sqrt{5})$.

Suppose Q has equation $Y^2 = XZ$ as before, and suppose that R passes through $(1 : 0 : 0)$ and is tangent to Q there. Then R^* has an equation

$$al^2 + bm^2 + 2enl + 2flm = 0.$$

Now one mimics the method of the start of this section: the condition that there is a pentagon with vertices on Q and edges tangent to R is

$$b^2 + 6be + 4e^2 = 0.$$

Hence R is defined over some field k' containing $\mathbb{Q}(\sqrt{5})$; this implies that the RM by $\mathbb{Q}(\sqrt{5})$ for any associated curve of genus 2 is also defined over $k' \supseteq \mathbb{Q}(\sqrt{5})$. □

The condition above that k does not contain $\mathbb{Q}(\sqrt{5})$ genuinely is necessary. An example that demonstrates this is the curve $Y^2 = X^5 - 2$ over $\mathbb{Q}(\sqrt{5})$. Here the only Weierstrass point defined over $\mathbb{Q}(\sqrt{5})$ is the point at infinity, the RM is defined over $\mathbb{Q}(\sqrt{5})$, but the two conics in an Humbert configuration for this curve meet tangentially in two distinct points.

Notice that a by-product of this is to produce a family of quintic polynomials with Galois group D_{10}, namely that appearing on the right-hand side of equation 3.5 above.

We should also make it clear that this does not give a moduli space for such triples (X, i, P), since different values of the parameters A and B can give rise to isomorphic

curves. In particular, for each B, the curve $\mathscr{C}_{1,B}$ is isomorphic to the curve $\mathscr{C}_{-1,B+7}$ via $(X, Y) \mapsto (-X + 1, Y)$. It is natural to ask when two pairs of parameters (A, B) and (A', B') give (geometrically) isomorphic curves $\mathscr{C}_{AB}$ and $\mathscr{C}_{A'B'}$, and it would seem that a straightforward calculation should yield the answer: one needs to determine when a fractional linear transformation of the X-coordinate turns the equation for $\mathscr{C}_{AB}$ into the equation for $\mathscr{C}_{A'B'}$ (see section 2.1). However, from a practical point of view, this approach rapidly degenerates into very long and tedious manipulations; so far it has not been possible to find the desired condition.

We would very much prefer a family that included all genus 2 curves with a $\sqrt{5}$-multiplication, without the hypothesis that there be a rational Weierstrass point, but we do not know how to achieve this. As already mentioned (section 1.2), Brumer has produced families, but it is not known how comprehensive these are (and the details are as yet unpublished).

Finally, the table in section A.2 gives the odd part of the conductors of some of the curves $\mathscr{C}_{AB}$.

Chapter 4

The ℓ-adic Galois representations

4.1 Introduction

In this chapter we put our criterion for when a real multiplication by $\mathbb{Q}(\sqrt{5})$ is defined over $\mathbb{Q}$, namely theorem 3.3.2, into a more general context, and see what can be said about the structure of the Tate module at a prime ℓ of an abelian variety with RM. Note that more is known about the ℓ-adic Galois representations attached to RM abelian varieties than is presented here. In particular Ribet [Rib76] has determined that the image of Galois is "as large as possible" for almost all primes ℓ. (This means that we may assert equality, not just containment, in theorem 4.3.1(i),(ii) for almost all ℓ.)

The calculation that follows was done independently of Ribet's work (indeed, before I learnt about his paper) and has a different emphasis, so it is presented in full here, as opposed to a strategy of quoting from [Rib76] and deducing what we should like to say.

We should also remark that Taylor and Shepherd-Barron [SBT97, theorem 3.4] have proved that any mod 2 icosahedral Galois representation can be realized as the action on the 2-division points of some abelian surface with real multiplication by $\mathbb{Q}(\sqrt{5})$. As already remarked (section 1.1), they also prove, modulo some technical restrictions, that abelian surfaces over $\mathbb{Q}$ with RM by $\mathbb{Q}(\sqrt{5})$ are modular; thus they deduce that any representation $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_4)$ which is unramified at 3 and 5 is

modular in the sense of Serre's conjecture (for which, see [Ser87]).

In section 4.5, we use some of the information we have gained about the structure of the Tate module to prove two theorems relating to the question of when a polarized abelian surface with RM by a field F is isogenous to a *principally* polarized abelian surface with *maximal* RM by F.

4.2 Abelian varieties with real multiplication

Let F be a totally real number field of degree g over $\mathbb{Q}$, and let $\mathcal{O}$ be the ring of integers of F. Let k be a number field and let A/k be an abelian variety of dimension g. Suppose that A has real multiplication by F; more specifically, suppose there is an embedding $i\colon \mathcal{O}' \hookrightarrow \mathrm{End}(A)$, where $\mathcal{O}'$ is some order in F.

Let ℓ be a rational prime which does not divide the conductor $f(\mathcal{O}') = [\mathcal{O} : \mathcal{O}']$. The Tate module $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$, and is also a module for $R := \varprojlim (\mathcal{O}/\ell^n\mathcal{O})$ via i, since $\mathrm{End}(A) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}(T_\ell A)$ (see [Mil86a, Theorem 12.5]).

Suppose that ℓ decomposes in $\mathcal{O}$ as follows:

$$\ell\mathcal{O} = \prod_{j=1}^{m} \mathfrak{p}_j^{e_j},$$

where the $\mathfrak{p}_j$ are distinct primes of $\mathcal{O}$ with $[\mathcal{O} : \mathfrak{p}_j] = \ell^{f_j}$ and $e_j \geqslant 1$ for each j.

Then, by the Chinese Remainder Theorem, we have a decomposition

$$R \cong \bigoplus_{j=1}^{m} R_j$$

where $R_j := \varprojlim \left(\mathcal{O}/\mathfrak{p}_j^{ne_j}\right)$. Set $\mathcal{O}_j = \varprojlim \left(\mathcal{O}/\mathfrak{p}_j^{n}\right)$, so then $R_j \twoheadrightarrow \mathcal{O}_j$ with kernel $\varepsilon_j = \varprojlim \left(\mathfrak{p}_j^n/\mathfrak{p}_j^{ne_j}\right)$, and set $T_j = \varprojlim \left(\ker \mathfrak{p}_j^{ne_j}\right)$ for $j = 1, \ldots, m$, so each T_j is a $\mathbb{Z}_\ell$-submodule of $T_\ell A$ and is an R_j-module.

Since the ideals $\mathfrak{p}_j^{e_j}$ are coprime, the pairwise intersections of the T_j are all zero. If we write $I_j = \sum_{r \neq j} \mathfrak{p}_r^{e_r}$ then $\mathfrak{p}_j^{e_j}$ and I_j are coprime, so $T_j = \varprojlim \left(I_j^n \cdot A[\ell^n]\right)$, but also $I_1 + \cdots + I_m = \mathcal{O}$, so

$$T_\ell A = \bigoplus_{j=1}^{m} T_j. \tag{4.1}$$

Now fix j and, for each $r = 0, 1, \ldots, e_j$, set $F_j^r = \varprojlim \left(\ker \mathfrak{p}_j^{nr}\right)$. This gives a filtration

$$T_j = F_j^{e_j} \supseteq \cdots \supseteq F_j^1 \supseteq F_j^0 = (0), \tag{4.2}$$

where $\varepsilon_j \cdot F_j^r \subseteq F_j^{r-1}$ for each r.

The ideal $\mathfrak{p}_j$ is generated by ℓ and an element $x \in \mathcal{O}$ such that $\ell^{f_j} \parallel \mathrm{N}_{F/\mathbb{Q}}(x)$. We then have $\dim_{\mathbb{F}_\ell}(A[x] \cap A[\ell]) \leqslant 2f_j$ and $x \cdot A[\mathfrak{p}_j^r] \subseteq A[\mathfrak{p}_j^{r-1}]$ for each $r = 1, 2, \ldots, e_j$, whence $\operatorname{rank}_{\mathbb{Z}_\ell} F_j^r \leqslant 2f_j + \operatorname{rank}_{\mathbb{Z}_\ell} F_j^{r-1}$ for each r. In particular, $\operatorname{rank}_{\mathbb{Z}_\ell} T_j \leqslant 2e_j f_j$. But $\operatorname{rank}_{\mathbb{Z}_\ell} T = 2g = 2\sum_j e_j f_j = \sum_j \operatorname{rank}_{\mathbb{Z}_\ell} T_j$, so $\operatorname{rank}_{\mathbb{Z}_\ell} T_j = 2e_j f_j$ for each j, whence $\operatorname{rank}_{\mathbb{Z}_\ell} F_j^r = 2rf_j$ for each r and each j.

F_j^1 is then a free $\mathcal{O}_j$-module which is of rank $2f_j$ over $\mathbb{Z}_\ell$. Since $[\mathcal{O}_j : \mathbb{Z}_\ell] = f_j$,

$$F_j^1 \text{ is a free rank 2 } \mathcal{O}_j\text{-module.} \tag{4.3}$$

Now suppose that $i(\mathcal{O}') \subseteq \mathrm{End}_k(A)$. The absolute Galois group G_k of k acts on $T_\ell A$, and preserves both the decomposition (4.1) and each filtration (4.2). Write $\rho_\ell \colon G_k \to \mathrm{Aut}(T_\ell A)$ for the Galois representation on the Tate module. Then (4.1) gives

$$\rho_\ell(G_k) \subseteq \mathrm{Aut}_R(T_\ell A) = \prod_{j=1}^{m} \mathrm{Aut}_{R_j}(T_j). \tag{4.4}$$

Let G_j denote the image of ρ_ℓ in $\mathrm{Aut}_{R_j}(T_j)$ for each $j = 1, \ldots, m$. We get a sequence of homomorphisms

$$G_j = H_j^{e_j} \to \cdots \to H_j^1 \to H_j^0 = \{1\} \tag{4.5}$$

where each map $(H_j^r \to H_j^{r-1})$ is restriction from F_j^r to F_j^{r-1} in the filtration (4.2). In particular, (4.3) gives

$$H_j^1 \subseteq \mathrm{Aut}_{\mathcal{O}_j}(F_j^1) \cong \mathrm{GL}_2(\mathcal{O}_j). \tag{4.6}$$

Further, if $\phi \in \ker(H_j^r \to H_j^{r-1})$ for $r > 1$, then $(\phi - 1)$ is an R-linear map $F_j^r \to F_j^r$ which acts as zero on F_j^{r-1}. But $\varepsilon_j(\phi - 1) \cdot F_j^r = (\phi - 1)\varepsilon_j \cdot F_j^r = (\phi - 1)F_j^{r-1} = (0)$, so $(\phi - 1)F_j^r \subseteq F_j^1$. Hence we can view $(\phi - 1)$ as an $\mathcal{O}_j$-linear map $(F_j^r / F_j^{r-1}) \to F_j^1$.

Now if $\phi, \psi \in \ker(H_j^r \to H_j^{r-1})$, then $(\phi-1)(\psi-1)\cdot F_j^r = (0)$, which implies that $(\phi\psi - 1) = (\phi - 1) + (\psi - 1)$. Thus $\phi \mapsto \phi - 1$ defines a map from $\ker(H_j^r \to H_j^{r-1})$ to the additive group $\mathrm{Hom}_{\mathcal{O}_j}(F_j^r/F_j^{r-1}, F_j^1)$. But $F_j^r/F_j^{r-1} \cong F_j^1 \cong \mathcal{O}_j^2$ as $\mathcal{O}_j$-modules, and so we have

$$\ker\left(H_j^r \to H_j^{r-1}\right) \hookrightarrow \mathrm{M}_2(\mathcal{O}_j)^+ \cong \mathcal{O}_j^4. \tag{4.7}$$

To say more, we use the following further information available to us, namely the existence of a Weil pairing.

Lemma 4.2.1 *Let A/k be an abelian variety. Then, for each $m \in \mathbb{Z}$, there is a nondegenerate bilinear pairing $\overline{e}_m \colon A[m] \times A^\vee[m] \to \mu_m$ such that*

(i) ${}^\sigma\overline{e}_m(x,y) = \overline{e}_m({}^\sigma x, {}^\sigma y)$ *for each $\sigma \in G_k$;*

(ii) *if $f \colon A \to A$ is a homomorphism then $\overline{e}_m(f(x), y) = \overline{e}_m(x, f^\vee(y))$;*

(iii) $\overline{e}_{mn}(x,y)^n = \overline{e}_m(nx, ny)$.

Proof See [Mil86a, §16]. □

Property (iii) allows us to define a pairing $e_\ell \colon T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ as the inverse limit of the pairings $\overline{e}_{\ell^n}$. This is then a nondegenerate bilinear pairing.

If $\lambda \colon A \to A^\vee$ is a polarization (or, more generally a homomorphism) then we define $\overline{e}_m^\lambda = \overline{e}_m \circ (1 \times \lambda)$ and $e_\ell^\lambda = e_\ell \circ (1 \times \lambda)$; this is then an antisymmetric pairing on $T_\ell A$ precisely when λ is a polarization [Mil86a, Prop 16.6].

Recall that the Rosati involution associated with λ is given by

$$\dagger \colon \alpha \mapsto \lambda^{-1} \circ \alpha^\vee \circ \lambda.$$

Therefore $e_\ell^\lambda(\alpha x, y) = e_\ell^\lambda(x, \alpha^\dagger y)$ for $\alpha \in \mathrm{End}^0(A)$, by part (ii) of the lemma.

Recall also that G_k acts on $\mathbb{Z}_\ell(1)$ via the cyclotomic character $\chi_\ell \colon G_k \to \mathbb{Z}_\ell$. Specifically, if ζ is a generator of $\mathbb{Z}_\ell(1)$ (a compatible choice of primitive ℓ^nth roots of 1 for each n), then ${}^\sigma\zeta = \zeta^{\chi_\ell(\sigma)}$ for each $\sigma \in G_k$.

So if we now assume that † acts as the identity on $i(\mathcal{O}')$ then $T_\ell A$ has a $\mathbb{Z}_\ell$-bilinear antisymmetric pairing e_ℓ^λ such that

$$e_\ell^\lambda(x, i(a)y) = e_\ell^\lambda(i(a)x, y) \text{ for } a \in \mathcal{O}$$
$$\text{and } e_\ell^\lambda({}^\sigma x, {}^\sigma y) = \chi_\ell(\sigma) \cdot e_\ell^\lambda(x, y) \text{ for } \sigma \in G_k.$$

(Note that we are writing $\mathbb{Z}_\ell(1)$ additively.) When λ is a principal polarization, then we also have that e_ℓ^λ is nondegenerate.

Fix $\sigma \in G_k$, and then write $t = \chi_\ell(\sigma)$ and $V = T_\ell A \otimes \mathbb{Q}_\ell\left(t^{1/2}\right)$. Then e_ℓ^λ gives a symplectic pairing (that is, one which is nondegenerate, bilinear and alternating) on V and $t^{-1/2}\rho_\ell(\sigma)$ is an element of $\mathrm{Sp}(V)$ (that is, it preserves the given symplectic pairing). It is well known that symplectic groups are generated by their transvections (see, for instance, [Die67, proposition 4]) and thus as a consequence that $\mathrm{Sp}(V) \subseteq \mathrm{SL}(V)$. Hence we have

$$\det \rho_\ell = \chi_\ell^g. \tag{4.8}$$

4.3 Abelian surfaces with real multiplication

We now record the results of the previous section in the case $g = 2$ in the following theorems.

Theorem 4.3.1 *Let F be a real quadratic field with ring of integers $\mathcal{O}$, and let A be an abelian surface over k with $i\colon \mathcal{O}' \hookrightarrow \mathrm{End}_k(A)$, where $\mathcal{O}'$ is an order in F.*

Let ℓ be a (rational) prime coprime to the conductor $f(\mathcal{O}')$ and let $\rho_\ell\colon G_k \to \mathrm{GL}_4(\mathbb{Z}_\ell)$ be the Galois representation on the Tate module $T_\ell A$; write $G = \rho_\ell(G_k)$ and $R = \varprojlim \mathcal{O}/\ell^n\mathcal{O}$. Then

(i) *if ℓ is inert in F then $G \hookrightarrow \mathrm{GL}_2(R)$;*

(ii) *if ℓ splits in F then $G \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$;*

(iii) *if ℓ ramifies in F then there is an exact sequence $1 \to K \to G \to H \to 1$, with $K \hookrightarrow (\mathbb{Z}_\ell)^4$ and $H \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Proof

(i) Both (4.1) and (4.2) become trivial, and so (4.6) gives the result.

(ii) Here the decomposition (4.1) becomes

$$T_\ell A = T_1 \oplus T_2$$

with T_1, T_2 free rank 2 $\mathbb{Z}_\ell$-modules.

The filtrations (4.2) become trivial, and $\mathcal{O}_1 \cong \mathcal{O}_2 \cong \mathbb{Z}_\ell$, so (4.4) and (4.6) give the result.

(iii) Here the decomposition (4.1) is trivial, but the filtration (4.2) becomes

$$T_\ell A = F^2 \supset F^1 \supset (0)$$

where F^1 is a free rank 2 $\mathbb{Z}_\ell$-module. (4.5), (4.6) and (4.7) combine to give the short exact sequence of the statement, where we write $H = \mathrm{Aut}_{\mathbb{Z}_\ell}(F^1)$ and $K = \ker(G \to H)$.

□

Theorem 4.3.1 has already given us some information about the image of a Galois representation on $T_\ell(A)$, but we can now use the pairing e_ℓ^λ to calculate that the determinants of such Galois representations are given by the character χ_ℓ. First, a lemma.

