**Endomorphism rings of elliptic curves over finite fields**

by

David Kohel

B.S. Biochemstry (Texas A&M University) 1989
B.S. Mathematics (Texas A&M University) 1989
Candidate in Philosophy (University of California, Berkeley) 1992

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Hendrik W. Lenstra, Jr., Chair
Professor Paul Vojta
Professor John Canny

Fall 1996

The dissertation of David Kohel is approved:

Chair Date

Date

Date

University of California at Berkeley

Fall 1996

**Endomorphism rings of elliptic curves over finite fields**

## Abstract

Endomorphism rings of elliptic curves over finite fields

by

David Kohel
Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Hendrik W. Lenstra, Jr., Chair

Let $k$ be a finite field and let $E$ be an elliptic curve. In this document we study the ring $\mathcal{O}$ of endomorphisms of $E$ that are defined over an algebraic closure of $k$. The purpose of this study is to describe algorithms for determining the isomorphism type of $\mathcal{O}$, and in certain cases for producing generators for the ring $\mathcal{O}$. The content of this work is naturally divided into the theory of ordinary and supersingular elliptic curves. For each case we present the relevant background material and develop new methods for working with these curves. The main results for ordinary elliptic curves are classical, and the primary innovation added here is the development of computational methods for computing with these curves. The main result is the following theorem.

**Theorem 1** *There exists a deterministic algorithm that given an elliptic curve $E$ over a finite field $k$ of $q$ elements, computes the isomorphism type of the endomorphism ring of $E$ and if a certain generalization of the Riemann hypothesis holds true, for any $\varepsilon > 0$ runs in time $\mathcal{O}(q^{1/3+\varepsilon})$.*

For the study of supersingular elliptic curves, theoretical background material is developed to prove the correctness of the following main theorem.

**Theorem 2** *There exists an algorithm that given a supersingular elliptic curve over a finite field $k$ computes four endomorphisms in $\mathcal{O}$ linearly independent over $\mathbb{Z}$. For any $\varepsilon > 0$ the algorithm terminates deterministically in $\mathrm{O}(p^{2/3+\varepsilon})$ operations in the field $k$ and probabilistically with expected $\mathrm{O}(p^{1/2+\varepsilon})$ operations in $k$, where $p$ is the characteristic of $k$.*

Professor Hendrik W. Lenstra, Jr.
Dissertation Committee Chair

A Tita,

y a nuestros años juntos en Berkeley.

# Contents

## Acknowledgements

This work would not have been possible without the support and advice of Hendrik Lenstra. From our early meetings I would emerge both overwhelmed and inspired by the body of mathematics to be mastered. His openness to all problems mathematical, and continual quest for correct formulation served as a model for my mathematical development.

# Chapter 1

# Introduction

This document is ostensibly concerned with the computational problem of determining the isomorphism type of the endomorphism ring of an elliptic curve over a finite field. Along the way I hope to take a stroll through classical theory of elliptic curves and complex multiplication. This tour will have served its goal if it inspires a geometric intuition for the arithmetic theory of elliptic curves.

On the surface the rings of endomorphisms of ordinary and supersingular elliptic curves appear quite dissimilar. While the familiar correspondences with lattices in characteristic zero fits well with the ordinary curves, the noncommutative endomorphism rings of supersingular elliptic curves appear of quite a different flavor. The geometry provides intuition for making the plunge into the world of noncommutative rings and makes the arithmetic theory palatable if not refreshing. The familiar lattices and commutative rings reemerge in intricately interwoven webs inside of the world of quaternions.

The question of determination of the endormorphism ring of an elliptic curve $E$ over a finite field $k$ arises as a natural sequel to that of determining the number of points on $E(k)$. The cardinality of $E(k)$ is an isogeny invariant of $E$, and in fact determines the isogeny class. If we denote by $\pi$ the Frobenius endomorphism relative to the field $k$ of $q$ elements, then $E(k)$ is the set of points fixed by $\pi$. Moreover, $\deg(\pi - 1)$, equal to the norm of $\pi - 1$ in the ring $\mathrm{End}(E)$, is the cardinality of the kernel of $\pi - 1$, so the cardinality of $E(k)$ is $q - t + 1$, where $t$ is the trace of Frobenius. Thus knowing the number of $k$-rational points on $E$ is equivalent to knowing the characteristic equation for $\pi$, which is equivalent to knowing, up to isomorphism, the subring $\mathbb{Z}[\pi]$ contained in the endomorphism ring of $E$ with its distinguished element $\pi$ of norm $q$. This suggests the question of the determination of the isomorphism type of the full ring of endomorphisms $\mathrm{End}(E)$ having distinguished element $\pi$.

Since the determination of the trace of Frobenius serves as the motivation and historical predecesor to the problem undertaken here, we review this recent history here. The first deterministic polynomial time algorithm for point counting was established

by René Schoof [27] in 1985. Using the action of the Frobenius endomorphism on the subgroup of $l$-torsion points of the elliptic curve for a prime $l$, Schoof proposed calculating the characteristic polynomial of the Frobenius endomorphism acting on the finite group scheme of $l$-torsion points. This gives the trace of the Frobenius endomorphism $\pi$ modulo the prime $l$, and by calculating this trace modulo various small primes $l$, one is able to recover the trace $t$ as an integer via the Chinese Remainder Theorem and the Riemann hypothesis for function fields. Later improvements by A. O. L. Atkin, Noam Elkies, and Jean-Marc Couveignes [5] used precalculated models for modular curves to determine congruence data modulo $l$ for the trace of Frobenius by considering the action of $\pi$ on the much smaller kernels of isogenies in $E[l]$ or the partial information from the action on the set of cyclic subgroups in $E[l]$ (see Schoof [28], Morain [21]).

As further motivation for the problem of computing $\mathrm{End}_k(E)$, we note that the pair $(\mathrm{End}_k(E), \pi)$ determines the $\mathrm{End}_k(E)$-module structure of $E(k)$. In [18], Hendrik Lenstra shows that for each degree $r$ extension $\kappa/k$ of the base field there exists an isomorphism of $\mathrm{End}_k(E)$-modules relating the structure of the group of $\kappa$-rational points and the quotient of $\mathrm{End}_k(E)$ by the ideal $(\pi^r - 1)$. If the Frobenius endomorphism $\pi$ does not lie in $\mathbb{Z}$ this isomorphism is

$$\mathrm{End}_k(E)/(\pi^r - 1) \cong E(\kappa).$$

For $\pi \in \mathbb{Z}$ the isomorphism of $\mathrm{End}_k(E)$-modules is given by:

$$\mathrm{End}_k(E)/(\pi^r - 1) \cong E(\kappa) \oplus E(\kappa).$$

One should note that for ordinary elliptic curves $\mathrm{End}_k(E) = \mathrm{End}_\kappa(E)$ for all extensions $\kappa$ of $k$, so we may write unambiguously $\mathrm{End}(E)$. For supersingular elliptic curves we will denote $\mathrm{End}_{\bar{k}}(E)$ by $\mathrm{End}(E)$. As a consequence of the result of Lenstra, the pair $(\mathrm{End}(E), \pi)$ determines the group structure of $E(\kappa)$ for all finite extensions $\kappa$ of $k$. Thus the calculation of this pair, up to isomorphism, determines the group structure of $E(k)$ in addition to the number of points, and determines the group structure of $E(\kappa)$ for all finite extensions $\kappa/k$.

The exposition is organized as follows. Chapter 2 reviews elliptic curves and their isogenies as given by rational functions. In practice one works with modular curves, and makes use of practical improvements as described by Atkin and Elkies, however asymptotically we know of no good algorithm for computing these curves and for theoretical purposes work with the full $l$-torsion groups. Chapter 3 then reviews the classical analytic and algebraic theory relating elliptic curves, complex multiplication, and class field theory. Chapter 4 deals with the computation of the endomorphism ring of an ordinary elliptic curve. The main result in the following theorem.

**Theorem 1** *There exists a deterministic algorithm that given an elliptic curve $E$ over a finite field $k$ of $q$ elements, computes the isomorphism type of the endomorphism*

*ring of $E$ and if a certain generalization of the Riemann hypothesis holds true, for any $\varepsilon > 0$ runs in time $\mathcal{O}(q^{1/3+\varepsilon})$.*

For the study of supersingular elliptic curves, background material is developed to obtain results for the computational complexity of determining the endomorphism ring of a supersingular elliptic curve. Chapter 5 first turns to the setting of quaternion algebras and describes the arithmetic necessary for understanding the structure of isogenies of supersingular elliptic curves. Prior to describing the algorithm for supersingular elliptic curves, Chapter 6 takes a digression into quadratic spaces associated to quaternion algebras, and the integral quadratic modules which they contain. The main result of Chapter 7 is the following algorithm for partial determination of the endomorphism ring of a supersingular elliptic curve.

**Theorem 2** *There exists an algorithm that given a supersingular elliptic curve over a finite field $k$ computes four endomorphisms in $\mathcal{O}$ linearly independent over $\mathbb{Z}$. For any $\varepsilon > 0$ the algorithm terminates deterministically in $\mathrm{O}(p^{2/3+\varepsilon})$ operations in the field $k$ and probabilistically with expected $\mathrm{O}(p^{1/2+\varepsilon})$ operations in $k$, where $p$ is the characteristic of $k$.*

The chapter concludes with conditions under which the ring detetermined by this algorithm coincides with the endomorphism ring of $E$.

# Chapter 2

# Elliptic curves and isogenies

An elliptic curve $E$ over a field $k$ is a complete curve of genus one over $k$ with a given point $\mathbf{O}$ defined over $k$. For each point $P$ of $E$ there is an associated valuation $v_P$ of the function field $k(E)$ of $E$ over $k$. From the Riemann-Roch theorem, there exist functions $x$ and $y$ in $k(E)$ having no poles outside of $\mathbf{O}$ and satisfying the following conditions at $\mathbf{O}$.

$$v_{\mathbf{O}}(x) = -2, \qquad v_{\mathbf{O}}(y) = -3, \qquad \frac{y^2}{x^3}(\mathbf{O}) = 1. \tag{2.1}$$

Then $x$ and $y$ are related by a relation in $k[x, y]$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.2}$$

which we call a Weierstrass equation for $E$. This equation, or more correctly, the homogeneous equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

defines $E$ as a closed subvariety of $\mathbb{P}^2$, with $\mathbf{O}$ the unique point on the line at infinity. For ease of notation, we define

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \quad \text{from which} \quad 4b_8 = b_2b_6 - b_4^2.$$

And further,

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad \text{from which} \quad 12^3\Delta = c_4^3 - c_6^2.$$

The constant $\Delta$ is called the discriminant of the Weierstrass equation. The curve defined by Weierstrass equation (2.2) is nonsingular if and only if $\Delta$ is nonzero.