Lemma 4.3.2 *Suppose that $S \subset R$ are commutative rings with 1, and that M is an R-module with an S-linear map $t\colon R \to S$ and a nondegenerate antisymmetric S-bilinear pairing $\psi\colon M \times M \to S$ satisfying*

(i) *$(r_1, r_2) \mapsto t(r_1 r_2)$ is a perfect pairing and*

(ii) *$\psi(rx, y) = \psi(x, ry)$ for all $x, y \in M$, $r \in R$.*

Then there is a unique $\phi\colon M \times M \to R$ such that $\psi = t \circ \phi$. Further, ϕ is nondegenerate, antisymmetric and R-bilinear.

Proof Fixing $x, y \in M$, we have an S-linear map $r \mapsto \psi(rx, y)$, so there is a unique $\phi(x, y) \in R$ such that $t\,(r\phi(x, y)) = \psi(rx, y)$ for all $x, y \in M$, $r \in R$ by (i). This defines ϕ.

It follows immediately from the nondegeneracy of ψ that ϕ is nondegenerate. To check that ϕ is antisymmetric, we note that, by the definition of ϕ and property (ii),

$$t(r\phi(x, y)) = -t(r\phi(y, x)) \text{ for all } r \in R \text{ and all } x, y \in M.$$

Property (i) implies that that $\phi(x, y) = -\phi(y, x)$ for $x, y \in M$. The R-bilinearity of ϕ follows similarly (again, using the assumption that t is perfect). □

Theorem 4.3.3 *Let F be a real quadratic field with ring of integers $\mathcal{O}$, and let A be an abelian surface over k with a principal polarization $\lambda\colon A \xrightarrow{\sim} A^\vee$ defined over k and $i\colon \mathcal{O}' \hookrightarrow \mathrm{End}_k(A)^{\dagger=1}$ for some order $\mathcal{O}'$ in F.*

Let ℓ be a prime which does not divide $f(\mathcal{O}')$, let $\rho_\ell\colon G_k \to \mathrm{GL}_4(\mathbb{Z}_\ell)$ be the Galois representation on $T_\ell A$ and let χ_ℓ be the cyclotomic character.

Then $\det \rho_\ell = \chi_\ell^2$. Further,

(i) *if ℓ is inert in F and ρ'_ℓ is the composition $G_k \to \rho_\ell(G_k) \hookrightarrow \mathrm{GL}_2(R)$, with the second map as in* (4.3.1)(i)*, then $\det \rho'_\ell = \chi_\ell$;*

(ii) *if ℓ splits in F and $\rho'_\ell\colon G_k \to \rho_\ell(G_k) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$, with the second map as in* (4.3.1)(ii)*, then $\det(p_1 \circ \rho'_\ell) = \chi_\ell = \det(p_2 \circ \rho'_\ell)$, where $p_1, p_2\colon \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ are the projections onto each factor;*

(iii) *if ℓ ramifies in F then in the short exact sequence of* (4.3.1)(iii)*, $K \hookrightarrow \mathbb{Z}_\ell^3$.*

Proof The first assertion is just equation 4.8.

(i) After (4.3.1)(i), T is a free rank 2 R-module, where $R = \varprojlim \mathcal{O}/\ell^n\mathcal{O}$.

The determinant of the bilinear form $(r_1, r_2) \mapsto \mathrm{Tr}_{R/\mathbb{Z}_\ell}(r_1 r_2)$ is the discriminant of $R/\mathbb{Z}_\ell$, which is a unit in $\mathbb{Z}_\ell$, and so we can apply lemma 4.3.2 to define $\phi\colon T \times T \to R$ such that $\mathrm{Tr}_{R/\mathbb{Z}_\ell}\,\phi = e_\ell^\lambda$.

Now for $\sigma \in G_k$, we have $\chi_\ell(\sigma) \cdot e_\ell^\lambda(x,y) = \mathrm{Tr}_{R/\mathbb{Z}_\ell}(\det \rho'_\ell(\sigma) \cdot \phi(x,y))$.

We can write $R = \mathbb{Z}_\ell[\varepsilon]$ for some element $\varepsilon \in R \setminus \mathbb{Z}_\ell$ and so, given $\sigma \in G_k$, can write $\det \rho'_\ell(\sigma) = s + t\varepsilon$ for some $s, t \in \mathbb{Z}_\ell$. Since ϕ is nondegenerate, we can choose x and y so that $\phi(x,y) = 1$. This gives the equation

$$2\chi_\ell(\sigma) = 2s + t\,\mathrm{Tr}(\varepsilon).$$

But now replacing x with εx gives the equation

$$\mathrm{Tr}(\varepsilon)\chi_\ell(\sigma) = \mathrm{Tr}(\varepsilon)s + t(\mathrm{Tr}(\varepsilon)^2 - 2\mathrm{N}(\varepsilon)).$$

Eliminating s gives

$$t(4\mathrm{N}(\varepsilon) - \mathrm{Tr}(\varepsilon)^2) = 0,$$

whence $t = 0$ since $\varepsilon \notin \mathbb{Z}_\ell$, and so $\det \rho'_\ell(\sigma) = s = \chi_\ell(\sigma)$.

(ii) With the notation of the proof of (4.3.1)(ii), $T_1 = \mathcal{O}_2 \cdot T$ and $T_2 = \mathcal{O}_1 \cdot T$, but $\mathcal{O}_1\mathcal{O}_2 T = (0)$. Therefore $T_1 \subseteq T_2^\perp$.

Since e_ℓ^λ is nondegenerate on T, e_ℓ^λ must restrict to a nondegenerate pairing on each of T_1 and T_2, and so for $\sigma \in G_k$ we can apply equation 4.8 to each of T_1 and T_2 separately.

(iii) Take the notation of (4.3.1)(iii) again. Then (in a similar way to (ii) above) F^1 is totally isotropic for e_ℓ^λ. We can choose a $\mathbb{Z}_\ell$-basis for F^1 and extend it to a basis for T such that e_ℓ^λ is represented by the matrix $\mathbb{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in 2×2 block form.

Now, for $\sigma \in G_k$, $\rho_\ell(\sigma)$ is represented by a matrix of the form $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ with respect to the same basis. Then we know that $\rho_\ell(\sigma)^{\mathrm{t}} \mathbb{J} \rho_\ell(\sigma) = \chi_\ell(\sigma) \cdot \mathbb{J}$, which implies that $\beta^{\mathrm{t}}\delta = \delta^{\mathrm{t}}\beta$ and $\alpha^{\mathrm{t}}\delta = \chi_\ell(\sigma) \cdot 1$. Further, $\rho_\ell(\sigma)$ lies in the kernel of restriction to F^1 exactly when $\alpha = 1$, and then the injection (4.7), which is $\rho_\ell(\sigma) \mapsto \beta$, has image contained in the symmetric matrices.

□

We are most interested in the Galois representations on the 2-division points, and so record the following corollary explicitly.

Corollary 4.3.4 *Suppose that $F, \mathcal{O}, A, \lambda, i$ are as in* (4.3.3)*. Let $\overline{\rho}_2$ be the Galois representation on $A[2]$, and write $G = \overline{\rho}_2(G_k)$.*

Then

(i) *if 2 is inert in F then $G \hookrightarrow \mathrm{A}_5$;*

(ii) *if 2 splits in F then $G \hookrightarrow \mathrm{S}_3 \times \mathrm{S}_3$;*

(iii) *if 2 ramifies in F then there is an exact sequence $1 \to H \to G \to K \to 1$ with $H \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^3$ and $K \hookrightarrow \mathrm{S}_3$.*

Proof We use the fact that χ_2 is trivial modulo 2, along with the following isomorphisms: $\mathrm{SL}_2(\mathbb{F}_4) \xrightarrow{\sim} \mathrm{A}_5$ via the natural action on $\mathbb{P}^1(\mathbb{F}_4)$; and $\mathrm{GL}_2(\mathbb{F}_2) \xrightarrow{\sim} \mathrm{S}_3$ via the natural action on $\mathbb{P}^1(\mathbb{F}_2)$. □

We note that P. Bending [Ben98] has identified the Galois group G in case (iii) above more precisely: we shall see in the following section that G is naturally a subgroup of S_6, and Bending shows that, up to conjugacy, G is contained in the subgroup $\langle (1\ 2\ 4\ 5), (1\ 3)(4\ 6) \rangle \cong \mathrm{C}_2 \times \mathrm{S}_4$.

4.4 Connexions with curves of genus 2

Let C be a curve of genus 2 defined over k and write $J = \mathrm{Jac}(C)$, so that J is an abelian surface over k with a natural principal polarization λ. Notice that the nonzero 2-division points on J can be identified with the pairs of distinct Weierstrass points on C—this follows from the general description of the Jacobian in section 2.2, along with the fact that the hyperelliptic involution on C extends to multiplication by (-1) on J. Now $J[2]$ is a 4-dimensional $\mathbb{F}_2$-vector space, and this phenomenon is an example of a well-known isomorphism of groups.

In general, let V be any 4-dimensional vector space over $\mathbb{F}_2$ which carries a symplectic form. Then we have the following.

Lemma 4.4.1 *There is a bijection between the nonzero elements of V and the set of pairs of distinct elements of $B = \{1,2,3,4,5,6\}$ which induces an isomorphism $\mathrm{Sp}(V) \cong \mathrm{S}_6$.*

Proof We equip the set $\mathscr{P}^{\mathrm{even}}(B)$ of even-cardinality subsets of B with the structure of an $\mathbb{F}_2$-vector space by considering it as a set of functions $B \to \mathbb{F}_2$ (so addition is given by taking symmetric differences). This vector space now carries a degenerate alternating pairing $\langle X, Y\rangle = \#X \cap Y \pmod 2$ with radical $\{\emptyset, B\}$. Putting $W = \mathscr{P}^{\mathrm{even}}(B)/\{\emptyset, B\}$, we obtain a symplectic $\mathbb{F}_2$-vector space whose nonzero elements are in bijection with cardinality 2 subsets $\{i,j\}$ of B. (If we denote the class of $\{i,j\}$ in W by $[i,j]$, then $\{[1,2],[4,5],[2,3],[5,6]\}$ is a symplectic basis for W over $\mathbb{F}_2$, that is with respect to this basis the pairing is represented by the matrix $\mathbb{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in 2×2-block form.)

A choice of symplectic basis for V induces an isomorphism $V \xrightarrow{\sim} W$ of symplectic vector spaces, and so a bijection between the nonzero elements of V and subsets $\{i,j\} \subset B$ as well as an isomorphism $\mathrm{Sp}(V) \xrightarrow{\sim} \mathrm{Sp}(W)$ of groups.

Now it is readily checked that the action of the symmetric group S_6 on B gives rise to a linear action of S_6 on W which respects the pairing $\langle \cdot\,, \cdot \rangle$, and so an embedding $\mathrm{S}_6 \hookrightarrow \mathrm{Sp}(W)$. But $\#\,\mathrm{Sp}(W) = 720 = \#\mathrm{S}_6$ and so $\mathrm{Sp}(V) \cong \mathrm{S}_6$, as claimed. □

Notice that a similar construction shows more generally that, for each l, we have an injection $\mathrm{S}_{2l+2} \hookrightarrow \mathrm{Sp}_{2l}(\mathbb{F}_2)$. Note also that for any two isomorphisms $V \cong W$ as in the lemma, the corresponding isomorphisms $\mathrm{Sp}(V) \cong \mathrm{S}_6$ differ by an inner automorphism of S_6.

We consider $V = J[2]$ with the symplectic form $\overline{e}_2^{\lambda}$, and identify B with the set of Weierstrass points of C, or equivalently with the branch locus of a canonical map $C \to \mathbb{P}^1$. Thus the G_k-action on V is determined by and determines the G_k-action on B by the previous lemma. Rephrasing this,

Lemma 4.4.2 *Suppose that $Y^2 = f(X)$ is an affine model of C, where f is a sextic polynomial over k. Then the image of $\overline{\rho}_2(G_k)$ in S_6 is conjugate to the Galois group of f over k.*

Now suppose further that there is an embedding $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$ (where $\dagger$ is the Rosati involution induced by λ). Let G be the image of $\overline{\rho}_2(G_k)$ in S_6. Notice that by (4.3.4), if $\mathrm{im}(i) \subseteq \mathrm{End}_k(J)$, then G embeds in a copy of A_5 in S_6. However, the G_k-action on B is generically transitive, and so we expect that G is actually contained in one of the six transitive copies of A_5 contained in S_6. There is precisely one conjugacy class of such subgroups, and one of these subgroups is $\mathrm{A}_5^{\mathrm{tr}} := \langle (1\ 2\ 3\ 4\ 5), (1\ 6)(2\ 5)\rangle$. This leads us to expect that if $\mathrm{im}(i) \subseteq \mathrm{End}_k(J)$ then $G \subseteq \mathrm{A}_5^{\mathrm{tr}}$ up to conjugacy in S_6. Of course theorem 3.3.2 tells us something just like this, and we can now restate it as

Theorem 4.4.3 *With C, J and $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$ as above, $\mathrm{im}(i) \subseteq \mathrm{End}_k(J)$ if and only if $G \subseteq \mathrm{A}_5^{\mathrm{tr}}$ up to conjugacy in S_6.*

Note that the form of this result is peculiar to the case of maximal real multiplication by $\mathbb{Q}(\sqrt{5})$. First, in this case we do have an explicit description of the real multiplication. Secondly, if J has maximal real multiplication by $\mathbb{Q}(\sqrt{d})$, where d is a (positive) squarefree integer, $d \not\equiv 1 \pmod 4$ and $\mathrm{End}(J)$ is commutative, then the restriction of the multiplication to $J[2]$ is necessarily defined over k: given any $\sigma \in G_k$, the endomorphism ${}^{\sigma}i(\sqrt{d})$ is a square root of d in $\mathrm{End}(J)$, so must be one of $\pm i(\sqrt{d})$.

4.5 Making polarizations principal

We finish this chapter with some work which, while not directly related to the ℓ-adic Galois representations arising from RM abelian varieties, uses some similar techniques to the earlier sections. Our first result returns to the issue of making a real multiplication be maximal after isogeny, as in section 2.5. Before that we need to recall some of the theory of polarizations, and fix some terminology.

By a map $\pi\colon (A,\lambda) \to (B,\lambda')$ of polarized abelian varieties, we shall mean a map $\pi\colon A \to B$ such that $\lambda = \pi^*\lambda'$. When we say that a map $\pi\colon (A,\lambda) \to (B,\lambda')$ of polarized abelian varieties is defined over the field k, we shall mean that each of A, B, λ, λ' and $\pi\colon A \to B$ is defined over k.

Let (A,λ) be a polarized abelian variety defined over a number field k. We define a pairing e^λ on $\ker\lambda$ as follows: given $a, a' \in \ker\lambda$, choose m such that $ma = 0 = ma'$ and $b \in A(\overline{k})$ such that $mb = a'$, then set $e^\lambda(a,a') = \overline{e}_m(a,\lambda(b))$. Note that this makes sense since $m\lambda(b) = \lambda(a') = 0$; the definition is also independent of the choice of b and m, and e^λ is an alternating pairing (see [Mil86a, §16]).

Lemma 4.5.1 *Let M be a free module over a principal ideal domain R and suppose the characteristic of R is not 2. Suppose given a nondegenerate antisymmetric and R-bilinear pairing $\langle\cdot,\cdot\rangle\colon M \times M \to R$, and a nonzero R-endomorphism ε of M such that $\langle u, \varepsilon v\rangle = \langle \varepsilon u, v\rangle$ for all $u, v \in M$. Then*

(i) *$\varepsilon(v) \in v^\perp$ for all $v \in M$ and*

(ii) *$\operatorname{rank}_R(\operatorname{im}\varepsilon)$ is even.*

Proof

(i) Given $v \in M$, we have $\langle\varepsilon(v), v\rangle = \langle v, \varepsilon(v)\rangle = -\langle\varepsilon(v), v\rangle$.

(ii) Define $(\cdot,\cdot)\colon \operatorname{im}\varepsilon \times \operatorname{im}\varepsilon \to R$ as follows: given $u, v \in \operatorname{im}\varepsilon$, choose $w \in \varepsilon^{-1}(u)$ and set $(u,v) = \langle w, v\rangle$. This is independent of the choice of w since $\ker\varepsilon \subseteq (\operatorname{im}\varepsilon)^\perp$; it is also clearly bilinear.

Given $u \in \operatorname{im}\varepsilon \setminus \{0\}$, choose w' so that $\langle u, w'\rangle \neq 0$, and choose $w \in \varepsilon^{-1}(u)$. Put $v = \varepsilon w'$, and then $(u,v) = \langle w, v\rangle = \langle u, w'\rangle \neq 0$. Hence $(\cdot,\cdot)$ is nondegenerate.

Further, given $u = \varepsilon(w)$ and $v = \varepsilon(w')$, we have $(v,u) = \langle w', u\rangle = \langle v, w\rangle = -\langle w, v\rangle = -(u,v)$.

Since $(\cdot,\cdot)\colon \operatorname{im}\varepsilon \times \operatorname{im}\varepsilon \to R$ is nondegenerate, R-bilinear and antisymmetric, $\operatorname{im}\varepsilon$ must be of even rank.