The $j$-invariant of $E$ is defined to be $j = c_4^3/\Delta$. The $j$-invariant is known to determine the isomorphism class of the elliptic curve over the algebraic closure. Over a nonalgebraically closed field $k$, multiple nonisomorphic curves may have the same $j$-invariant.

Since $E$ is a curve of genus one, the space of global sections of the sheaf of differentials $\Omega_E$ of $E$ has dimension one as a vector space over $k$. We may take as generator

$$\omega = \frac{dx}{2y + a_1 x + a_3},$$

which we refer to as the *invariant differential* of $E$.

The single most significant fact about elliptic curves is that $E$ admits the structure of a group scheme with $\mathbf{O}$ as the identity. In fact we may identify $E$ in a canonical way with its Jacobian, via the map of points to divisors of degree zero

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{Pic}^0(E). \\ P & \longmapsto & P - \mathbf{O} \end{array}$$

The group law on $\mathrm{Pic}^0(E)$ is equivalent to the geometrically defined "chord-and-tangent" rule that three colinear points under the embedding of $E$ in $\mathbb{P}^2$ sum to zero. The nomenclature for the invariant differential is justified by the fact that $\omega$ is invariant under translation of the underlying curve of $E$ by a point $P$.

## 2.1 Isogenies

An *isogeny* of elliptic curves $\varphi : E_1 \to E_2$ is a nonconstant morphism of curves satisfying $\varphi(\mathbf{O}) = \mathbf{O}$. We say that $E_1$ and $E_2$ are *isogenous* over $k$ if there exists an isogeny of $E_1$ to $E_2$ defined over $k$. A morphism of curves $\varphi : E_1 \to E_2$ is called a *homomorphism* if $\varphi$ is also a homomorphism of group varieties. We will see shortly that the relation of isogeny is an equivalence relation on elliptic curves. It would be natural to restrict to isogenies which respect the group structures of $E_1$ and $E_2$. Fortunately this is no additional constraint: every isogeny of elliptic curves is a homomorphism [29, Theorem III.4.8].

We denote by $\mathrm{Hom}_k(E_1, E_2)$ the collection of homomorphisms from $E_1$ to $E_2$ over $k$, and let $\mathrm{End}_k(E) = \mathrm{Hom}_k(E, E)$. We write $\mathrm{Hom}(E_1, E_2)$ for $\mathrm{Hom}_{\overline{k}}(E_1, E_2)$, and $\mathrm{End}(E)$ for $\mathrm{End}_{\overline{k}}(E)$. The group structure on $E_2$ determines a group structure on $\mathrm{Hom}(E_1, E_2)$ such that as a $\mathbb{Z}$-module, $\mathrm{Hom}(E_1, E_2)$ is free of rank at most four [29, Corollary III.7.5]. Composition of endomorphisms gives a ring structure on $\mathcal{O} = \mathrm{End}(E)$, and we refer to $\mathcal{O}$ as the *ring of endomorphisms* of $E$.

For an elliptic curve $E$, the abelian group law $E \times E \to E$ is a morphism of varieties.

Thus the map

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\longmapsto P + \cdots + P \end{aligned}$$

sending a point to the sum of $P$ with itself $m$ times is a morphism of $E$ to itself sending $\mathbf{O}$ to $\mathbf{O}$. This allows us to define an injective ring homorphism

$$[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E).$$

Since any isogeny $\varphi : E_1 \to E_2$ is a group homomorphism, for all integers $m$ we have $[m]_{E_2} \circ \varphi = \varphi \circ [m]_{E_1}$. We use this injection to identify $\mathbb{Z}$ with its image in $\mathrm{End}(E)$. We maintain the use of the bracket notation only where it is desirable to emphasize the role of $[m]$ as a morphism of curves.

We can define a degree map on the collection of isogenies $\mathrm{Hom}(E_1, E_2)$ by $\deg(\varphi) = [K(E_2) : \varphi^* K(E_1)]$. Moreover, we define respectively

$$\begin{aligned} \deg_i(\varphi) &= [K(E_2) : \varphi^* K(E_1)]_i, \quad \text{and,} \\ \deg_s(\varphi) &= [K(E_2) : \varphi^* K(E_1)]_s, \end{aligned}$$

the inseparable and separable degrees of $\varphi$. Then for every point $Q$ in $E_2(k)$ the number of points $\#\varphi^{-1}(Q)$ in the inverse image of $Q$ is $\deg_s(\varphi)$, and in particular if $\varphi$ is separable then $\#\ker(\varphi) = \deg(\varphi)$. By convention we set $\deg([0]) = 0$.

A separable isogeny of elliptic curves is determined up to isomorphism over $\overline{k}$ by the kernel of the isogeny. Conversely given any finite subgroup $G$ of $E(\overline{k})$, there is up to isomorphism a unique elliptic curve $E/G$ and separable isogeny $f_G : E \to E/G$ with $G$ equal to the kernel [29, Proposition III.4.12]. If $G$ is defined over $k$, then the isogeny can also be defined over $k$.

**Theorem 3** *Let $\varphi : E_1 \to E_2$ be an homomorphism of degree $m$. Then there exists a unique isogeny $\widehat{\varphi} : E_2 \to E_1$ such that*

$$\widehat{\varphi} \circ \varphi = [m] : E_1 \to E_1,$$

*and $\deg(\widehat{\varphi}) = m$.*

**Proof.** Silverman [29, Theorem III.6.1].

The isogeny $\widehat{\varphi}$ is called the *dual* isogeny to $\varphi$. The properties of the dual isogeny are summarized in the following theorem.

**Theorem 4** *Let $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$ be homomorphisms of elliptic curves, and let $m$ be the degree of $\varphi$. Then the dual isogeny satisfies the following conditions.*

1. $\widehat{\varphi} \circ \varphi = [m] : E_1 \to E_1$.
2. $\varphi \circ \widehat{\varphi} = [m] : E_2 \to E_2$.
3. $\widehat{[m]} = [m]$.
4. $\widehat{(\varphi + \psi)} = \widehat{\varphi} + \widehat{\psi}$.
5. $\widehat{(\varphi \circ \psi)} = \widehat{\psi} \circ \widehat{\varphi}$.
6. $\widehat{\widehat{\varphi}} = \varphi$.

**Proof.** Silverman [29, Theorem III.6.2].
Note that if $\varphi : E_1 \to E_2$ is an isogeny, then

$$\widehat{\varphi}\,\mathrm{End}(E_2)\varphi \subseteq \mathrm{End}(E_1), \text{ and } \varphi\,\mathrm{End}(E_1)\widehat{\varphi} \subseteq \mathrm{End}(E_2).$$

The map $\mathrm{End}(E_1) \to \mathrm{End}(E_2)$ given by $\psi \mapsto \varphi\psi\widehat{\varphi}$ is a $\mathbb{Z}$-module homomorphism but if $\deg(\varphi) \neq 1$, is not a ring homomorphism. To correct this deficiency, we may choose any elliptic curve $E$ isogenous to $E_1$ and $E_2$, and set $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $K$ is either a field of degree at most 2 over $\mathbb{Q}$ or a definite quaternion algebra over $\mathbb{Q}$. For any isogeny $\varphi_i : E_i \to E$ of degree $m$ we have a ring homomorphism

$$\begin{array}{ccc} \mathrm{End}(E_i) & \xrightarrow{\quad\iota\quad} & K \\ \psi & \longmapsto & \widehat{\varphi}_i\psi\varphi_i \otimes m^{-1}. \end{array}$$

An immediate consequence is that $\mathrm{End}_k(E_i) \otimes \mathbb{Q} \cong K$ for all elliptic curves $E_i$ isogenous to $E$ over $k$.
We will classify endomorphism rings of elliptic curves in later sections, but one classical case of interest is when $\mathrm{End}(E)$ is an order in an imaginary quadratic extension of $\mathbb{Q}$. In this particular case we can deduce the following result.

**Proposition 5** *Suppose that* $\mathrm{End}(E_1)$ *is isomorphic to an order in an imaginary quadratic extension* $K$ *of* $\mathbb{Q}$. *If* $E_1$ *and* $E_2$ *are isogenous then there exist unique relatively prime integers* $m_1$ *and* $m_2$ *such that*

$$\mathbb{Z} + m_2\,\iota(\mathrm{End}(E_1)) = \mathbb{Z} + m_1\,\iota(\mathrm{End}(E_2)),$$

*and the degree of every isogeny* $E_1 \to E_2$ *is divisible by* $m_1m_2$.

**Proof.** Let $\mathcal{O}_K$ be the maximal order of $K$. The set $S$ of orders $\mathcal{O} \subseteq \mathcal{O}_K$ forms a partially ordered set under the ordering of containment. The natural numbers $\mathbb{N}$ can be mapped bijectively to the set of orders via the map $m \mapsto \mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$. This gives an isomorphism of partially ordered sets under the partial ordering on $\mathbb{N}$ given by $m \leq n$ if $m|n$. Write

$$\mathcal{O}_1 = \iota(\mathrm{End}(E_1)) = \mathbb{Z} + nm_1\mathcal{O}_K \text{ and } \mathcal{O}_2 = \iota(\mathrm{End}(E_2)) = \mathbb{Z} + nm_2\mathcal{O}_K,$$

for integers $m_1$, $m_2$ and $n$ such that $\gcd(m_1, m_2) = 1$. Suppose $\varphi : E_1 \longrightarrow E_2$ is an isogeny of degree $m$. Then $\mathbb{Z} + \varphi\,\mathrm{End}(E_1)\widehat{\varphi}$ is contained in $\mathrm{End}(E_2)$, and $\iota(\mathbb{Z} + \varphi\,\mathrm{End}(E_1)\widehat{\varphi})$ is contained in $\iota(\mathrm{End}(E_1))$ with index $m$. Thus $nm_2$ divides $nm_1m$, hence $m_2$ divides $m$. Reciprocally $m_1$ divides $m$, and the result follows.
We now recall the definition of a quadratic space. A quadratic space $V$ over $\mathbb{Q}$ is a vector space $V$ over $\mathbb{Q}$ together with a symmetric bilinear form $\Phi : V \times V \to \mathbb{Q}$.