□

If (A, λ) is a polarized abelian variety, we shall use † to denote the associated Rosati involution on $\mathrm{End}^0(A)$. Note that $\alpha \in \mathrm{End}^0(A)$ is fixed by † if and only if $\lambda \circ \alpha = \alpha^\vee \circ \lambda$. We therefore define

$$\mathrm{End}(A)^{\dagger=1} := \{\alpha \in \mathrm{End}(A) \mid \lambda \circ \alpha = \alpha^\vee \circ \lambda\}.$$

Lemma 4.5.2 *Let $\pi\colon (A, \lambda) \to (B, \lambda')$ be an isogeny defined over a number field k, and suppose $R \subseteq \mathrm{End}_k(A)^{\dagger=1}$ preserves $\ker \pi$. Then π induces $R \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$.*

Proof It is clear that π induces a map $R \to \mathrm{End}(B)$. Let $\alpha \in R$ and let β be the induced endomorphism of B so that the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & A \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ B & \xrightarrow[\beta]{} & B \end{array}$$

If $\beta = 0$ then for all $a \in A(\overline{k})$ we have $\alpha(a) \in \ker \pi$. Suppose n kills $\ker \pi$, and choose $a' \in A(\overline{k})$ such that $na' = a$. Then $\alpha(a) = n\alpha(a') = 0$. Thus $\alpha = 0$ and so π induces $R \hookrightarrow \mathrm{End}(B)$.

For any $\sigma \in G_k$, we have $({}^\sigma\beta - \beta)\pi = {}^\sigma(\beta\pi) - (\beta\pi) = {}^\sigma(\pi\alpha) - (\pi\alpha) = 0$, whence ${}^\sigma\beta = \beta$ since π is surjective. Hence the image of R lies in $\mathrm{End}_k(B)$.

Also, $\lambda\alpha = \alpha^\vee\lambda$ implies $\pi^\vee(\lambda'\beta)\pi = \pi^\vee(\beta^\vee\lambda')\pi$, whence $\lambda'\beta = \beta^\vee\lambda'$, arguing as before. Thus the image of R commutes with the Rosati involution as claimed. □

Proposition 4.5.3 *Let (A, λ) be a polarized abelian variety over a number field k.*

(i) *A homomorphism $\mu\colon A \to A^\vee$ is a polarization if and only if the pairings e_ℓ^μ are antisymmetric.*

(ii) *Suppose that $\alpha \in \mathrm{End}_k(A)^{\dagger=1}$ is an isogeny. Then $\lambda = \lambda'\alpha$ for some polarization λ' on A defined over k if and only if $\ker \lambda \supseteq \ker \alpha$.*

(iii) *Let $f\colon A \to B$ be an isogeny defined over k. Then $\lambda = f^*\lambda'$ for some polarization λ' on B defined over k if and only if* $\ker\lambda \supseteq \ker f$ *and the pairing e^λ is trivial on* $\ker f \times \ker f$.

Proof

(i) [Mil86a, proposition 16.6].

(Note that Milne prefaces his theorem 16.5 with the hypothesis that k is algebraically closed. Since we are working over a number field, hence a perfect field, the results we quote extend to our situation—cf. [Mil86a, remark 16.14].)

(ii) Necessity is clear. For sufficiency, note that we can define a homomorphism $\lambda'\colon A \to A^\vee$, defined over k, such that $\lambda = \lambda'\alpha$.

Now let $a = (a_n) \in T_\ell A$. By the definitions,

$$\overline{e}^{\lambda'}_{\ell^n}(a_n, a_n) = \overline{e}_{\ell^n}(a_n, \lambda'(a_n)) = \overline{e}_{\ell^n}(a_n, \lambda(b_n)),$$

where $b = (b_n) \in T_\ell A$ satisfies $\alpha b_n = a_n$.

There is an isogeny α' such that $\alpha'\alpha = \deg\alpha$. Suppose that $\deg\alpha = \ell^r s$, where ℓ does not divide s. Then

$$\begin{aligned} s \cdot \overline{e}^{\lambda'}_{\ell^n}(a_n, a_n) &= (\deg\alpha) \cdot \overline{e}_{\ell^{n+r}}(a_{n+r}, \lambda(b_{n+r})) \\ &= \overline{e}_{\ell^{n+r}}(a_{n+r}, \lambda(\alpha'\alpha b_{n+r})) \\ &= \overline{e}^{\lambda}_{\ell^{n+r}}(a_{n+r}, \alpha'(a_{n+r})) \\ &= 0, \end{aligned}$$

where the last step applies (4.5.1)(i).

We conclude from (i) that λ' is a polarization.

(iii) [Mil86a, proposition 16.8].

□

Note that in (ii), $\deg\lambda = \deg\alpha \cdot \deg\lambda'$, and in (iii), $\deg\lambda = (\deg f)^2 \deg\lambda'$.

Theorem 4.5.4 *Let F be a real quadratic field. Let $R' \supseteq R$ be orders in F and write $[R' : R] = n$. Let (A, λ) be a polarized abelian surface, defined over a number field k, and suppose that there is an embedding $i\colon R \hookrightarrow \mathrm{End}_k(A)^{\dagger=1}$, that $\deg\lambda$ is coprime to n, and that n is odd.*

Then there is an isogeny $\pi\colon A \to B$ defined over k and a polarization λ' on B also defined over k such that $\deg\lambda' = \deg\lambda$ and $R' \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$.

Proof We may clearly suppose that R is maximal among orders of F contained in R' which embed in $\mathrm{End}_k(A)^{\dagger=1}$. We shall then proceed by an induction on n, observing that the case $n = 1$ is trivial.

For $n > 1$ choose a prime ℓ dividing n, and write $n = \ell s$. Write $R' = \mathbb{Z}[\alpha]$ for some $\alpha \in F$, then set $\alpha' = s\alpha$, and use the construction in the proof of proposition 2.5.4 to find B with an action of $\mathbb{Z}[\alpha']$. More precisely, take π to be an isogeny with kernel $(\ell\mathbb{Z}[\alpha']) \cdot A[\ell^2]$.

Now we have that $\ker\pi \supseteq A[\ell]$, and that

$$\ell \ker\pi = (\ell\mathbb{Z}[\alpha']) \cdot A[\ell] = \mathrm{im}(\ell\alpha' \mid A[\ell]).$$

Thus $\#\ker\pi = \ell^{4+t}$, where $t = \dim_{\mathbb{F}_\ell} \mathrm{im}(\ell\alpha' \mid A[\ell])$.

Set $\lambda_A = \ell^3\lambda$. Then $\ker\lambda_A \supseteq A[\ell^3] \supseteq \ker\pi$. Also, if $a, a' \in \ker\pi$ and $\ell^2 b = a'$ then

$$\begin{aligned} e^{\lambda_A}(a, a') &= \overline{e}_{\ell^2}(a, \lambda_A(b)) \\ &= \overline{e}_{\ell^2}(a, \ell\lambda(a')) \\ &= \overline{e}^{\lambda}_{\ell}(\ell a, \ell a'). \end{aligned}$$

But now $a = (\ell\varepsilon)c$ and $a' = (\ell\varepsilon')c'$ for some $\varepsilon, \varepsilon' \in \mathbb{Z}[\alpha']$ and some $c, c' \in A[\ell^2]$, so

$$\begin{aligned} e^{\lambda_A}(a, a') &= \overline{e}^{\lambda}_{\ell}(\ell(\ell\varepsilon)c, \ell(\ell\varepsilon')c') \\ &= \overline{e}^{\lambda}_{\ell}(\ell^2(\ell\varepsilon\varepsilon')c, \ell c') \\ &= 0. \end{aligned}$$

Hence by proposition 4.5.3(iii), $\lambda_A = \pi^*\lambda'$ for some polarization λ' on B, defined over k. Note that

$$\deg\lambda' = \frac{\ell^{12}\deg\lambda}{\ell^{2(4+t)}} = \ell^{2(2-t)}\deg\lambda.$$

Further, applying lemma 4.5.2 to $\pi\colon (A, \lambda_A) \to (B, \lambda')$ shows that the action of $\mathbb{Z}[\alpha']$ on B will be defined over k and fixed by the Rosati involution. All that remains, then, is to show that $t = 2$.

Note that e_ℓ^λ is a nondegenerate pairing on $T_\ell A$ since $\ell \nmid \deg\lambda$. Also, $(\ell\alpha')$ is not zero on $A[\ell]$ since we are assuming that A does not have an action of $\mathbb{Z}[\alpha']$. Thus $t = \dim_{\mathbb{F}_\ell} \mathrm{im}(\ell\alpha' \mid A[\ell])$ is even by lemma 4.5.1(ii).

Also, $(\ell\alpha')^2 = \ell(\ell\alpha'^2)$ acts as zero on $A[\ell]$, and so $\mathrm{im}(\ell\alpha' \mid A[\ell]) \subseteq \ker(\ell\alpha' \mid A[\ell])$. Hence $t \leqslant 2$ by the rank-nullity formula. □

Now we consider the problem of reducing the degree of a polarization via isogeny. The following lemma is concerned with what can be said without reference to any real multiplication.

Lemma 4.5.5 *Let (A, λ) be a polarized abelian variety defined over a number field k. Then there is an isogeny $\pi\colon A \to B$ defined over k and a polarization λ' on B, also defined over k, such that for each prime dividing $\deg\lambda'$, we have that $(\ker\lambda')[\ell^\infty]$ is properly contained in $B[\ell]$ and is of even dimension over $\mathbb{F}_\ell$. Moreover, $\mathrm{End}_k(A)^{\dagger=1} \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$ via π.*

Proof Write $\Lambda = \ker\lambda$. We shall induct on $\deg\lambda$, taking as our base cases those where $\Lambda[\ell^\infty] \subsetneq A[\ell]$ for each ℓ.

In general, suppose ℓ is a prime dividing $\deg\lambda$. If $\Lambda[\ell^\infty] \supseteq A[\ell^n]$ for any $n \geqslant 1$ then we can find a polarization λ' on A such that $\lambda = \ell^n\lambda'$ by proposition 4.5.3(ii). Thus we reduce to the case where $\Lambda[\ell^\infty] \not\supseteq A[\ell^n]$ for all $n \geqslant 1$.

Now choose the minimal $n \geqslant 1$ such that $\Lambda[\ell^\infty] \subseteq A[\ell^n]$, that is, such that $\Lambda[\ell^\infty] = \Lambda[\ell^n]$. Suppose $n > 1$. Then $\ell \cdot \Lambda[\ell^2] \subseteq \Lambda[\ell]$, and $\ell \cdot \Lambda[\ell^2] \neq (0)$, for otherwise we would have $\ell^{n-2} \cdot \Lambda[\ell^n] \subseteq \Lambda[\ell^2] = \Lambda[\ell]$, whence $\Lambda[\ell^\infty] = \Lambda[\ell^n] = \Lambda[\ell^{n-1}]$, contradicting the minimality of n.

Let $a, a' \in \ell \cdot \Lambda[\ell^2]$, and choose $b \in \Lambda[\ell^2]$ such that $\ell b = a'$. Then $e^\lambda(a, a') = \overline{e}_\ell(a, \lambda(b)) = 0$, since $b \in \ker\lambda$. Hence, by proposition 4.5.3(iii), we have an isogeny $\pi\colon (A, \lambda) \to (B, \lambda')$ defined over k, with $\ker\pi = \ell \cdot \Lambda[\ell^2]$. Then $\deg\lambda' < \deg\lambda$ and,

since the action of $\mathrm{End}_k(A)^{\dagger=1}$ preserves $\ker\pi$, we have that π induces $\mathrm{End}_k(A)^{\dagger=1} \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$, by lemma 4.5.2.

In this way we reduce to the case where $\Lambda[\ell^\infty] \subsetneq A[\ell]$. The assertion about the dimension of $\Lambda[\ell^\infty]$ follows from the fact that the degree of a polarization is always a square [Mil86a, theorem 13.3(a)]. □

Note that if A is an abelian surface this reduces the degree of a given polarization to the square of a squarefree integer (without making the endomorphism ring any smaller). Given a real multiplication we can say more.

Lemma 4.5.6 *Let F be a real quadratic field, and let R be an order in F. Let (A, λ) be a polarized abelian surface with an embedding $R \hookrightarrow \mathrm{End}(A)^{\dagger=1}$. Then every prime factor of $\deg\lambda$ which does not divide the conductor of R is either split or ramified in F.*

Proof Write Δ for the discriminant of R, and write $\deg\lambda = d^2$. Then let $H_{\Delta,d}$ denote the moduli space of triples (A, λ, i) formed of a polarized abelian surface A, a polarization λ with $\deg\lambda = d^2$, and an embedding $i\colon R \hookrightarrow \mathrm{End}(A)^{\dagger=1}$. In [vdG88, chapter IX, §2], van der Geer describes $H_{\Delta,d}$ as a quotient of the Siegel upper half plane of degree 2, and shows that $H_{\Delta,d} \neq \emptyset$ exactly when Δ is a square modulo $4d$. The result as stated is now a straightforward deduction. □

Theorem 4.5.7 *Let F be a real quadratic field of class number 1, and let R be an order in F. Let (A, λ) be a polarized abelian surface over a number field k, and suppose there is an embedding $i\colon R \hookrightarrow \mathrm{End}_k(A)^{\dagger=1}$. Write $\deg\lambda = (d_1 d_2)^2$, where d_2 is odd and coprime to the conductor of R.*

Then there is an isogeny $\pi\colon A \to B$ defined over k and a polarization λ' on B, also defined over k, such that $(\deg\lambda')^{1/2}$ is a squarefree divisor of d_1, and $R \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$.

Proof Write $\Lambda = \ker\lambda$. After lemma 4.5.5 we are reduced to considering squarefree values of $(\deg\lambda)^{1/2}$ such that, for each prime ℓ dividing $\deg\lambda$, we have $\Lambda[\ell^\infty] \subset A[\ell]$

and $\dim_{\mathbb{F}_\ell}(\Lambda[\ell^\infty]) = 2$. Under this assumption, write $\deg\lambda = (d_1 d_2)^2$ with d_1 and d_2 as in the statement of the theorem. If $d_2 = 1$ then the result is trivial. Otherwise, let ℓ be a prime divisor of d_2. After lemma 4.5.6, we know that ℓ is either split or ramified in F.

Suppose that ℓ splits in F, with $\ell\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$. This induces a decomposition $\Lambda[\ell] = \Lambda[\mathfrak{p}_1] \oplus \Lambda[\mathfrak{p}_2]$ (cf. equation 4.1).

Suppose that both factors are nonzero. Then $\Lambda[\mathfrak{p}_1]$ is 1-dimensional and rationally defined. The pairing e^λ is alternating, so will be trivial on $\Lambda[\mathfrak{p}_1] \times \Lambda[\mathfrak{p}_1]$ and so we may take an isogeny $\pi\colon (A,\lambda) \to (B,\lambda')$ with $\ker\pi = \Lambda[\mathfrak{p}_1]$ by proposition 4.5.3(iii). Note that $\deg\lambda' = \ell^{-2}\deg\lambda$. Also, R preserves $\Lambda[\mathfrak{p}_1]$, and so $R \hookrightarrow \mathrm{End}_k(B)^{\dagger=1}$ by lemma 4.5.2, and we are done by the inductive hypothesis.

Suppose instead that one of the factors is zero. Without loss of generality, then, we have $\Lambda[\ell] = \Lambda[\mathfrak{p}_1] = A[\mathfrak{p}_1]$. Now $\mathfrak{p}_1 = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{O}$, and so we can apply proposition 4.5.3(ii) to give a polarization λ' on A such that $\lambda = \lambda'\alpha$. Again, $\deg\lambda' = \ell^{-2}\deg\lambda$ and we are done by the inductive hypothesis.

Suppose that ℓ ramifies in F, with $\ell\mathcal{O} = \mathfrak{p}^2$. This induces $\Lambda[\ell] \supseteq \Lambda[\mathfrak{p}] \supseteq (0)$. Note that $\mathfrak{p}\cdot\Lambda[\ell] \subseteq \Lambda[\mathfrak{p}]$ and so $\Lambda[\mathfrak{p}] \neq (0)$. We now proceed exactly as in the case when ℓ splits in F, since $\Lambda[\mathfrak{p}]$ is of dimension 1 or 2 over $\mathbb{F}_\ell$. □

We are interested in applying theorems 4.5.4 and 4.5.7 to the 2-dimensional factors of $J_0(N)$, particularly those with RM by $\mathbb{Q}(\sqrt{5})$. Here it seems that in almost every case one can assert that the given abelian variety is isogenous to one with a principal polarization and maximal RM by $\mathbb{Q}(\sqrt{5})$. In particular, the numerical data in section A.4 illustrates lemma 4.5.6 very well.

Chapter 5

The moduli space

5.1 Abelian surfaces with level 2 structure

By a level 2 structure on a principally polarized abelian surface (A, λ) we shall mean an isomorphism $A[2] \xrightarrow{\sim} \mathbb{F}_2^4$ of $\mathbb{F}_2$-vector spaces which carries the Weil pairing $\overline{e}_2^{\lambda}$ to the standard pairing on $\mathbb{F}_2^4$ described by the matrix $\mathbb{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in 2×2 block form.

One way to describe a curve C of genus 2 up to isomorphism is to specify the branch locus of the canonical map $C \to \mathbb{P}^1$ up to projective equivalence (see section 2.1). As we have seen in section 4.4, choosing a level 2 structure on $J = \mathrm{Jac}(C)$ is equivalent to choosing an ordering of this branch locus, so we can obtain a moduli space for principally polarized abelian surfaces with level 2 structure by considering the space of ordered sextuples of points of $\mathbb{P}^1$ modulo projective equivalence, that is $P_1^6 := (\mathbb{P}^1)^6 / \operatorname{PGL}_2$. We can even give a simple concrete model for this moduli space, as follows.

Let $Z \subset \mathbb{P}^5$ be the *Segre cubic*, that is the variety defined by

$$\sum_{i=1}^{6} z_i = \sum_{i=1}^{6} z_i^3 = 0.$$

It is proved in [DO88] that the following describes an isomorphism $P_1^6 \xrightarrow{\sim} Z$. (The computations in [DO88] are heavy, although clearly set out; in what follows a great

deal is omitted. In particular, the cross ratios (ij) defined below are far from independent, and much use is made of the relations between them, without explicit reference.)

Suppose we start with a point of P_1^6. This is represented by an ordered sextuple of points $(a_i : b_i) \in \mathbb{P}^1$ $(i = 1, \ldots, 6)$. Write (ij) for the *cross-ratio* $(a_i b_j - a_j b_i)$, and form the following five numbers.

$$t_1 = (12)(34)(56); \quad t_2 = (13)(24)(56); \quad t_3 = (12)(35)(46);$$
$$t_4 = (13)(25)(46); \quad t_5 = (14)(25)(36).$$

We then make the following linear change of variables to define $P_1^6 \xrightarrow{\sim} Z$.

$$\begin{aligned} z_1 &= 2t_1 - t_2 - t_3 + t_4 + t_5; \\ z_2 &= -2t_1 + t_2 + t_3 + t_4 - t_5; \\ z_3 &= -t_2 + t_3 - t_4 + t_5; \\ z_4 &= t_2 + t_3 - t_4 - t_5; \\ z_5 &= -t_2 - t_3 + t_4 - t_5; \\ \text{and } z_6 &= t_2 - t_3 - t_4 + t_5. \end{aligned}$$

Working with these explicit forms, we can verify that any permutation $\sigma \in \mathrm{S}_6$ of the points $(a_i : b_i)$ corresponds to the permutation σ^{out} of the coordinates z_i, where $\mathsf{out}\colon \mathrm{S}_6 \xrightarrow{\sim} \mathrm{S}_6$ is the outer automorphism which maps

$$\begin{aligned} (12) &\mapsto (14)(23)(56); \\ (23) &\mapsto (15)(26)(34); \\ (34) &\mapsto (14)(25)(36); \\ (45) &\mapsto (15)(23)(46); \\ \text{and } (56) &\mapsto (14)(26)(35). \end{aligned}$$

(For the purposes of the verification, we recommend first using a computer algebra package to expand the z_i in terms of the a_i and b_i. It seems at first sight that there is a sign change for odd permutations but, of course, we are free to rescale the z_i.)

In the interpretation of Z as a coarse moduli space for abelian surfaces with level 2 structure, this implies that the natural permutation action on Z comes from considering the same abelian surface with different level 2 structures. Hence we can regard P_1^6/S_6 as a coarse moduli space for principally polarized abelian surfaces: the quotient map corresponds to "forgetting" the level 2 structure. We also see that if the point $z \in Z$ corresponds to a nonsingular curve C of genus 2, then z lies in the locus $Z^0 = \{z \in Z \mid z_i + z_j \neq 0 \text{ for } i \neq j\}$.

5.2 The relation with the invariants

Suppose that $x_1, \ldots, x_n$ are independent (commuting) variables. Then we shall denote by $\sigma_i(x_1, \ldots, x_n)$, or simply $\sigma_i(x)$ when the range of indices is clear from the context, the ith elementary symmetric function in $x_1, \ldots, x_n$, and by $\tau_i(x)$ the ith power sum $\tau_i(x) = \sum_j x_j^i$. We shall also write $\Delta(x) := \prod_{i<j}(x_i - x_j)$ so that $\Delta(x)^2$ is the usual discriminant of the polynomial $\prod_{i=1}^n (T - x_i)$.

If $f(T)$ is a polynomial in one variable, then we use the shorthand notation $\sigma_i(f(x)) = \sigma_i(f(x_1), \ldots, f(x_n))$, and similarly for $\tau_i(f(x))$.

Igusa in [Igu60] defines four integral invariants I_2, I_4, I_6, and I_{10} of a sextic form

$$f(X, Y) = \prod_{i=1}^{6} (X - a_i Y).$$

Writing $(ij) := (a_i - a_j)$, these are given by

$$\begin{aligned} I_2 &= \sum_{15 \text{ terms}} (12)^2(34)^2(56)^2 \\ I_4 &= \sum_{10 \text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \\ I_6 &= \sum_{60 \text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \\ \text{and } I_{10} &= \Delta(a)^2, \end{aligned} \tag{5.1}$$

where the sums are over all symmetric conjugates of the summand. (Our notation here is that of [Wan95]; in [Igu60] these invariants are called A, B, C and D. One should beware that these invariants are not the same as the I_n defined in [Liu94].)

The I_{2n} are invariants under projective equivalence of the sextuple $(a_1, \ldots, a_6)$, and are also symmetric in the a_i, so they can be written as symmetric functions in the coordinates of the point $z \in Z$ corresponding to the class of $(a_1, \ldots, a_6)$ in P_1^6.

The relations are as follows.

$$\begin{aligned} I_2 &= \tau_2(z), \\ 32I_4 &= 6\tau_4(z) - \tau_2(z)^2, \\ 64I_6 &= -6\tau_6(z) + 7\tau_2(z)\tau_4(z) - \tau_2(z)^3 \\ \text{and } 2^{10}I_{10} &= \sigma_5(z)^2. \end{aligned} \tag{5.2}$$

I_2 is easy to calculate in terms of $z_1, \ldots, z_6$:

$$I_2 = \sum \Big((12)(34)(56)\Big)^2 = \sum \left(\frac{1}{2}(z_1 + z_4)\right)^2 = \frac{5}{4}\tau_2(z) + \frac{1}{2}\sigma_2(z) = \tau_2(z)$$

because $\tau_1(z)^2 = 0 = \tau_2(z) + 2\sigma_2(z)$.

To get I_{10}, we note that $\prod_{i<j}(z_i + z_j) = 2^{15}\prod_{i<j}(ij)^3$, but then

$$\prod_{j=2}^{6}(z_1 + z_j) = z_1^5 + \sum_{i=1}^{5} z_1^{5-i}\sigma_i(z_2, z_3, z_4, z_5, z_6) = \sigma_5(z_1, z_2, z_3, z_4, z_5, z_6),$$

using $\sigma_1(z) = \sigma_3(z) = 0$. Thus $\prod_{i<j}(z_i + z_j) = \sigma_5(z)^3$, and so $2^{10}I_{10} = \sigma_5(z)^2$.

The relations for the other two invariants were obtained by a "brute force" calculation, using Mathematica to write each of I_4, I_6, and the power sums $\tau_2(z), \tau_4(z), \tau_6(z)$ in terms of the elementary symmetric functions $\sigma_i(a)$, then doing a little linear algebra to deduce what the coefficients are.

Igusa also defines three absolute invariants (whenever $I_{10} \neq 0$).

$$i_1 := \frac{I_2^5}{I_{10}},\ i_2 := \frac{I_2^3 I_4}{I_{10}} \text{ and } i_3 := \frac{I_2^2 I_6}{I_{10}}. \tag{5.3}$$

5.3 Abelian surfaces with $\sqrt{5}$-multiplication

It is proved in [vdG88] that the variety $Y \subset \mathbb{P}^4$ given by

$$\sum_{i=1}^{5} y_i = \sum_{i=1}^{5} y_i^3 = 0$$

is a moduli space for principally polarized abelian surfaces A with level 2 structure and an embedding $i\colon \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(A)^{\dagger=1}$.

It is then proved in [SBT97, lemma 2.4] that the map $j\colon Y \to Z$ induced by their moduli interpretations is given, up to the permutation action of S_6 on Z, by

$$j\colon (y_i) \longmapsto (4y_1^2 - \tau_2(y) : 4y_2^2 - \tau_2(y) : 4y_3^2 - \tau_2(y) : 4y_4^2 - \tau_2(y) : 4y_5^2 - \tau_2(y) : \tau_2(y)).$$

(As already remarked, the permutation action on Z corresponds to the different choices of level 2 structure.)

Let us examine the intersection of Y with the hyperplane defined by $y_5 = 0$. The other coordinates y_1, y_2, y_3 and y_4 are then roots of a polynomial with no odd degree terms, so we may order y_1, y_2, y_3, y_4 so that $y_1 + y_2 = y_3 + y_4 = 0$. In other words, this intersection is the union of 3 lines, the orbit of $(s : -s : t : -t : 0)$ under permutation of the first four coordinates. We let Y^0 be the complement in Y of the 15 lines in the orbit of $(s : -s : t : -t : 0)$ under the natural S_5-action on $\mathbb{P}^4$.

Lemma 5.3.1 *j is an embedding when restricted to Y^0.*

Proof Suppose that $j(y) = j(y')$ for points $y, y' \in Y$. Then, for some choice of signs $\varepsilon_i \in \{+1, -1\}$, $y_i = \varepsilon_i y_i'$ for each $i = 1, 2, 3, 4, 5$. Put $N = \#\{i \,|\, \varepsilon_i = +1\}$.

If $N = 0, 5$ then $y = y'$.

If $N = 1, 4$ then some $y_i = 0$ because $\sigma_1(y) = \sigma_1(y') = 0$; after permuting by an element of S_5, we may suppose that $y_5 = 0$.

If $N = 2, 3$ then, up to S_5-conjugacy, $y_3 + y_4 + y_5 = y_3^3 + y_4^3 + y_5^3 = 0$, which implies (after possible further re-ordering) that $y_5 = 0$.

The remarks above now show that y lies on one of the lines in $Y \setminus Y^0$. □

This begs the question of the moduli interpretation of the locus $Y \setminus Y^0$. The image of $Y \setminus Y^0$ under j lies in the union of the lines which are in the orbit of $(s : s : -s : -s : t : -t)$ under the S_6-action on Z. But, referring to the end of section 5.1, such points lie in $Z \setminus Z^0$, and so correspond to choices of six points of $\mathbb{P}^1$ which

are no longer all distinct. This means that points of $Y \setminus Y^0$ do not correspond to curves of genus 2.

We now compute the image $j(Y) \subset Z$, proceeding in a number of steps, using the various relations between the power sums and elementary symmetric polynomials. Let $y = (y_i)$ be a point of Y, and $j(y) = (z_i)$ be its image in Z.

(1) First, $\tau_1(y^2) = \tau_2(y) = \tau_1(y)^2 - 2\sigma_2(y)$ implies

$$\tau_1(y^2) = -2\sigma_2(y).$$

(2) Secondly, $\sigma_2(y)^2 = \sigma_2(y^2) + 2\sigma_1(y)\sigma_3(y) - 2\sigma_4(y)$, and so we have $\tau_1(y^2)^2 = 4\sigma_2(y^2) - 8\sigma_4(y)$

$$\Rightarrow\ 8\sigma_4(y) = \left[\tau_1(y^2)^2 - 2\tau_2(y^2)\right].$$

(3) Squaring again, $\sigma_4(y)^2 = \sigma_4(y^2) + 2\sigma_5(y)\sigma_3(y) = \sigma_4(y^2)$

$$\Rightarrow\ 64\sigma_4(y^2) = \left[\tau_1(y^2)^2 - 2\tau_2(y^2)\right]^2.$$

(4) We have the identity $24\sigma_4 = \tau_1^4 - 6\tau_1^2\tau_2 + 8\tau_1\tau_3 + 3\tau_2^2 - 6\tau_4$, and so we obtain the relation

$$5\tau_1(y^2)^4 - 36\tau_1(y^2)^2\tau_2(y^2) + 64\tau_1(y^2)\tau_3(y^2) + 12\tau_2(y^2)^2 - 48\tau_4(y^2) = 0.$$

(5) We can evaluate the power sums of $z_1, \ldots, z_6$ in terms of the even power sums of $y_1, \ldots, y_5$:

$$\begin{aligned}
\tau_1(z) &= 0;\\
\tau_2(z) &= 16\tau_2(y^2) - 2\tau_1(y^2)^2;\\
\tau_3(z) &= 64\tau_3(y^2) - 48\tau_2(y^2)\tau_1(y^2) + 8\tau_1(y^2)^3 = 0;\\
\text{and } \tau_4(z) &= 256\tau_4(y^2) - 256\tau_3(y^2)\tau_1(y^2) + 96\tau_2(y^2)\tau_1(y^2)^2 - 10\tau_1(y^2)^4.
\end{aligned}$$

(6) We then invert these relations to obtain:

$$\begin{aligned}\tau_1(y^2) &= z_6;\\ \tau_2(y^2) &= \frac{1}{16}\tau_2(z) + \frac{1}{8}z_6^2;\\ \tau_3(y^2) &= \frac{3}{64}\tau_2(z)z_6 - \frac{1}{32}z_6^3;\\ \text{and } \tau_4(y^2) &= \frac{1}{256}\tau_4(z) + \frac{3}{128}\tau_2(z)z_6^2 - \frac{5}{128}z_6^4.\end{aligned}$$

(7) Finally, we substitute from (6) into (4) to obtain the relation

$$12z_6^4 - 4\tau_2(z)z_6^2 + \big(\tau_2(z)^2 - 4\tau_4(z)\big) = 0.$$

We now know that $j(Y) \subseteq Z \cap H$ where $H \subset \mathbb{P}^5$ is the hypersurface defined by the equation in (7) above. The degree of $Z \cap H$ is 12, and so to check equality we show that $j(Y)$ has degree 12 as well.

A hyperplane in $\mathbb{P}^5$ pulls back under j to a diagonal quadric in $\mathbb{P}^4$, and indeed every diagonal quadric in $\mathbb{P}^4$ is the pullback under j of a hyperplane in $\mathbb{P}^5$. The intersection of Y and two diagonal quadrics in general position consists of twelve points. It follows that the intersection of $j(Y)$ with two hyperplanes in general position consists of twelve points, that is that the degrees of $j(Y)$ and $Z \cap H$ are equal.

Thus $j(Y)$ is the variety in $\mathbb{P}^5$ defined by the equations

$$\tau_1(z) = \tau_3(z) = 0 \text{ and } 12z_6^4 - 4\tau_2(z)z_6^2 + \big(\tau_2(z)^2 - 4\tau_4(z)\big) = 0.$$

If we write $s_i = \sigma_i(z_1, z_2, z_3, z_4, z_5)$ (so $\sigma_i(z) = z_6 s_{i-1} + s_i$) then these equations can be rewritten as

$$s_1 + z_6 = 0,\ s_3 = s_1 s_2 \text{ and } s_2^2 = 4s_4. \tag{5.4}$$

5.4 Rationality questions

Let k be a number field. Suppose that C is a curve of genus 2, defined over the algebraic closure $\overline{k}$. Let $J = \mathrm{Jac}(C)$ and let z be any corresponding point of the

moduli space Z. The curve C is defined up to isomorphism by the branch locus $a_1, a_2, a_3, a_4, a_5, a_6$ of a canonical map $C \to \mathbb{P}^1$ up to projective equivalence; we can define, then, the invariants of the curve C to be the invariants of this sextuple of points as defined in equations (5.1) and (5.3).

In this section we describe different conditions to do with "definition over k" and characterize them in terms of the coordinates of the point $z \in Z$. We shall talk of $\sigma_i(z)$ but, of course, these are only defined up to scaling $\sigma_i \mapsto \lambda^i \sigma_i$ and so a statement such as "$\sigma_i(z) \in k$" really means "there is some choice of $z_1, \ldots, z_6$ such that $\sigma_i(z) \in k$ and $z = (z_1 : \cdots : z_6)$."

We start by examining what it means for the absolute invariants of C to lie in k.

Lemma 5.4.1 *If C admits a double cover $\pi\colon C \to Q$ of a plane conic Q defined over k such that the branch locus of π is also defined over k then $i_1, i_2, i_3 \in k$. If further C has no nontrivial automorphisms then the converse is also true.*

In any case, $i_1, i_2, i_3 \in k$ corresponds to $\sigma_2(z), \sigma_4(z), \sigma_5(z), \sigma_6(z) \in k$.

Proof The correspondence $i_1, i_2, i_3 \in k$ to $\sigma_2(z), \sigma_4(z), \sigma_5(z), \sigma_6(z) \in k$ follows from the formulae (5.2) and the remark that we are free to rescale the z_i.

Now, for any Galois automorphism $\sigma \in G_k$, it is clear from the definitions (5.1) that the invariants I_s all satisfy $I_s({}^\sigma C) = {}^\sigma I_s(C)$, and so it follows that i_1, i_2 and i_3 all lie in k if and only if C and ${}^\sigma C$ are geometrically isomorphic for all $\sigma \in G_k$. (Compare this with our general discussion on rational points of coarse moduli spaces in section 2.3.) But given $\pi\colon C \to Q$ as in the statement of the lemma, ${}^\sigma\pi = \sigma \circ \pi \circ \sigma^{-1}$ is a double cover ${}^\sigma C \to Q$ with the same branch locus as π and so C and ${}^\sigma C$ are geometrically isomorphic.

Conversely, in the case that C has no nontrivial automorphisms, Mestre [Mes91b] gives an explicit construction of a plane conic Q and a plane cubic M such that C admits a double cover of Q with branch locus $Q \cap M$, and such that Q and M are defined over the field $k(i_1, i_2, i_3)$. □

Lemma 5.4.2 *C admits a double cover $\pi\colon C \to Q$ of a plane conic Q defined over k with branch locus also defined over k if and only if the Kummer surface $K = J/\langle -1\rangle$ has a model over k.*

Proof Suppose $\pi\colon C \to Q$ is as in the statement, and let B be the branch locus on Q. Then we can recover K from the double cyclic cover of $\mathbb{P}^2$ branched over the six lines which are the tangents to Q at points of B as in [Jak94, §1]. (See also the proof of theorem 3.1.3.)

Conversely, suppose that K has a model over k. We claim that the node P on K which lies under the zero of J is defined over k. Then projection through P to $\mathbb{P}^2$ is defined over k and the branch locus, which consists of six lines $L_1, \ldots, L_6$, is defined over k. The composition $C \to J \to K \to \mathbb{P}^2$ then defines a double cover $\pi\colon C \to Q$ of a conic defined over k. The lines L_i are tangent to Q and the branch locus of π is the set of intersections $L_i \cap Q$.