Associated with a quadratic space $V$ is a quadratic map $\mathbf{q} : V \to \mathbb{Q}$ such that $\mathbf{q}(u+v)-\mathbf{q}(u)-\mathbf{q}(v) = \Phi(u,v)$. A quadratic module over $\mathbb{Z}$ is a lattice $M$ in $V$ such that the associated quadratic map on $V$ restricts to an integer-valued map on $M$. A quadratic space or quadratic module is said to be positive definite if $\mathbf{q}(v) > 0$ for all nonzero $v$ in $V$.

**Theorem 6** *Let $E_1$ and $E_2$ be elliptic curves. Then there is a bilinear form*

$$\Phi : \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

*defined by $\Phi(\varphi,\psi) = \widehat{\varphi}\psi + \widehat{\psi}\varphi$. The bilinear form $\Phi$ defines the structure of a positive definite quadratic space on $V = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$, with associated quadratic map* deg*, extended to $V$ by setting $\deg(\varphi \otimes r) = r^2 \deg(\varphi)$. The lattice $\mathrm{Hom}(E_1, E_2)$ is a quadratic module with respect to* deg*.*

**Proof.** [29, Corollary 6.3].

As a demonstration of the quadratic module structure on $\mathrm{Hom}(E_1, E_2)$, consider the following two elliptic curves over the field $k = \mathbb{F}_{41}$.

$$\begin{aligned} E_1 :&\quad y^2 = x^3 + 15x + 35 \\ E_2 :&\quad y^2 = x^3 + x + 33. \end{aligned}$$

The $\mathbb{Z}$-module $\mathrm{Hom}(E_1, E_2)$ is generated by isogenies $\varphi$ and $\psi$ of degree 3 and 7, respectively, and such that

$$\Phi(\varphi,\psi) = \widehat{\varphi}\psi + \widehat{\psi}\varphi = 1.$$

In terms of the basis $\{\varphi, \psi\}$ the quadratic map deg on $\mathrm{Hom}(E_1, E_2)$ defines a *quadratic form*

$$\mathbf{q}(x_1, x_2) = \deg(x_1\varphi + x_2\psi) = 3x_1^2 + x_1x_2 + 7x_2^2.$$

Such binary quadratic forms arise in the ideal theory of orders in quadratic extensions of $\mathbb{Q}$. In Chapter 3 we turn to the relation between elliptic curves and the ideal theory of such orders. This construction of quadratic modules from isogenies of elliptic curves will be further exploited in Chapter 6 when our principal objects of study will be quadratic modules of rank four over $\mathbb{Z}$.

## 2.2 The image of $\mathbb{Z}$ in $\mathrm{End}(E)$

We have seen that for an elliptic curve $E/k$, the abelian group law $E \times E \to E$ is a morphism of varieties, defined over $k$. Silverman [29, III §2] gives explicit rational functions for the maps. Thus the map

$$\begin{aligned} [n] : E &\longrightarrow E \\ P &\longmapsto P + \cdots + P \end{aligned}$$

sending a point to the sum of $P$ with itself $n$ times is an endomorphism in $\mathrm{End}_k(E)$, given by rational functions. From the group law on $E$ we can recursively derive the rational functions defining $[n]$ on $E$. There exist relatively prime polynomials $\phi_n, \psi_n$, and $\omega_n$ in $k[x,y]$ such that $[n]$ is given as follows.

$$\begin{array}{ccc} E & \xrightarrow{\qquad [n] \qquad} & E \\ (x,y) & \longmapsto & (x_n, y_n) = (\dfrac{\phi_n(x,y)}{\psi_n(x,y)^2}, \dfrac{\omega_n(x,y)}{\psi_n(x,y)^3}). \end{array}$$

**Definition.** The polynomials $\phi_n, \psi_n$, and $\omega_n$ are called the $n$th *division polynomials* on $E$.

The polynomial $\psi_n$ plays a distinguished role in that the ideal $(\psi_n(x,y))$ defines the closed subscheme $E[n] - \{\mathbf{O}\}$ of $E$, so we may refer to $\psi_n$ as the $n$-th division polynomial.

The division polynomials satisfy many relations which can be obtained from the associativity of the group law on $E$, the Weierstrass equation relating $x$ and $y$, and the explicit formulas for addition. In the case that $a_1 = a_2 = a_3 = 0$, Silverman [29] and Lang [17] give recursive formulas for the division polynomials. Morain [21] gives general formulas for $\phi_n$ and $\psi_n$. For completeness we include here recursive formulas and relations for the division polynomials on an elliptic curve $E$.

The division polynomial $\psi_n$ can be defined recursively via:

$$\begin{gathered} \psi_0 = 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y + a_1x + a_3, \\ \psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\ \psi_4 = \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2) \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2), \\ \psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/\psi_2 \quad (m > 2), \end{gathered}$$

and $\phi_n$ by

$$\phi_0 = 1, \quad \phi_1 = x, \quad \text{and} \quad \phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}.$$

Note that all of the above relations among the $\phi_n$ and $\psi_n$ are generated by the relations defining $\psi_0, \ldots, \psi_4$, $\phi_0$, and $\phi_1$, and the relations:

$$\phi_r\psi_m^2 - \phi_m\psi_r^2 = \psi_{m-r}\psi_{m+r}, \quad \text{where} \quad r \leq m,$$

which can be verified directly from the group law on $E$. The following formula for $\omega_n$ is valid if the characteristic of $k$ is different from 2.