To prove the claim, let P_0 be the zero on J and let $\sigma \in G_k$. Now P_0 is represented by any degree 0 divisor on C of the form $\kappa = T - i(T)$. But then ${}^\sigma\kappa$ maps to the zero of ${}^\sigma J$ because ${}^\sigma i(T) = i({}^\sigma T)$. If $q\colon J \to K$ is the natural map, then ${}^\sigma q$ is the natural map ${}^\sigma J \to K$ (here we use that K is defined over k) and ${}^\sigma q({}^\sigma P_0) = {}^\sigma(q(P_0))$. But there is some $\overline{k}$-isomorphism $\psi\colon J \to {}^\sigma J$ such that ${}^\sigma q \circ \psi = q$ and so ${}^\sigma q({}^\sigma P_0) = q(P_0)$, whence $P = q(P_0)$ is a k-point of K. □

Notice that $I_2, I_4, I_6, I_{10} \in k$ is not sufficient for C (or equivalently, J) to have a model over k. The further condition (assuming that C has no nontrivial automorphisms) is that the conic Q of lemma 5.4.1 has a k-point [Mes91b, §2.1], or equivalently, that the tangent cone at the node on K lying below the zero on J contains a rational ray [CF96, theorem 3.10.1].

We can rewrite this, taking our cue from the discussion in section 2.3.

Lemma 5.4.3 *Suppose that the invariants i_1, i_2, i_3 of the curve C lie in k, and that C has no nontrival automorphisms. Then C defines a class $[\phi] \in H^1(G_k, \mathrm{PGL}_2(\overline{k}))$*

which depends only on the $\overline{k}$-isomorphism class of C and which is trivial exactly when C has a model over k.

Proof After lemma 5.4.1, we know that a curve C as in the statement defines a k-point of the moduli space P_1^6/S_6. This point of P_1^6/S_6 corresponds to the choice of an unordered sextuple $\{a_1, \ldots, a_6\}$ of points of $\mathbb{P}^1$ up to projective equivalence, this being the branch locus of a canonical map $C \to \mathbb{P}^1$. Now, as in our general discussion in section 2.3, for each $\sigma \in G_k$ we can define $\phi(\sigma)$ to be the unique $\overline{k}$-automorphism of $\mathbb{P}^1$ which carries $\{{}^\sigma a_1, \ldots, {}^\sigma a_6\}$ onto $\{a_1, \ldots, a_6\}$. Thus C defines a 1-cocycle ϕ with values in $\mathrm{Aut}(\mathbb{P}^1/\overline{k}) \cong \mathrm{PGL}_2(\overline{k})$.

Varying $\{a_1, \ldots, a_6\}$ within the same projective equivalence class, or equivalently varying the map $C \to \mathbb{P}^1$, replaces $\phi(\sigma)$ with $\psi \circ \phi(\sigma) \circ ({}^\sigma\psi)^{-1}$ for some $\psi \in \mathrm{Aut}(\mathbb{P}^1/\overline{k})$, and hence the class $[\phi] \in H^1(G_k, \mathrm{Aut}(\mathbb{P}^1/\overline{k}))$ is well-defined by the $\overline{k}$-isomorphism class of C.

If C has a model over k then we can choose the a_i to be defined over k as a set, and so $\phi = 1$. If $[\phi]$ is trivial, then there is some $\psi \in \mathrm{Aut}(\mathbb{P}^1)$ such that $\psi = \phi(\sigma) \circ {}^\sigma\psi$ for all $\sigma \in G_k$, and so varying the map $C \to \mathbb{P}^1$ by ψ^{-1} gives a map with branch locus defined over k, which means that C has a model over k. □

Now the cohomology set $H^1(G_k, \mathrm{PGL}_2(\overline{k}))$ classifies forms of $\mathbb{P}^1$ over k [Ser68, X§6], that is k-isomorphism classes of conics defined over k, and the class of a given conic Q is trivial exactly when $Q(k) \neq \emptyset$. As already mentioned in the proof of lemma 5.4.1, Mestre [Mes91b] has given an explicit construction for the conic arising in this manner from a curve of genus 2. Checking whether C has a model over k then becomes, at least computationally, a straightforward matter. We discuss this in detail in chapter 6.

Now suppose that the curve C is defined over k, that is that the branch locus $\{a_1, \ldots, a_6\}$ can be chosen to be defined over k as a set. Then, using the relation between the S_6-actions on P_1^6 and Z, we see that $\{z_1, \ldots, z_6\}$ can be chosen to be Galois and, indeed, that $\mathrm{Gal}(k(z)/k) = \mathrm{Gal}(k(a)/k)^{\mathsf{out}}$ in S_6, where out is the outer

automorphism described in section 5.1. If, further, C has maximal RM by $\mathbb{Q}(\sqrt{5})$ then, by theorem 4.4.3, $\mathrm{Gal}(k(a)/k)$ is contained in $\mathrm{A}_5^{\mathrm{tr}}$; this is mapped by out to a copy of A_5 which fixes one of the z_i. Thus we have the following.

Proposition 5.4.4 *If C has a model over k and J has maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over k then the associated point $z \in j(Y) \subset Z$ satisfies*

(i) *$\{z_1, \ldots, z_6\}$ is defined over k, and*

(ii) *$\mathrm{Gal}(k(z)/k)$, considered as a permutation group on $\{z_1, \ldots, z_6\}$, is contained in a copy of A_5 which fixes one of the z_i. (In particular, $z_i \in k$ for some i.)*

Note that the converse is not true since the obstruction described in lemma 5.4.3 may be nontrivial. We present an example of this in section 6.1.

5.5 Moduli for curves with $\sqrt{5}$-multiplication

Looking at the equations (5.4) for $j(Y)$ and proposition 5.4.4, we see that we can choose z_6, s_2 and $\sigma_5 = \sigma_5(z)$ as moduli for curves C of genus 2 such that $J = \mathrm{Jac}(C)$ has maximal real multiplication by $\mathbb{Q}(\sqrt{5})$. (We disregard the level 2 structure, and so can re-order the coordinates of z at will.)

We can rewrite equations (5.2) in terms of these new invariants, using the equations (5.4). After a little algebra these become

$$\begin{aligned} I_2 &= -2s_2 + 2z_6^2, \\ 16I_4 &= (s_2 + 2z_6^2)^2, \\ 64I_6 &= 36z_6\sigma_5 - 16I_4(3s_2 - 2z_6^2) \\ \text{and } 2^{10}I_{10} &= \sigma_5^2. \end{aligned} \tag{5.5}$$

Next, we observe that $\phi(T) := \prod_{i=1}^{5}(T - z_i)$ can be written

$$\phi(T) = (T + z_6)(T^2 + \frac{1}{2}s_2)^2 - \sigma_5$$

and has discriminant $\Delta_1 = \Delta(z_1, \ldots, z_5)^2$ given by

$$\frac{\Delta_1}{\sigma_5^2} = 8(8z_6^6 s_2^2 + 12z_6^4 s_2^3 + 6z_6^2 s_2^4 + s_2^5) - 8(32z_6^5 + 50z_6^3 s_2 + 125z_6 s_2^2)\sigma_5 + 3125\sigma_5^2. \quad (5.6)$$

We wish to determine those curves C of genus 2 defined over k such that $J = \mathrm{Jac}(C)$ has maximal real multiplication by $\mathbb{Q}(\sqrt{5})$, also defined over k. Proposition 5.4.4 tells us that such C will be given by certain choices of $z_6, s_2, \sigma_5 \in k$ which make Δ_1 a square in k. We can parametrize such triples. The first point to note is that we can complete the square for σ_5 on the right-hand side of equation (5.6) and then obtain

$$5T_4^2 = T_3^2 + T_1^3 T_2^2, \quad (5.7)$$

where we write

$$\begin{aligned} T_1 &= 2(5s_2 - 8z_6^2), \\ T_2 &= 5s_2 + 2z_6^2, \\ T_3 &= 3125\sigma_5 - 128z_6^5 - 200z_6^3 s_2 - 500z_6 s_2^2 \\ \text{and } T_4^2 &= 625\frac{\Delta_1}{\sigma_5^2}. \end{aligned} \quad (5.8)$$

The variety T (in weighted projective space) whose equation is given in (5.7) is a rational variety. Note that the formulae in (5.8) do not give a 1-1 correspondence between points of T and the triples (z_6, s_2, σ_5) in which we are interested, but we can get round this by choosing a parametrization of T carefully. To be precise, let us take three parameters

$$u_1 = \frac{2}{5}z_6, \ u_2 = \frac{T_4}{10T_1T_2} \text{and } u_3 = \frac{T_3}{10T_1T_2}.$$

This gives a parametrization of T, and also parametrizes the triples (z_6, s_2, σ_5) such that Δ_1 is a square. Explicitly, we have

$$\begin{aligned} 2z_6 &= 5u_1, \\ s_2 &= 10(u_1^2 + 5u_2^2 - u_3^2) \\ \text{and } \sigma_5 &= 2(27u_1^5 + 225u_1^3u_2^2 - 45u_1^3u_3^2 + 50u_1^2u_2^2u_3 - 10u_1^2u_3^3 \\ &\qquad + 500u_1u_2^4 - 200u_1u_2^2u_3^2 + 20u_1u_3^4 + 200u_2^4u_3 - 80u_2^2u_3^3 + 8u_3^5). \end{aligned}$$

This completes our description of the moduli space.

For completeness' sake, we list the invariants (z_6, s_2, σ_5) for the family of curves $\mathscr{C}_{AB}$ of equation (3.5).

$$\begin{aligned}
z_6(\mathscr{C}_{AB}) &= -2B + 7 - 7A + A^2,\\
s_2(\mathscr{C}_{AB}) &= 2(-13 + 26A - 7A^2 + 2A^3 + 4B - A^4 + 4A^2B)\\
\text{and } \sigma_5(\mathscr{C}_{AB}) &= 2^5A^2(117 - 338A + 223A^2 - 106A^3 + 29A^4 - 4A^5 - 114B + 240AB\\
&\qquad - 112A^2B + 26A^3B + 37B^2 - 42AB^2 + A^2B^2 - 4B^3).
\end{aligned}$$

We also list (z_6, s_2, σ_5) for Brumer's family [Bru95, equation 6.2], namely

$$\begin{aligned}
C_{bcd} : Y^2 + (X^3 + X + 1 + c(X^2 + X))Y = b &+ (1 + 3b)X + (1 - bd + 3b)X^2\\
&+ (b - 2bd - d)X^3 - bdX^4.
\end{aligned}$$

$$\begin{aligned}
z_6(C_{bcd}) &= 2(5 + 2b + 3c - c^2 + 2d + 4bd),\\
s_2(C_{bcd}) &= 2^5(9 + 22b - b^2 - 9bc + bc^2 + 4d + 5bd - 4b^2d + 3cd\\
&\qquad + c^2d - d^2 - 4bd^2)\\
\text{and } \sigma_5(C_{bcd}) &= 2^{11}(103 + 484b + 567b^2 - 27b^3 + 39c - 27bc - 252b^2c - 4c^2\\
&\qquad - 56bc^2 + 27b^2c^2 - 6c^3 - 13bc^3 + b^2c^3 + c^4 + 9bc^4 - bc^5\\
&\qquad + 34d + 121bd + 66b^2d - 108b^3d + 147cd + 627bcd\\
&\qquad + 720b^2cd - 36b^3cd + 43c^2d - 74bc^2d - 334b^2c^2d - 5c^3d\\
&\qquad - 63bc^3d + 40b^2c^3d - 6c^4d - 12bc^4d + b^2c^4d + c^5d + 9bc^5d\\
&\qquad - bc^6d + 81d^2 + 381bd^2 + 456b^2d^2 - 24b^3d^2\\
&\qquad + 63cd^2 + 96bcd^2 - 132b^2cd^2 - 144b^3cd^2 + 36c^2d^2\\
&\qquad + 80bc^2d^2 + 152b^2c^2d^2 - 8b^3c^2d^2 - c^3d^2 - 52bc^3d^2 - 72b^2c^3d^2\\
&\qquad + bc^4d^2 + 12b^2c^4d^2 - 27d^3 - 216bd^3 - 528b^2d^3\\
&\qquad - 416b^3d^3 + 16b^4d^3 + 36bcd^3 + 192b^2cd^3 + 144b^3cd^3\\
&\qquad - 8b^2c^2d^3 - 48b^3c^2d^3 + 16b^3d^4 + 64b^4d^4).
\end{aligned}$$

Chapter 6

Finding equations for curves

6.1 Equations for curves with $\sqrt{5}$-multiplication

Now that we have an explicit description of the moduli space of pairs of a curve C of genus 2 and an action i of $\mathbb{Z}[\eta]$ on $\mathrm{Jac}(C)$, and know something about the locus cut out by such pairs (C, i) which are defined over $\mathbb{Q}$, our aim is to describe these curves by equations.

There is a method for constructing an equation for a curve of genus 2 from its invariants described by Mestre [Mes91b] (which has already been alluded to in the proof of lemma 5.4.1), but a first step is to tabulate some appropriate values for our invariants (z_6, s_2, σ_5). We can, of course, scale so that z_6, s_2, σ_5 are all integers, but it is better, in order to control the powers of 2 that arise, to take $z_6 \in \frac{1}{2}\mathbb{Z}$, $s_2, \sigma_5 \in \mathbb{Z}$. We note in this case that 2 divides each of s_2 and σ_5.

Another point is that although we could use the parametrization at the end of section 5.5, we prefer to stick with (z_6, s_2, σ_5) since this gives some control over the discriminant of the curve, and so (hopefully) over the conductor.

The results of an exhaustive search for appropriate values of (z_6, s_2, σ_5) over the range $|\sigma_5| \leqslant 206$, $|s_2| \leqslant 50$, $0 \leqslant z_6 \leqslant 50$ are tabulated in section A.3.

Now we review Mestre's method briefly. He uses a different set of invariants (as originally given by Clebsch in the previous century) and, rather than define them

here, we shall simply express them in terms of our chosen set of invariants in the case of RM by $\mathbb{Q}(\sqrt{5})$.

First, he takes a set of invariants (A, B, C, D) which correspond to (I_2, I_4, I_6, I_{10}) and which are given in terms of (z_6, s_2, σ_5) by

$$\begin{aligned}
2^2 3 \cdot 5A &= s_2 - z_6^2, \\
2^5 3^2 5^4 B &= 7s_2^2 - 4s_2 z_6^2 + 12 z_6^4, \\
2^8 3^2 5^6 C &= -3s_2^3 + 100\sigma_5 z_6 - 26 s_2^2 z_6^2 - 4 s_2 z_6^4 + 8 z_6^6 \\
\text{and } 2^{11} 3^6 5^{10} D &= 2s_2^5 - 3125\sigma_5^2 + 1900 s_2^2 \sigma_5 z_6 - 485 s_2^4 z_6^2 - 6800 s_2 \sigma_5 z_6^3 \\
&\quad + 1520 s_2^3 z_6^4 + 400 \sigma_5 z_6^5 - 120 s_2^2 z_6^6 + 160 s_2 z_6^8 + 48 z_6^{10}.
\end{aligned}$$

Mestre also defines several further invariants $\{A_{ij} \mid 1 \leqslant i, j \leqslant 3\}$ and $\{a_{ijk} \mid 1 \leqslant i, j, k \leqslant 3\}$, which can all be written in terms of (A, B, C, D). We simply copy these relations from [Mes91b]. Note that $A_{ij} = A_{ji}$ for all i, j and that $a_{ijk} = a_{ikj} = a_{jik}$ for all i, j, k.

$$\begin{aligned}
A_{11} &= 2C + \tfrac{1}{3}AB & A_{12} &= \tfrac{2}{3}(B^2 + AC) \\
A_{13} &= D & A_{22} &= D \\
A_{23} &= \tfrac{1}{3}B(B^2 + AC) + \tfrac{1}{3}C(2C + \tfrac{1}{3}AB) & A_{33} &= \tfrac{1}{2}BD + \tfrac{2}{9}C(B^2 + AC)
\end{aligned} \tag{6.1}$$

$$\begin{aligned}
36a_{111} &= 8(A^2C - 6BC + 9D) \\
36a_{112} &= 4(2B^3 + 4ABC + 12C^2 + 3AD) \\
36a_{113} &= 4(AB^3 + \tfrac{4}{3}A^2BC + 4B^2C + 6AC^2 + 3BD) \\
36a_{122} &= 36a_{113} \\
36a_{123} &= 2(2B^4 + 4AB^2C + \tfrac{4}{3}A^2C^2 + 4BC^2 + 3ABD + 12CD) \\
36a_{133} &= 2(AB^4 + \tfrac{4}{3}A^2B^2C + \tfrac{16}{3}B^3C + \tfrac{26}{3}ABC^2 + 8C^3 \\
&\quad + 3B^2D + 2ACD) \\
36a_{222} &= 4(3B^4 + 6AB^2C + \tfrac{8}{3}A^2C^2 + 2BC^2 - 3CD) \\
36a_{223} &= 2(-\tfrac{2}{3}B^3C - \tfrac{4}{3}ABC^2 - 4C^3 + 9B^2D + 8ACD) \\
36a_{233} &= 2(B^5 + 2AB^3C + \tfrac{8}{9}A^2BC^2 + \tfrac{2}{3}B^2C^2 - BCD + 9D^2) \\
36a_{333} &= -2B^4C - 4AB^2C^2 - \tfrac{16}{9}A^2C^3 - \tfrac{4}{3}BC^3 + 9B^3D \\
&\quad + 12ABCD + 20C^2D
\end{aligned} \tag{6.2}$$

Let us suppose that we have a curve C with maximal RM by $\mathbb{Q}(\sqrt{5})$, with invariants (z_6, s_2, σ_5), and suppose for now that C has no nontrivial automorphisms. (We shall examine the cases where $\mathrm{Aut}(C)^{\mathrm{red}}$ is not trivial in section 6.3.) The crucial fact is that if we define a plane conic L and cubic M by the equations

$$L : \sum_{i,j} A_{ij} x_i x_j = 0$$
$$\text{and } M : \sum_{i,j,k} a_{ijk} x_i x_j x_k = 0,$$

then the curve C can be recovered as a double cover of L branched over the points of $L \cap M$.

In order to write an equation for C in the usual shape, then, we must calculate the equation for L, and project through a point P on L to determine the images of $L \cap M$ in $\mathbb{P}^1$. The relations are such that if $z_6, s_2, \sigma_5 \in \mathbb{Q}$ then L and M are defined over $\mathbb{Q}$ and so C has a model over $\mathbb{Q}$ exactly when we can choose $P \in L(\mathbb{Q})$. This is a concrete version of the obstruction described in lemma 5.4.3, and raises the question of how to find points on conics, which we discuss in section 6.2.

It is also worth noting that Mestre defines an invariant R such that the discriminant of the conic L is $2R^2$. When C has maximal RM by $\mathbb{Q}(\sqrt{5})$, then R^2 is a square multiple of the discriminant Δ_1 defined in equation (5.6). Explicitly,

$$2^{36}3^{18}5^{20} \cdot R^2 = (4z_6^5 + 4z_6^3 s_2 + z_6 s_2^2 - 2\sigma_5)^2 \Delta_1. \tag{6.3}$$

Now, as has been remarked before, not all of the rational choices for (z_6, s_2, σ_5) which make Δ_1 a square actually correspond to a curve with a model over $\mathbb{Q}$. One example where the obstruction is nontrivial is provided by taking $z_6 = 7/2$, $s_2 = 8$ and $\sigma_5 = 14$. We can check (by using the criteria of section 6.3) that a curve with these invariants has no nontrivial automorphisms. In this case, the invariants A_{ij} are

$$A_{11} = \frac{-1655981}{2592000000}, \qquad A_{12} = \frac{124837043}{1555200000000},$$
$$A_{13} = A_{22} = \frac{6150111571}{933120000000000}, \qquad A_{23} = \frac{255358687187}{559872000000000000}$$
$$\text{and } A_{33} = \frac{9642570072739}{3359232000000000000}.$$

We can transform the equation for L to

$$x_1^2 - 5x_2^2 - 26x_3^2 - 2x_2x_3 = 0$$

(see section 6.2), and now it is a routine matter to check that $L(\mathbb{Q}) = \emptyset$ since this new equation has discriminant $3 \cdot 43$ but has no 3-adic points and no 43-adic points.

Finally for this section, we give an example in detail to show how the calculation goes. We start from $z_6 = 5/2$, $s_2 = 18$ and $\sigma_5 = 206$. (This isomorphism class has a Jacobian which is a simple factor of $J_0(103)$ and appears in Wang's tables [Wan95].) From the formulae (5.5), we obtain

$$I_2 = \frac{-47}{2},\ I_4 = \frac{61^2}{2^6},\ I_6 = \frac{-11 \cdot 14593}{2^9} \text{ and } I_{10} = \frac{103^2}{2^8}.$$

Calculating the invariants A_{ij} gives

$$A_{11} = \frac{-219743}{864000000}, \qquad A_{12} = \frac{19108301}{518400000000},$$

$$A_{13} = A_{22} = \frac{-3718418807}{311040000000000}, \qquad A_{23} = \frac{52268246549}{186624000000000000}$$

$$\text{and } A_{33} = \frac{-9248523360143}{111974400000000000000}.$$

Note that $R = (7 \cdot 23 \cdot 103)/(2^{16}5^{10})$ and $\Delta_1 = 2^{10}3^4 23^2 103^2$, in accordance with equation (6.3).

By using the methods of section 6.2, the equation for L can be reduced to give

$$8x_2^2 + 11x_3^2 + 2x_1x_2 + 2x_1x_3 + 4x_2x_3 = 0;$$

after the same change of coordinates, the equation for M becomes

$$\begin{aligned} 1375x_1^3 &+ 13650x_1^2x_2 + 18150x_1^2x_3 + 1800x_1x_2^2 + 162900x_1x_2x_3 \\ &+ 44100x_1x_3^2 - 8072x_2^3 + 89544x_2^2x_3 + 340104x_2x_3^2 + 39988x_3^3 = 0. \end{aligned}$$

The conic L has an obvious $\mathbb{Q}$-point, namely $(1 : 0 : 0)$. Projecting through this point, the images of $L \cap M$ are the roots of the sextic polynomial

$$34112x^6 - 2688x^5 - 65120x^4 + 118640x^3 - 29420x^2 + 30372x + 34877;$$

scaling x by a factor of 2 gives the polynomial

$$f(x) = 533x^6 - 84x^5 - 4070x^4 + 14830x^3 - 7355x^2 + 15186x + 34877.$$

This polynomial has Galois group contained in $\mathrm{A}_5^{\mathrm{tr}}$ as it should (see theorem 4.4.3).

Now the invariants for the model we have here are

$$I_2 = -2^3 5^{10} 47,\ I_4 = 2^2 5^{20} 61^2,\ I_6 = -2^3 5^{30} 11 \cdot 14593 \text{ and } I_{10} = 2^{12} 5^{50} 103^2.$$

Comparing these with the ones we started with it is at least clear that we have a curve from the correct $\overline{\mathbb{Q}}$-isomorphism class. However, we would prefer to find an equation $y^2 = g(x)$ such that the odd part of the discriminant of g is 103^2; then the conductor of this curve would have no odd factors other than 103. Note that the invariants (z_6, s_2, σ_5) determine only the $\overline{\mathbb{Q}}$-isomorphism class of the curve, whereas the conductor varies with the $\mathbb{Q}$-isomorphism class.

In this case, we might consider a twist defined over $\mathbb{Q}(\sqrt{5})$. Specifically, consider the curve $y^2 = 5f(x)$. Liu's program `genus2reduction` calculates a $\mathbb{Z}[1/2]$-minimal model $y^2 = g(x)$ for this curve, where

$$\begin{aligned} g(x) &= 5^{-11} f(25x + 18) \\ &= 2665x^6 + 11496x^5 + 20630x^4 + 19718x^3 + 10589x^2 + 3030x + 361. \end{aligned}$$

We note that the discriminant of g is $2^{12}103^2$ and that the odd part of the conductor of this curve is 103^2.

There is now one more technique we use to reduce the size of the coefficients. Let us define the *size* of a polynomial to be the sum of the squares of the coefficients. Now, given an equation $y^2 = g(x)$, we can transform by a linear change to the x-coordinate to ensure that the new coefficient of x^5 is less than 6 times the coefficient of x^6 in modulus. Very often this will reduce the size of the polynomial on the right-hand side as well. Then we are free to reverse the order of the coefficients on the right-hand side (that is, to make the change of coordinates $(x, y) \mapsto (1/x, y/x^3)$) and repeat this process for as long as the size of the right-hand side continues to decrease.

For the equation $y^2 = g(x)$ above, we find that we can transform to

$$\begin{aligned} y^2 &= (4x-1)^6 g\left(\frac{1-3x}{4x-1}\right) \\ &= x^6 + 6x^5 - 19x^4 + 22x^3 - 10x^2 + 1. \end{aligned}$$

The table of invariants in section A.3 lists whether or not the associated curve has a model over $\mathbb{Q}$. When there is a model over $\mathbb{Q}$, an equation has been found using the methods described above (including the techniques for reducing the sizes of the coefficients). Further, the odd part of the conductor of the model has been calculated using `genus2reduction`, and these are tabulated.

6.2 Finding points on conics

A key step in the procedure described in the previous section is the effective determination of points on conics defined over $\mathbb{Q}$. We now outline the methods used in compiling the table in section A.3.

Suppose that the conic L has the equation given by the symmetric matrix A. We shall say that we *transform by the matrix* $P \in \mathrm{GL}_2(\mathbb{Q})$ if we make a coordinate transformation so as to replace A by $P^{\mathrm{t}}AP$. We may suppose that the initial matrix has entries in $\mathbb{Z}$, and at each stage we note that we are free to clear the denominators and remove common factors from the transformed matrix $P^{\mathrm{t}}AP$.

First, we describe a procedure reducedet which finds a matrix P such that the transformed matrix $P^{\mathrm{t}}AP$ has squarefree determinant.

Suppose that p is a prime such that $p^2 \mid \det A$. Then there is some linear combination (over $\mathbb{Z}$) of the rows of A which is a multiple of p. Thus there is some $P_1 \in \mathrm{SL}_3(\mathbb{Z})$ such that

$$P_1{}^{\mathrm{t}} A P_1 \equiv \begin{pmatrix} 0 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \pmod{p}.$$

We can readily determine such a matrix P_1 given a nonzero vector in the kernel of A mod p, and such a vector can be found by performing row reduction on A mod p. (Compare with [Coh95, algorithm 2.3.1], which computes the kernel of a matrix.)

Since $p^2 \mid \det A$, one of the following two cases must hold:

(1) p^2 divides the top left entry in ${P_1}^{\mathrm{t}} A P_1$; or

(2) p divides the determinant of the bottom right 2×2 minor of ${P_1}^{\mathrm{t}} A P_1$.

In case (1), we may further transform by the matrix

$$P_2 = \begin{pmatrix} \frac{1}{p} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

note that $\det({P_2}^{\mathrm{t}} {P_1}^{\mathrm{t}} A P_1 P_2) = p^{-2} \det A$.

In case (2), we may transform by some $P_2 \in \mathrm{SL}_3(\mathbb{Z})$ so that

$${P_2}^{\mathrm{t}} {P_1}^{\mathrm{t}} A P_1 P_2 \equiv \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & * \end{pmatrix} \pmod{p}.$$

Transforming further by the matrix $P_3 = \mathrm{diag}(1, 1, p)$, we may clear a factor of p from $(P_1 P_2 P_3)^{\mathrm{t}} A (P_1 P_2 P_3)$. The determinant of this transformed matrix is then $p^{-1} \det A$.

Iterating this process for every prime p such that p^2 divides the determinant, we arrive at a transformed matrix which has squarefree determinant as desired.

In our example at the end of section 6.1 (starting from $z_6 = 5/2$, $s_2 = 18$ and $\sigma_5 = 206$) we have the following initial matrix for L after clearing denominators and common factors:

$$A = \begin{pmatrix} -28478692800000000 & 4127393016000000 & -1338630770520000 \\ 4127393016000000 & -1338630770520000 & 31360947929400 \\ -1338630770520000 & 31360947929400 & -9248523360143 \end{pmatrix}.$$

The determinant of A is $2^{38}3^{21}5^{22}7^2 23^2 103^2$.

Applying reducedet, we find that

$$A_1 := -\tfrac{1}{5}P^{\mathrm{t}}AP = \begin{pmatrix} 2587456485 & 927383819 & 3305520465 \\ 927383819 & 332388556 & 1184748867 \\ 3305520465 & 1184748867 & 4222859640 \end{pmatrix},$$

$$\text{where } P = 2^{-13}3^{-8}5^{-5}7^{-1}23^{-1}103^{-1} \cdot P' \tag{6.4}$$

$$\text{and } P' = \begin{pmatrix} 11485777794 & 4124446201 & 14670927982 \\ 2114602809840 & 759332751096 & 2701009664400 \\ 106782738912000 & 38272305916800 & 136416875040000 \end{pmatrix}.$$

Note that $\det(A_1) = 15$.

Our next step is to try to perform further unimodular transformations so as to reduce the size of the entries in the transformed matrix. For our purposes, we shall call a 3×3 symmetric integer matrix $A = (a_{ij})$ *reduced* if it satisfies the inequalities $|a_{11}| \leqslant |a_{22}| \leqslant |a_{33}|$, as well as $\frac{1}{2}|a_{11}| \geqslant |a_{12}|, |a_{13}|$ when $a_{11} \neq 0$, and $\frac{1}{2}|a_{22}| \geqslant |a_{23}|$ when $a_{22} \neq 0$. We aim to transform a given matrix into a reduced matrix by some $P \in \mathrm{SL}_3(\mathbb{Z})$, and proceed by a naïve approach.

Let swap denote the following procedure: given A, find a permutation $\sigma \in \mathrm{S}_3$ such that $|a_{\sigma(1),\sigma(1)}| \leqslant |a_{\sigma(2),\sigma(2)}| \leqslant |a_{\sigma(3),\sigma(3)}|$ by performing a bubble sort on the triple $(|a_1|, |a_2|, |a_3|)$; let P be the permutation matrix corresponding to σ.

Then define the procedure reducefirst as follows: call swap and then, when $a_{11} \neq 0$, transform by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ -q & 1 & 0 \\ -q' & 0 & 1 \end{pmatrix},$$

where q is the closest integer to a_{12}/a_{11} and q' is the closest integer to a_{13}/a_{11}, repeating both steps until the transformed matrix A satisfies $|a_{11}| \leqslant |a_{22}| \leqslant |a_{33}|$ as well as $\frac{1}{2}|a_{11}| \geqslant |a_{12}|, |a_{13}|$ when $a_{11} \neq 0$.

Now define reduce as follows: call reducefirst and then, when $a_{22} \neq 0$, transform by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -q & 1 \end{pmatrix},$$

where q is the closest integer to a_{23}/a_{22}, repeating both steps until the transformed matrix is reduced.

Note that for arbitrary initial matrices, reduce need not terminate. In the following example each direction of the arrow indicates one complete loop in reduce:

$$\begin{pmatrix} -5 & 2 & 3 \\ 2 & 5 & 1 \\ 3 & 1 & 5 \end{pmatrix} \longleftrightarrow \begin{pmatrix} -5 & 2 & -4 \\ 2 & 5 & -2 \\ -4 & -2 & 5 \end{pmatrix}$$

When encoding reduce, the easiest way to avoid this problem is simply to restrict the maximum number of iterations allowed; a maximum of 12 iterations sufficed for the cases encountered in compiling the table in section A.3. We note that, in these cases, reduce terminates for all but the curve corresponding to $z_6 = 9/2$, $s_2 = 4$ and $\sigma_5 = -106$. Further, this method produces transformed matrices with much smaller entries than the original matrices. We also note that, experimentally at least, reduce does terminate very often (tests with a large number of random matrices suggest a failure rate of less than 2%).

Taking up our example again, applying reduce to the matrix A_1 of (6.4), we determine that

$$A_2 := Q^{\mathrm{t}} A_1 Q = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 8 & 2 \\ 1 & 2 & 11 \end{pmatrix}, \text{ where } Q = \begin{pmatrix} -56854 & 59680 & 14017 \\ 12420 & -13037 & -3062 \\ 41019 & -43058 & -10113 \end{pmatrix}.$$

In the example we have been following, we have an obvious rational point on the transformed equation for L, namely $(1 : 0 : 0)$. It need not always be the case that the transformed equation produced by applying reducedet and reduce has such an obvious rational point, and so we need some way to find rational points in general.

Suppose, then, that we are given a 3×3 symmetric integer matrix $A = (a_{ij})$.

Theorem 6.2.1 (Cassels, Davenport) *Given that the equation $x^{\mathrm{t}}Ax = 0$ has a nonzero solution $x \in \mathbb{Z}^3$, there is a solution with*

$$0 < \sum_{i=1}^{3} x_i^2 \leqslant \frac{32}{3} \sum_{i,j=1}^{3} a_{ij}^2.$$

Proof In this form, this is quoted from [Dav57], using the fact that Hermite's constant γ_2 is $2/\sqrt{3}$, achieved by the triangular lattice A_2. Note that there is a slight error in the original paper which has been corrected in the collected works. □

Thus a simple search procedure yields an effective method for determining integer points on a conic, if there are any. We may apply our procedures reducedet and reduce to assume that $\det A$ is squarefree, and to reduce the size of the search region suggested by theorem 6.2.1. It is also useful to solve $x^{\mathrm{t}}Ax = 0$ modulo $\det A$ in order to reduce the size of the search region further. When doing this in practice, one might consider first finding a matrix $P \in \mathrm{SL}_3(\mathbb{Z})$ such that $P^{\mathrm{t}}AP$ is diagonal modulo $\det(A)$ as this then reduces the problem to determining square-roots modulo primes, which can be done by Shanks' algorithm [Coh95, algorithm 1.5.1].

The combination of reducedet, reduce and then the method of search suggested above does seem in practice to be a very fast method of finding rational points on conics. Also, when applied as part of the method of section 6.1 for finding equations for curves of genus 2 with a $\sqrt{5}$-multiplication, this technique seems a good way to reduce the size of the coefficients of the final equation.

6.3 Curves with nontrivial automorphisms

In this section we examine the invariants for those curves of genus 2 with nontrivial automorphisms and maximal RM by $\mathbb{Q}(\sqrt{5})$. These are precisely those not covered by the methods of section 6.1.

We shall work from Bolza's classification (see section 2.5), and we are particularly interested in those curves defined over $\mathbb{Q}$ with the RM by $\mathbb{Q}(\sqrt{5})$ also defined over $\mathbb{Q}$. Bolza gives a second table, which we reproduce here, which classifies the different reduced automorphism groups in terms of Clebsch's invariants.