$$\omega_n = ((\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/\psi_2 - (a_1\phi_n + a_3\psi_n^2)\psi_n)/2.$$

This equation stems from the action of the endomorphism $[n]$ on the invariant differential, namely that

$$n\frac{dx}{2y + a_1x + a_3} = \frac{dx_n}{2y_n + a_1x_n + a_3}.$$

In general $\omega_n$ is defined recursively as follows.

$$\omega_0 = 1, \quad \omega_1 = y, \quad \text{and}$$
$$\omega_2 = -(3x^2 + 2a_2x + a_4 - a_1y)\phi_2 - (-x^3 + a_4x + 2a_6 - a_3y)\psi_2^2 - (a_1\phi_2 + a_3\psi_2^2)\psi_2,$$
$$\omega_{2m+1} = \omega_m\psi_{3m+2} - \omega_{m+1}\psi_{3m+1} - (a_1\phi_{2m+1} + a_3\psi_{2m+1}^2)\psi_{2m+1} \quad (m \geq 1),$$
$$\omega_{2m} = (\omega_{m-1}\psi_{3m+1} - \omega_{m+1}\psi_{3m-1})/\psi_2 - (a_1\phi_{2m} + a_3\psi_{2m}^2)\psi_{2m} \quad (m \geq 2),$$

Among the $\omega_n$ we have the following relations

$$\frac{\omega_r\psi_{n+r} - \omega_{n-r}\psi_{2n-r}}{\psi_{n-2r}} = \frac{\omega_s\psi_{n+s} - \omega_{n-s}\psi_{2n-s}}{\psi_{n-2s}},$$

which hold for all $r$ and $s$ such that $2r$ and $2s$ are less than $n$.

This defines $\psi_n$, $\phi_n$, $\omega_n$ as polynomials in $\mathbf{Z}[x, y, \{a_i\}]$. One checks for odd $n$ that $\psi_n$ and $\phi_n$ lie in $\mathbf{Z}[x, \psi_2^2, \{a_i\}]$, and for even $n$ that $\psi_2^{-1}\psi_n$ and $\phi_n$ lie in $\mathbf{Z}[x, \psi_2^2, \{a_i\}]$. Since $\psi_2^2$ is equivalent to $4x^3 + b_2x^2 + 2b_4x + b_6$, modulo the relation (2.2), these can be calculated as polynomials in $\mathbf{Z}[x, \{a_i\}]$.

## 2.3 The Frobenius endomorphism

Let $k$ be a finite field of $q$ elements. Then the Galois group $\mathrm{Gal}(\overline{k}/k)$ is generated by the *Frobenius automorphism* $\phi$ relative to $k$, defined by $\phi(\alpha) = \alpha^q$ for all $\alpha$ in $\overline{k}$. For any finite extension of $\kappa/k$, the automorphism

$$\kappa \xleftarrow{\ \phi\ } \kappa$$

determines a morphism $\mathrm{Spec}(\kappa) \longrightarrow \mathrm{Spec}(\kappa)$. Thus for any variety $V$ over $\mathrm{Spec}(\kappa)$, we can extend the base by $\phi$ to define a new variety $V^\phi = V \times_\phi \kappa$. Let $\mathcal{O}_V$ be the sheaf of functions of $V$, and for each open subset $U \subseteq V$ let $\iota : \kappa \longrightarrow \mathcal{O}_V(U)$ be the homomorphism determined by the map $V \to \mathrm{Spec}(\kappa)$. Define also

$$\iota_1 : \mathcal{O}_V(U) \longrightarrow \mathcal{O}_V(U) \otimes_\phi \kappa \quad \text{and} \quad \iota_2 : \kappa \longrightarrow \mathcal{O}_V(U) \otimes_\phi \kappa$$

to be the injections $f \mapsto f \otimes 1$ and $\alpha \mapsto 1 \otimes \alpha$ respectively, and define a map $\pi^*$ by

$$\begin{array}{ccc} \mathcal{O}_V(U) \otimes_\phi \kappa & \xrightarrow{\ \pi^*\ } & \mathcal{O}_V(U) \otimes_\phi \kappa \\ f \otimes \alpha & \longmapsto & f^q \otimes \alpha^q. \end{array}$$

Then we have a commutative diagram

$$\begin{array}{ccccc} \mathcal{O}_V(U) & \xrightarrow{\ \iota_1\ } & \mathcal{O}_V(U) \otimes_\phi \kappa & \xrightarrow{\ \pi^*\ } & \mathcal{O}_V(U) \otimes_\phi \kappa \\ \uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle \iota_2} & & \uparrow{\scriptstyle \iota_1 \circ \iota} \\ \kappa & \xrightarrow{\ \phi\ } & \kappa & \xrightarrow{\ 1\ } & \kappa \end{array}$$

where the left hand square defines the extension of base by $\phi$ and the right hand square defines a morphism of varieties $\pi : V \longrightarrow V^\phi$ over $\kappa$, by means of the isomorphism

$$\begin{array}{ccc} \mathcal{O}_V(U) & \xrightarrow[\cong]{\iota_1} & \mathcal{O}_V(U) \otimes_\phi \kappa \\ \uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle \iota_1 \circ \iota} \\ \kappa & \xrightarrow[\cong]{1} & \kappa. \end{array}$$

We call this morphism the Frobenius morphism. If we replace $V$ with an elliptic curve $E$ over $\kappa$ and define $\pi(\mathbf{O})$ to be the identity element on $E^\phi$, then the Frobenius morphism determines a *Frobenius isogeny* $\pi : E \longrightarrow E^\phi$. We will be particularly interested in the case that $\kappa = k$, so that $\phi$ fixes the field of definition of $E$. Then $E^\phi = E$ and $\pi$ is called the *Frobenius endomorphism* relative to $k$, or the $q$th power Frobenius endomorphism.

If $E$ is given by Weierstrass equation

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

then the Weierstrass equation of the curve $E^\phi$ is

$$y^2 + a_1^qxy + a_3^qy = x^3 + a_2^qx^2 + a_4^qx + a_6^q,$$

and the Frobenius isogeny is given by the map

$$\begin{array}{ccc} E & \xrightarrow{\quad\pi\quad} & E^\phi \\ (x_0, y_0) & \longmapsto & (x_0^q, y_0^q). \end{array}$$

The basic properties of the Frobenius isogeny are summarized in the following proposition.

**Proposition 7** *The $q$th power Frobenius isogeny $\pi$ is purely inseparable and the degree of $\pi$ is $q$.*

**Proof.** Silverman [29, Proposition II.2.12].

From this proposition, we can deduce the following result by which we can decompose an isogeny into a purely inseparable isogeny composed with a separable isogeny.

**Proposition 8** *For any isogeny $\psi : E_1 \to E_2$ of elliptic curves over a finite field, there exists a factorization*

$$E_1 \xrightarrow{\quad\pi\quad} E_1^\phi \xrightarrow{\quad\varphi\quad} E_2,$$

*where $q = \deg_i(\psi)$ and $\pi$ is the $q$th power Frobenius isogeny, and where $\psi$ separable.*

**Proof.** Silverman [29, Corollary II.2.12].

Suppose that $E/k$ is an elliptic curve over the field $k$. The Frobenius endomorphism relative to $k$ satisfies a characteristic equation $\pi^2 - t\pi + q = 0$ in the ring of endomorphisms. For any extension $\kappa/k$ of degree $r$, the Frobenius endomorphism relative to $\kappa$ is $\pi^r$. The collection of points fixed by $\pi$ is exactly $E(\kappa)$, so the kernel of $\pi^r - 1$ is $E(\kappa)$. Since the isogeny $\pi - 1$ is separable, the cardinality of $E(\kappa)$ is $\deg(\pi^r - 1)$, and in particular, the number of $k$-rational points is $\deg(\pi - 1) = q - t + 1$. A theorem of Tate [31, Theorem 1] tells us that the characteristic polynomial for $\pi$ determines the isogeny class of $E$ over $k$.

From its definition, it is clear that $\pi$ commutes with all isogenies defined over $k$, hence we have that $\pi$ lies in the center of $\mathrm{End}_k(E)$. The following theorem shows the key role that the Frobenius endmorphism plays in the structure of the elliptic curve and its endomorphism ring.

**Theorem 9** *Let $k$ be a perfect field of characteristic $p$ and let $E$ be an elliptic curve over $k$. Let $\pi$ be the Frobenius endomorphism relative to $k$. The following conditions are equivalent.*

1. *$E[p^r] = 0$ for all $r \geq 1$.*
2. *The dual $\widehat{\pi}$ of the Frobenius endomorphism is purely inseparable.*
3. *The trace of the Frobenius is divisible by $p$.*
4. *The full endomorphism ring $\mathrm{End}(E)$ defined over an algebraic closure of $k$ is an order in a quaternion algebra.*

*If the preceding equivalent conditions do not hold, then the all of the following statements hold true.*

1. *$E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$.*
2. *The dual $\widehat{\pi}$ of the Frobenius endomorphism is separable.*
3. *The trace of the Frobenius endomorphism is relatively prime to $p$.*
4. *The endomorphism ring $\mathrm{End}(E)$ of $E$ is an order in a quadratic imaginary extension of $\mathbb{Q}$.*

**Proof.** Silverman [29, Theorem V.3.1].

In the first case of the theorem, we say that $E$ is *supersingular*, and in the second case we say that $E$ is *ordinary*. It is not in general true that if $E$ is supersingular then $\mathrm{End}_k(E)$ is an order in a quaternion algebra.

The Frobenius endomorphism determines more, however, than just these large scale structures of the elliptic curves. The following theorem shows that the group and $\mathrm{End}_k(E)$-structure of the rational points are determined by $\pi$.

**Theorem 10** *Let $k$ be a finite field and let $E$ be an elliptic curve over $k$, Let $\pi$ be the*

*Frobenius endomorphism of $E$. Further, let $\kappa$ be a finite extension of $k$, and denote be $r = [\kappa : k]$ its degree.*

1. *Suppose that $\pi \notin \mathbb{Z}$. Then $\mathrm{End}_k(E)$ has rank 2 over $\mathbb{Z}$, and there is an isomorphism*
$$E(\kappa) \cong \frac{\mathrm{End}_k(E)}{(\pi^r - 1)}.$$
2. *Suppose that $\pi \in \mathbb{Z}$. Then $\mathrm{End}_k(E)$ has rank 4 over $\mathbb{Z}$, we have*
$$E(\kappa) \cong \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)} \oplus \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)}$$
*as abelian groups, and this group has, up to isomorphism, exactly one left $\mathrm{End}_k(E)$-module structure. Furthermore, one has*
$$E(\kappa) \oplus E(\kappa) \cong \frac{\mathrm{End}_k(E)}{(\pi^r - 1)}$$
*as $\mathrm{End}_k(E)$-modules.*