Type	$\mathrm{Aut}^{\mathrm{red}}$	Relations between invariants	
I	C_2	$R = 0$	$A_{11}A_{22} - A_{12}^2 \neq 0$
II	C_5	$A = B = C = 0$	$D \neq 0$
III	D_4	$3AB^2 - 6BC + 4A^2C - 18D = 0$	$D \neq 0$
		$4B^3 + 5ABC + 6C^2 - 3AD = 0$	$6C^2 - B^3 \neq 0$
IV	D_6	$6C^2 - B^3 = 0$	$D \neq 0$
		$9D - 2B(6C + AB) = 0$	$2AB - 15C \neq 0$
V	D_{12}	$6B - A^2 = D = 6C + AB = 0$	$A \neq 0$
VI	S_4	$B = C = D = 0$	$A \neq 0$

As we remarked in section 2.5, it is possible to view types I and III–VI as specializations of the same condition, and it is straightforward to verify that this condition is just $R = 0$.

A curve of type II has CM by a 5th root of unity and so such a curve will always have maximal RM by $\mathbb{Q}(\sqrt{5})$. Moreover, all these curves are geometrically isomorphic; the corresponding point of our moduli space $j(Y)$ is just given by $z_6 = s_2 = 0$. However, then the discriminant Δ_1 becomes $3125\sigma_5^2$, and so none of these curves can be defined over $\mathbb{Q}$ and have the RM by $\mathbb{Q}(\sqrt{5})$ defined over $\mathbb{Q}$ as well.

Now let us look at the other cases. Let C be a (smooth) curve over $\mathbb{Q}$ with maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over $\mathbb{Q}$, and with a nontrivial automorphism of order 2 (that is C lies in one of cases I, or III–VI). As remarked in section 2.5, the Jacobian of C must be isogenous over $\overline{\mathbb{Q}}$ to a product of elliptic curves; for there to be RM by $\mathbb{Q}(\sqrt{5})$, the Jacobian must be isogenous to the square of an elliptic curve and the RM is then defined over $\mathbb{Q}$ when this isogeny is defined over $\mathbb{Q}$.

In terms of invariants, we must have that $R = 0$, which, from equation (6.3), forces one of

$$\sigma_5 = 0,\ \Delta_1 = 0,\ \text{or } 2\sigma_5 = 4z_6^5 + 4z_6^3 s_2 + s_2^2 z_6.$$

We cannot have $\sigma_5 = 0$ since then C would be singular. Also, assuming the third

condition allows us to write

$$4\Delta_1 = (32s_2 + 37z_6^2)(s_2 + 18z_6^2)^2(s_2 + 2z_6)^2.$$

Hence one of the following two cases must hold:

(1) $\Delta_1 = 0$;

(2) $2\sigma_5 = 4z_6^5 + 4z_6^3 s_2 + z_6 s_2^2$ with $32s_2 + 37z_6^2$ a square in $\mathbb{Q}$.

Now we can find all the rational invariants (z_6, s_2, σ_5) for nonsingular curves which lie in types III–VI. We have two conditions here, namely $R = 0$ and $A_{11}A_{22} - A_{12}^2 = 0$. We can write out R^2 and $A_{11}A_{22} - A_{12}^2$ as polynomials in z_6, s_2 and σ_5, and then take the resultant with respect to σ_5: this must be zero if these invariants give a curve with an automorphism group as in types III–VI. This condition factorizes to

$$s_2^6 z_6^8 (5s_2 + 2z_6^2)^2 (5s_2 - 8z_6^2)^2 (32s_2 + 37z_6^2)^4 (s_2 + 18z_6^2)^6 (s_2 + 2z_6^2)^{24}$$

and so we have just seven relations between z_6 and s_2 to check.

(1) If $s_2 = 0$ then the two conditions become

$$\sigma_5^3(256z_6^5 - 3125\sigma_5)(2z_6^5 - \sigma_5)^2 = 0$$
$$\text{and } z_6\sigma_5(-375\sigma_5^2 - 257z_6^5\sigma_5 + 16z_6^{10}) = 0,$$

so the only choice is to take $\sigma_5 = 0$, which leads to a singular curve.

(2) If $z_6 = 0$ then we again are forced to take $\sigma_5 = 0$.

(3) If $5s_2 + 2z_6^2 = 0$ then we must take $3125\sigma_5 = 128z_6^5$, and so we have that $(z_6, s_2, \sigma_5) \sim (5, -10, 128)$, that is these are equal up to rescaling. This appears in our table in section A.3 and is of type III.

(4) If $5s_2 - 8z_6^2 = 0$ we get $(z_6, s_2, \sigma_5) \sim (5, 40, 1728)$, and this curve is of type IV.

(5) If $32s_2 + 37z_6^2 = 0$ we get $(z_6, s_2, \sigma_5) \sim (8, -74, 11664)$ and this is of type III.

(6) If $s_2 + 18z_6^2 = 0$ we get $(z_6, s_2, \sigma_5) \sim (1, -18, 128)$. This is given in our table in section A.3 and is of type IV.

(7) Last, taking $s_2 + 2z_6^2$ forces $\sigma_5 = 0$.

It is quite a simple matter to find equations for these curves of types III and IV. One can take the canonical form given by Bolza (see the table in section 2.5), and write down the invariants A, B, C and D in terms of the parameters in the form, then solve the resulting simultaneous equations.

As an example, take case 6 above, where $(z_6, s_2, \sigma_5) \sim (1, -18, 128)$. This is of type IV, so must have an equation of the shape

$$y^2 = x^6 + \alpha x^3 + 1$$

for some α. The invariants for such a model are

$$\begin{aligned} A &= \frac{1}{20}(40 - \alpha^2) \\ B &= \frac{1}{3750}(2500 + 100\alpha^2 + \alpha^4) \\ C &= -\frac{1}{562500}(125000 + 7500\alpha^2 + 150\alpha^4 + \alpha^6) \\ \text{and } D &= -\frac{1}{703125000}\alpha^2(6250000 + 500000\alpha^2 + 15000\alpha^4 + 200\alpha^6 + \alpha^8) \end{aligned}$$

and taking $(z_6, s_2, \sigma_5) \sim (1, -18, 128)$ translates to taking Clebsch's invariants to be $(A, B, C, D) \sim (-19/60, 49/3750, 343/562500, -26411/18984375000)$.

Solving the simultaneous equations given by equating $(B/A^2), (C/A^3)$ and (D/A^5) gives $4\alpha^2 + 11 = 0$. This is not yet a model over $\mathbb{Q}$, but we only need to rescale x and y to obtain the equation

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

The other cases are dealt with in a similar way, and the results are tabulated in section A.3. A point to note is that the models we produce in this way do not have the RM by $\mathbb{Q}(\sqrt{5})$ defined over $\mathbb{Q}$, although some twist will do.

Appendix A

Tables

A.1 Principally polarized factors of $J_0(N)$ with $\sqrt{5}$-multiplication

Wang [Wan95] has determined the 2-dimensional factors of $J_0(N)$ for $N < 200$ and, in the case that the factor is principally polarized, has calculated values of Igusa's invariants which give a curve whose Jacobian is isogenous to the given factor of $J_0(N)$.

In the table, N is the conductor, and z_6, s_2, σ_5 are the invariants defined in sections 5.1 and 5.3.

I have used the methods of section 6.1 to find models for these curves, largely as a way of checking the method by verifying that the models produced have the correct conductor. These are given by taking $y^2 = f(x)$, where f is as tabulated.

N	$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$	$f(x)$
23	$3\cdot 5$	$2\cdot 23$	23^3	$x^6+2x^5-23x^4+50x^3-58x^2+32x-11$
31	23	$-2\cdot 31$	-31^2	$x^6-2x^5-81x^4+468x^3-689x^2+46x-447$
67	1	3^2	67	$x^6+8x^5-18x^4+14x^3-3x^2-2x+1$
73	5	3^2	-73	$x^6-2x^5-3x^4+6x^3+6x^2-16x+9$
87	5	$-2\cdot 3$	3^229	$-x^6+2x^4+6x^3+11x^2+6x+3$
93	3^2	13	3^231	$x^6-6x^5+5x^4+6x^3+2x^2-1$
103	5	3^2	103	$x^6+6x^5-19x^4+22x^3-10x^2+1$
107	5	$-2\cdot 3$	107	$x^6+10x^5-371x^4+3118x^3-12010x^2$ $+22456x-16575$
115	1	-3	5^223	$-x^6+6x^5-5x^4+10x^3-2x^2-1$
125	5	0	5^3	$3x^6+4x^5-20x^4-80x^3-160x^2-128x-64$
133	83	$-2\cdot 3\cdot 7\cdot 41$	-7^219	$-7x^6-98x^5-409x^4-204x^3+1111x^2$ $-722x+137$
133	7	3^2	$7\cdot 19$	$x^6-8x^5+10x^4-6x^3+5x^2-2x+1$
161	7	$2\cdot 3\cdot 5$	7^223	$5x^6-6x^5-37x^4-36x^3+11x^2+42x+85$
167	3^2	2	167	$-x^6+2x^5+3x^4-14x^3+22x^2-16x+7$
175	1	$-2\cdot 7$	5^27^2	$-17x^6+26x^5+155x^4-570x^3+770x^2$ $-464x+247$
177	3	2^2	$3\cdot 59$	$-3x^6+56x^4+176x^3+272x^2+192x+64$
177	17	2^23^219	-3^25^659	$3x^6-12x^5-10x^4+14x^3-x^2-6x+63$
188	2	$3\cdot 5$	2^447	$x^5+34x^4+463x^3+3158x^2+10792x+14785$
191	7	2^23	191	$x^6-6x^5+5x^4+2x^3+2x^2+1$

A.1. Principally polarized factors of $J_0(N)$ with $\sqrt{5}$-multiplication

A.2 Some conductors of the curves $\mathscr{C}_{AB}$

We list the odd part of the conductors of the curves $\mathscr{C}_{AB}$, as given in equation (3.5), with parameter values $A = 1$ and $-20 \leqslant B \leqslant 20$. Note that the odd part of the conductor is the square of the tabulated value N_{odd}.

These values were computed using Liu's program `genus2reduction`. This program also gives some information about the reduction type modulo 2 and in each case the Jacobian had potentially good reduction at 2 as the product of two elliptic curves each with j-invariant 0.

B	-20	-19	-18	-17	-16	-15	-14
N_{odd}	$53 \cdot 557$	25153	$17 \cdot 1249$	17737	11^2	$7 \cdot 13 \cdot 131$	$41 \cdot 233$
B	-13	-12	-11	-10	-9	-8	-7
N_{odd}	$11 \cdot 683$	$53 \cdot 109$	$29 \cdot 149$	3121	2153	$7 \cdot 199$	$19 \cdot 43$
B	-6	-5	-4	-3	-2	-1	0
N_{odd}	401	11^2	47	127	$11 \cdot 13$	$7 \cdot 17$	79
B	1	2	3	4	5	6	7
N_{odd}	47	47	103	239	479	$7 \cdot 11^2$	1367
B	8	9	10	11	12	13	14
N_{odd}	2063	$11 \cdot 269$	4079	$13 \cdot 419$	$19 \cdot 373$	$7 \cdot 1289$	11279
B	15	16	17	18	19	20	
N_{odd}	13879	$17 \cdot 991$	11^2167	$29 \cdot 827$	$163 \cdot 173$	$7 \cdot 11 \cdot 61$	

A.3 Invariants for curves with $\sqrt{5}$-multiplication

The table below lists all possible invariants for curves C defined over $\mathbb{Q}$ with maximal real multiplication by $\mathbb{Q}(\sqrt{5})$ also defined over $\mathbb{Q}$ with $|\sigma_5| \leqslant 206, |s_2| \leqslant 50$ and $z_6 \leqslant 50$ (note that we always choose $z_6 \geqslant 0$). The fourth column indicates one of three things. If the associated curves have nontrivial automorphisms then the type of the reduced automorphism group (as in section 6.3) is indicated. If the associated curves have no nontrivial automorphisms, and also no model defined over $\mathbb{Q}$, then this column is left blank. Otherwise, we give a polynomial $f(x)$ such that $y^2 = f(x)$ is an equation for a curve from the relevant isomorphism class. (These equations were found using the methods detailed in chapter 6.) For these equations, the odd part N^2_{odd} of the conductor is also tabulated, as calculated using `genus2conductor`.

We note that, of the 93 tabulated sets of values for the invariants, 19 give curves with nontrivial automorphisms. Of the remaining 74 cases, 57 have a model defined over $\mathbb{Q}$.

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
1	-3	-1	Type I	
3	-2^2	-1	$3x^6 + 8x^5 + 54x^4 - 26x^3 - 173x^2 + 218x - 73$	29^2
3	1	1	Type I	
5	0	-1	$-3x^6 + 34x^5 + 155x^4 - 20x^3 - 125x^2 - 14x + 37$	5^3
0	5	2^2	$x^6 + 4x^5 + 5x^2 - 8x + 3$	5^3
3	-2^3	-2^2	Type I	
5	0	2^2	Type I	
5	0	5	$-7x^6 - 82x^5 - 25x^4 - 140x^3 + 55x^2 - 34x + 41$	5^4
5	0	-5	$-x^6 + 10x^4 - 30x^3 - 5x^2 + 18x - 5$	5^4
3	-2	7	$11x^6 + 26x^5 + 59x^4 + 26x^3 - 26x^2 - 52x - 37$	$7 \cdot 19^2$
5	$2 \cdot 5$	-7	$3x^6 - 2x^5 - 25x^4 + 30x^3 + 50x^2 - 112x + 63$	$5^2 7$

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
7	2^2	7		
0	-5	2^3	Type I	
2^2	3	2^3	Type I	
5	$-3\cdot 5$	-3^2	Type I	
5	0	3^2	$-3x^6-12x^5-10x^4-10x^3+5x^2+6x+9$	$3\cdot 5^3$
7	-3	3^2	Type I	
3	-2^2	-11	$513x^6-6158x^5-14457x^4-1060x^3+6079x^2$	
			$-13550x-16423$	$11\cdot 71^2$
0	-5	2^23	$-x^6-5x^4+10x^2-12x+5$	$3\cdot 5^3$
2^23	5^2	-2^23		
3	2^2	13	$4357x^6-7574x^5-19245x^4+138028x^3$	
			$-117477x^2+288458x+356525$	$13\cdot 89^2$
0	5	2^4	$4x^5-5x^4+15x^2-20x+8$	5^3
1	-2	2^4		
2^2	1	2^4	$-3x^6+20x^5-25x^4+24x^3+123x^2$	
			$-172x+161$	11^2
5	0	-2^4	$4x^6+4x^5-35x^4+50x^2+28x+13$	5^3
$2\cdot 3$	5	-2^4		
7	-2^33	-2^4	Type I	
3^2	-2^3	2^4	Type I	
$2\cdot 5$	-11	2^4		
2^25	$-3\cdot 5$	-2^4	$-150x^6+550x^5-1025x^4-6800x^3-8695x^2$	
			$-4400x-796$	5^219^2
5	$-3\cdot 5$	-17	$-x^6-12x^5+10x^4-10x^3+55x^2-66x+23$	5^317

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
5	$-2\cdot 3$	-17	$-179x^6-360x^5+590x^4+1558x^3+941x^2$ $+774x+721$	$11^2 17\cdot 19^2$
$3\cdot 5$	$-2\cdot 5$	-17	$181x^6+64x^5-5430x^4-12930x^3-635x^2$ $+5338x+1577$	$5^3 11^2 17$
2^2	-3	$-2^2 5$	$39985x^6+32170x^5-80161x^4-5716x^3$ $+185359x^2-45974x-40991$	$5\cdot 11^2 31^2$
5	0	$2^2 5$	$-4x^6-4x^5+5x^4+10x^3+25x^2+8x+8$	5^4
3	$2\cdot 5$	23	$x^6-2x^5-3x^4+10x^3-6x^2-4x+5$	23
5	2^2	23		
$2\cdot 3$	1	$-2^3 3$		
$3^2 5$	$2\cdot 5$	$2^3 3$	$96x^6+1536x^5+365x^4-44610x^3+126845x^2$ $-126768x+42672$	$3\cdot 5^3 79^2$
11	$-3\cdot 5$	5^2	Type I	
41	2^4	-5^2		
1	-7	3^3	Type I	
3	$2\cdot 11$	-3^3	$239x^6-858x^5-653x^4+278x^3+4510x^2$ $+5880x+2007$	$3\cdot 449^2$
5	5	3^3	Type I	
5	$2\cdot 3$	-3^3	$3x^6-78x^5+821x^4+172x^3+125x^2$ $+2466x+1035$	$3\cdot 29^2$
31	$-2\cdot 3$	3^3	$309x^6-20208x^5-114242x^4-207454x^3$ $-107147x^2+62202x+56169$	$3\cdot 991^2$
0	-5	$2^2 7$	$-175x^6-350x^5-25x^4+700x^3+1615x^2$ $+1666x+665$	$5^3 7$

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
2^3	-5	-2^27	$19x^6-22x^5-361x^4-540x^3-142x^2$	
			$-44x-149$	$7\cdot 89^2$
2^23	-13	-2^27	$x^6-4x^5-19x^4+100x^3-6x^2-16x+3$	$7\cdot 11^2$
7	-2	31	$-x^6+2x^5-x^4-2x^3+6x^2-4x+3$	31
2	-5	2^5		
3	$2\cdot 5$	2^5	$2x^6+4x^5+263x^4-284x^3+1036x^2$	
			$+160x-64$	41^2
3^2	2^2	$3\cdot 11$		
13	-2^33	2^23^2	Type I	
0	5	2^211	$x^6+2x^5+15x^4+10x^2+2x-1$	5^211
5	0	-3^25	$3x^6-6x^5-25x^4+70x^3-70x^2+48x-21$	$3\cdot 5^4$
3	-7	7^2	$7x^6-14x^5+41x^4-468x^3-631x^2$	
			$-1054x-1017$	$7\cdot 11^2$
5	$-3\cdot 5$	-7^2	$x^6-8x^5+10x^4-70x^3+5x^2-2x+1$	5^37^2
5	$-2\cdot 7$	-7^2		
5	0	7^2	$5x^6-6x^5+25x^4-10x^3+10x^2-7$	5^37
1	-2^23	-53	$-101x^6+494x^5+1611x^4+3174x^3+4770x^2$	
			$+3916x+1215$	$53\cdot 239^2$
3^2	2	-53	$18939x^6-1618x^5-566813x^4+1173234x^3$	
			$-801602x^2+312448x-138601$	$11^253\cdot 71^2$
5	$2\cdot 5$	2^37	$x^6+2x^5+35x^4+180x^3+380x^2+448x+256$	5^37
$3\cdot 5$	2^2	59	$2965x^6-3116x^5-17430x^4+23290x^3$	
			$+20565x^2-40090x+14609$	$5^259\cdot 61^2$
29	-2^25	59	$13x^6-118x^5-231x^4+1742x^3+5670x^2$	
			$+5776x+1973$	$59\cdot 61^2$

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
3^2	-2^2	61	$-16331x^6 - 8312x^5 + 24112x^4 + 187136x^3$	
			$+428800x^2 + 444416x + 643072$	$61 \cdot 101^2$
13	-2^3	61	$15x^6 + 682x^5 + 8415x^4 + 44198x^3 + 110110x^2$	
			$+122452x + 42955$	$11^2 19^2 61$
2	-3^2	2^6	Type IV	
$2 \cdot 3$	7	2^6	Type I	
$2 \cdot 5$	-5	2^6	Type III	
1	3^2	67	$x^6 + 8x^5 - 18x^4 + 14x^3 - 3x^2 - 2x + 1$	67
$2^2 3$	11	$-2^2 17$		
5	2^4	71		
3^2	$-2 \cdot 11$	-71	$109x^6 - 398x^5 + 5195x^4 - 32212x^3 - 104589x^2$	
			$-91550x - 22251$	$71 \cdot 359^2$
0	-5	$2^3 3^2$	$375x^5 + 250x^4 + 250x^3 + 100x^2 + 15x + 2$	$3 \cdot 5^3$
2^2	$-3 \cdot 7$	$-2^3 3^2$	Type I	
2^3	3	$2^3 3^2$	Type I	
1	$-2 \cdot 3$	73		
3	$2 \cdot 5$	73	$21989x^6 + 38596x^5 + 119236x^4 - 628816x^3$	
			$+3229088x^2 - 7615232x + 4081216$	$19^2 41^2 73$
5	$-2^2 5$	-73		
5	3^2	-73	$x^6 - 2x^5 - 3x^4 + 6x^3 + 6x^2 - 16x + 9$	73
1	$2 \cdot 3$	79	$-4297x^6 - 1862x^5 - 30569x^4 - 89054x^3$	
			$-118138x^2 - 100460x - 28569$	$11^2 29^2 79$
3	-2	-3^4	$23x^6 - 30x^5 - 3551x^4 - 93060x^3 + 890665x^2$	
			$-4238718x + 10374527$	$3 \cdot 31^2$

$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$		N_{odd}
59	-2^2	3^4	$-57x^6 - 162x^5 + 1515x^4 - 1502x^3 - 3498x^2$	
			$+6876x - 3189$	$3^4 19^2$
1	3^2	83	$61x^6 - 144x^5 + 1258x^4 - 642x^3 + 1129x^2$	
			$-54x - 91$	$83 \cdot 181^2$
5	$2 \cdot 5$	83	$x^6 + 2x^5 - 35x^4 - 110x^3 - 150x^2 - 112x - 39$	$5^3 83$
5	$-2^3 3$	-89		
11	$2 \cdot 5$	89		
5	$-3 \cdot 5$	-97	$5x^6 - 794x^5 + 1915x^4 - 1020x^3 - 3925x^2$	
			$-3050x - 1003$	$5^3 11^2 97$
2^2	-3^2	$2^2 5^2$	$-15x^6 + 40x^5 - 10x^4 - 224x^3 + 505x^2$	
			$-470x + 185$	$5^2 41^2$
2^2	$3 \cdot 5$	$2^2 5^2$	$127x^6 - 50x^5 - 719x^4 - 540x^3 + 257x^2$	
			$+910x + 1615$	$5 \cdot 59^2$
5	$2 \cdot 5$	101	$-x^6 + 28x^5 + 140x^4 + 80x^3 + 480x^2 + 256x + 192$	$5^3 101$
5	3^2	103	$x^6 + 6x^5 - 19x^4 + 22x^3 - 10x^2 + 1$	103

Now we also list equations for those cases of curves from types III and IV (refer to section 6.3).

Type	z_6	s_2	σ_5	Equation
IV	1	-18	128	$y^2 = -11x^6 - 11x^3 + 4$
III	5	-10	128	$y^2 = x(5x^4 + 5x^2 + 1)$
IV	5	40	1728	$y^2 = 5x^6 + 10x^3 + 1$
III	8	-74	11664	$y^2 = x(9x^4 + 14x^2 + 9)$

A.4 Factors of $J_0(N)$ with $\sqrt{5}$-multiplication

Extending the table in [Wan95], Wang has determined all the 2-dimensional factors of $J_0(N)$ for $N \leqslant 750$ (communicated by email). The table below extracts from this information those levels N with a 2-dimensional factor with RM by $\mathbb{Q}(\sqrt{5})$.

For such a factor A, let R denote the largest order in $\mathbb{Q}(\sqrt{5})$ which embeds in $\mathrm{End}_{\mathbb{Q}}(A)$. Then the column headed by n in the table lists the conductor $[\mathbb{Z}[\eta] : R]$ when this is greater than 1. The abelian variety A carries a natural polarization λ, and d in the table is defined by $\deg \lambda = d^2$. Again, we only list those values of d which are greater than 1.

We also consider applying theorems 4.5.4 and 4.5.7 to reduce n and d by taking isogenies. The columns headed n_0 and d_0 list upper bounds for the smallest attainable values (again, when these are greater than 1)—they are the best upper bounds that we can assert from theorems 4.5.4 and 4.5.7, in the sense that there will be a $\mathbb{Q}$-isogenous abelian variety B with an action of an order $R' \subset \mathbb{Q}(\sqrt{5})$, defined over $\mathbb{Q}$, such that the conductor of R' divides n_0, and a polarization λ' on B, also defined over $\mathbb{Q}$, such that the degree of λ' divides d_0^2.

We note that there are 270 abelian varieties represented in the table. The only obstructions to making any variety represented in the table isogenous to a principally polarized abelian variety with maximal RM by $\mathbb{Q}(\sqrt{5})$ are that 2 might divide d, which occurs for 32 (12%) of these varieties, or that 5 might divide both d and n, which occurs in 6 cases (2%). Hence we can assert that the given abelian variety is isogenous to a principally polarized abelian variety with maximal RM by $\mathbb{Q}(\sqrt{5})$ for 232 (86%) of those listed in the table.

N	n	d	n_0	d_0
23				
31				
67		5		
67				
69	2	22	2	2
73				
74		5		
77	2	10	2	2
86		5		
87				
93				
103				
105	2	10	2	2
107				
115				
125				
125				
133				
133				
136	2	2	2	2
138	4	44	4	2
154	2	20	2	2
161	4		4	
166	2	131	2	
167				

N	n	d	n_0	d_0
175		5		
175				
177				
177				
177		31		
188				
191				
193		11		
199		71		
205				
207		11		
207	2	44	2	2
211		41		
213				
213		5		
218		451		
221	2	5	2	
221				
224	2		2	
224	2		2	
225	2	5	2	
227		31		
230		11		
231		5		
238	2	122	2	2

N	n	d	n_0	d_0
242	3	55		
242	3	55		
247		31		
250	3	5		
250		55		
250	3			
250		11		
255		55		
261	2		2	
261	2		2	
261	2		2	
262		11		
265		341		
265		5		
266	3			
268	2		2	
272	2	2	2	2
275		5		
275				
279				
279				
287				
287		19		
291		11		
291		55		

N	n	d	n_0	d_0
292				
299	2	2	2	2
299		11		
299				
313		41		
315	4	10	4	2
321	2	41	2	
321	2	5	2	
322	2	5	2	
334		11		
334		5		
335		179		
341		5		
347		19		
351				
351				
358		79		
358	3	29		
358	2	11	2	
361	5	55	5	5
361		11		
361		209		
361	5	1045	5	5
362	2	145	2	
363		5		

N	n	d	n_0	d_0
363		5		
363		55		
363	2	55	2	
363		55		
368	2	5	2	
371		5		
375		5		
375		155		
375		155		
375				
376	3			
376				
383		11		
386		19		
386		31		
391	2		2	
394		31		
394	3	5		
398		11		
398		11		
403		181		
410	2	20	2	2
412	2	5	2	
413		209		
414	6	44	2	2

N	n	d	n_0	d_0
415		11		
416	2	5	2	
417		19		
422	4	6061		
435		19		
435	2	220	2	2
437		55		
437		11		
438	2	580	2	2
439		31		
445	2	55	2	
448	2	4	2	2
448	6	4	2	2
453		11		
453		19		
453		491		
454		19		
457		31		
459		5		
459		5		
461		19		
471		19		
473	2	95	2	
473	2	55	2	
474		695		

N	n	d	n_0	d_0
476				
482		55		
483		295		
483		55		
483				
483		11		
484	5	5	5	5
484	3	5		
485	2	55	2	
491		19		
496	2	11	2	
498		61		
499		71		
500		5		
500		5		
502		145		
508	4	19	4	
508	2	11	2	
518		5		
520	2	20	2	2
523		149		
524		5		
525	5	55	5	5
525	6	10	2	2
525	3	55		

N	n	d	n_0	d_0
527	2	241	2	
529	2	11	2	
531	3			
531		31		
531	3			
532	5	11		
532				
534	3	1045		
536				
538		71		
551	2	5	2	
552	2	20	2	2
555		31		
555		5		
555		361		
566		61		
571		205		
575		5		
575				
577		295		
582	4	380	4	2
582	2	44	2	2
584				
590		3949		
592		5		

N	n	d	n_0	d_0
599		29		
602		31		
603		145		
603		95		
610		59		
621	5			
621	5			
623	2	44	2	2
625				
625				
625	3			
625	3			
626		55		
626		5		
632	2	5	2	
632		5		
635		155		
636		31		
636		5		
637	4	5	4	
637	4	5	4	
638				
638		19		
638	3	145		
639		5		

N	n	d	n_0	d_0
639				
640	2	2	2	2
640	2	2	2	2
640	6	2	2	2
640	6	2	2	2
642		55		
647		139		
651	2	20	2	2
651	2	20	2	2
657		145		
666		1045		
669	2	55	2	
674	2	55	2	
674	2	209	2	
675		5		
675		5		
677		101		
678	3	1705		
679		1969		
683	2	191	2	
687	3	5		
688	2	5	2	
689		55		
689				
693		55		

N	n	d	n_0	d_0
693	2	4	2	2
693		5		
693		55		
699	2	1829	2	
708	3	29		
713	2	121	2	
716		19		
717		31		
717				
717		19		
722	5	55	5	5
722	5	55	5	5
723	2	2222	2	2
726		30305		
726		30305		
726		5		
726		605		
735	4	10	4	2
745		1189		
750	3	19		

Bibliography

[Art86] M. Artin, *Néron models*, in *Arithmetic Geometry*, ed. G. Cornell and J.H. Silverman, Springer–Verlag (1986), 213–230.

[Ben98] P. Bending, *Curves of genus* 2 *with* $\sqrt{2}$ *multiplication*, Oxford University D.Phil thesis, in preparation.

[Bol88] O. Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1888), 47–70.

[BLR90] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergebnisse, 3.Folge Band 21, Springer–Verlag (1990).

[Bru95] A. Brumer, *The rank of* $J_0(N)$, Astérisque **228** (1995), 41–68.

[Car86] H. Carayol, *Sur les représentations p-adiques associeés aux formes modulaires de Hilbert*, Ann. Sci. Ec. Norm. Super. **19** (1986), 409–468.

[CGLR98] G. Cardona, J. González, J.C. Lario and A. Rio, *On curves of genus* 2 *with Jacobian of* GL_2 *-type*, preprint (1998).

[CF96] J.W.S. Cassels and E.V. Flynn, *Prologomena to a Middlebrow Theory of Curves of Genus* 2, LMS Lecture Notes Series **230**, Cambridge University Press (1996).

[Cha86] C.-L. Chai, *Siegel moduli schemes and their compactifications over* $\mathbb{C}$, in *Arithmetic Geometry*, ed. G. Cornell and J.H. Silverman, Springer–Verlag (1986), 231–251.

[Che96] I. Chen, *The Jacobians of modular curves associated to Cartan subgroups*, Oxford University D.Phil thesis (1996).

[Chi86] T. Chinburg, *Minimal models for curves over Dedekind rings*, in *Arithmetic Geometry*, ed. G. Cornell and J.H. Silverman, Springer–Verlag (1986), 309–326.

[Coh95] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, Springer–Verlag (1995).

[Dav57] H. Davenport, *Note on a theorem of Cassels*, Proc. Camb. Phil. Soc. **53** (1957), 539–540.

[Dia96] F. Diamond, *On deformation rings and Hecke rings*, Annals of Math. **144** no. 1 (1996), 137–166.

[Die67] J. Dieudonné, *Sur les groupes classiques*, Publ. de l'Institute de Math. de l'Université de Strasbourg **VI**, Hermann Paris (1967).

[DO88] I. Dolgachev and D. Ortland, *Point sets in projective space and theta functions*, Astérisque **165** (1988).

[vdG88] G. van der Geer, *Hilbert Modular Surfaces*, Springer–Verlag (1988).

[Gon94] M.R. Gonzalez-Dorrego, $(16, 6)$ *configurations and geometry of Kummer surfaces in* $\mathbb{P}^3$, Memoirs of the AMS, **512** (1994).

[GH77] P. Griffiths and J. Harris, *A Poncelet theorem in space*, Comment. Math. Helvetica **52** (1977), 145–160.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer–Verlag (1977).

[Hud05] R.W.H.T. Hudson, *Kummer's Quartic Surface*, Cambridge University Press (1905).

[Hum99] G. Humbert, *Sur les fonctionnes abéliennes singulières*, J. Math. Pures Appl. serie 5 t. V (1899), 233–350.

[Igu60] J.I. Igusa, *Arithmetic variety of moduli of genus two*, Ann. of Math. **72** (1960), 612–649.

[Jak94] B. Jakob, *Poncelet* 5*-gons and abelian surfaces*, Manuscripta Math. **83** (1994), 183–198.

[Lan86] H. Lange, *Jacobian surfaces in* $\mathbb{P}^4$, J.-Reine-Angew.-Math. **372** (1986), 71–86.

[Liu94] Q. Liu, *Modeles minimaux des courbes de genre deux*, J.-Reine-Angew.-Math. **453** (1994), 137–164.

[LRS93] P. Lockhart, M. Rosen and J.H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geometry **2** (1993), 569–601.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33–186.

[Mes91a] J.F. Mestre, *Familles de courbes hyperelliptiques à multiplications réelles*, Progress in Maths **89** (1991), 193–208.

[Mes91b] J.F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Progress in Maths **94** (1991), 313–334.

[Mil86a] J.S. Milne, *Abelian Varieties*, in *Arithmetic Geometry*, ed. G. Cornell and J.H. Silverman, Springer–Verlag (1986), 103–150.

[Mil86b] J.S. Milne, *Jacobian Varieties*, in *Arithmetic Geometry*, ed. G. Cornell and J.H. Silverman, Springer–Verlag (1986), 167–212.

[Mum70] D. Mumford, *Abelian Varieties*, Oxford University Press (1970).

[Nam73] Y. Namikawa and K. Ueno, *The complete classification of fibres in pencils of curves of genus* 2, Manus. Math. **9** (1973), 143–186.

[Nér64] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. I.H.E.S. **21** (1964).

[Ogg66] A.P. Ogg, *On pencils of curves of genus two*, Topology **5** (1966), 355–362.

[Rib76] K. Ribet, *Galois actions on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** no. 3 (1976), 751–804.

[Rib80] K. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** no. 1 (1980), 43–62.

[Rib92] K. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, in *1992 Proceedings of KAIST Mathematics Workshop*, Korea Advanced Institute of Science and Technology, Taejon (1992), 53–79.

[Ser68] J.P. Serre, *Corps locaux*, Hermann Paris (1968).

[Ser87] J.P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[ST68] J.P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[Sha74] I.R. Shafarevich, *Basic Algebraic Geometry*, Springer–Verlag (1974).

[SBT97] N.I. Shepherd-Barron and R. Taylor, *Mod* 2 *and mod* 5 *icosahedral representations*, Journal AMS **10** no. 2 (1997), 283–298.

[Shi63] G. Shimura, *Analytic families of abelian varieties*, Ann. of Math. **78** (1963), 149–192.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press (1971).

[Sil86] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer–Verlag (1986).

[Sil94] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer–Verlag (1994).

[TW95] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** no. 3 (1995), 553–572.

[Wan95] X. Wang, 2-*dimensional simple factors of* $J_0(N)$, Manuscripta Math. **87** no. 2 (1995), 179–197.

[Wei57] A. Weil, *Zum Beweis des Torellischen Satzes* Nachr. Acad. Wiss. Gottingen Math. Phys. K1 IIa (1957), 33–53.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** no. 3 (1995), 443–551.