**Proof.** Lenstra [18, Theorem 1].

## 2.4 Explicit isogenies

The goal of this section is not to duplicate Elkies' document [9] of the same name. Rather the goal is to show that given a polynomial $\psi(X)$ defining the ideal sheaf for a finite subgroup $G \subseteq E(\overline{k})$, there exist explicit functions for the isogeny in terms of $\psi(X)$. In fact this section is entirely credited to Vélu [33]. The modest modification made here is the description of the equations of Vélu not in terms of the coordinates of the points in the group $G$, but in terms of a generator of the ideal sheaf for $G$. This will simplify the task of exhibiting an isogeny to producing a generator polynomial for the ideal sheaf of $G$.

Note that we lose nothing by the assumption that $G$ is reduced and consequently the corresponding isogeny separable. We have seen that any inseparable isogeny can be factored as a purely inseparable Frobenius isogeny followed a separable isogeny.

If we let $x$ and $y$ be elements of the function field of $E$ satisfying the Weierstrass equation (2.1) of § 2.2, then a subgroup $G/k$ is defined on the coordinate ring $k[x, y]$ for $E - \{\mathbf{O}\}$ by an ideal $I_G$. Since $G$ is stable under the automorphism $[-1]$ on $E$ which fixes $x$, there exists a polynomial $\psi_G(x)$ in $k[x]$ which defines $I_G$. If $G$ has odd degree, $I_G$ is equal to the principal ideal $(\psi_G(x))$. Otherwise $I_G$ is non-principal, and $(\psi_G(x))$ has multiplicity two in the two-torsion points of $G$. We can define elements

$x_G$ and $y_G$ in the function field of $E$, invariant under $G$, as follows.

$$\begin{aligned} x_G(P) &= x(P) + \sum_{Q \in G - \{0\}} (x(P+Q) - x(Q)), \\ y_G(P) &= y(P) + \sum_{Q \in G - \{0\}} (y(P+Q) - y(Q)). \end{aligned} \tag{2.3}$$

The functions $x_G$ and $y_G$ generate the function field for a curve $E_G$ and satisfy the conditions (2.1) of § 2.2 on $E_G$. Then $f_G : E \to E_G$ defined by $(x, y) \mapsto (x_G, y_G)$, is an isogeny of Weierstrass equations. Under this isogeny of curves the invariant differential on the image curve $E_G$ pulls back to the invariant differential on $E$, that is,

$$f_G^*(\frac{dx_G}{2y_G + a_1 x_G + a_3}) = (\frac{dx}{2y + a_1 x + a_3}).$$

Following Vélu [33], we can write down explicit equations for $x_G$ and $y_G$ in terms of $x$ and $y$ defining the isogeny $f_G$ of curves with the kernel specified by $\psi(x)$ in $k[x]$. He develops rational functions in terms of the roots of $\psi(x)$, but the isogeny is more appropriately expressed in terms of symmetric functions in the roots as follows.

## Isogenies of odd degree

First we assume that the degree of the isogeny determined by the equation $\psi(x)$ for the kernel is odd. A general isogeny over $k$ can be decomposed over $k$ into a composite of isogenies of degree 2 or 4 and isogenies of odd degree. We will treat decomposition of $G$ in the sequel.

The isogeny is described in terms of the coefficients of $\psi(x)$ as follows.

$$(x, y) \longmapsto (x_G, y_G) = (\frac{\phi(x)}{\psi(x)^2}, \frac{\omega(x, y)}{\psi(x)^3}),$$

where $\phi(x)$ is given by

$$\begin{aligned} \phi(x) &= (4x^3 + b_2 x^2 + 2b_4 x + b_6)(\psi'(x)^2 - \psi''(x)\psi(x)) \\ &\quad -(6x^2 + b_2 x + b_4)\psi'(x)\psi(x) + (dx - 2s_1)\psi(x)^2, \end{aligned}$$

where the degree of the isogeny is $d = 2n + 1$, and $s_i$ is the $i$th elementary symmetric function in the roots of $\psi(x)$, so that $\psi(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$.

If the characteristic of the base field $k$ is different from 2, one can derive the equation for $\omega(x, y)$ from $\phi(x)$ and $\psi(x)$ using the condition that the the invariant differential on $E_G$ pulls back to the invariant differential on $E$.

$$\omega(x, y) = \phi'(x)\psi(x)\psi_2/2 - \phi(x)\psi'(x)\psi_2 + (a_1\phi(x) + a_3\psi(x)^2))\psi(x)/2.$$

Over an arbitrary field the following formula for $\omega(x,y)$ holds. First we must define $\underline{\psi}''(x)$ and $\underline{\psi}'''(x)$.

$$\underline{\psi}''(x) = \sum_{i=0}^{n-2} \binom{i+2}{2} a_{i+2} x^i, \qquad \underline{\psi}'''(x) = \sum_{i=0}^{n-3} 3\binom{i+3}{2} a_{i+3} x^i.$$

Then $\omega(x,y)$ can be defined as follows.

$$\begin{aligned}\omega(x,y) &= \phi'(x)\psi(x)y - \phi(x)\psi'(x)\psi_2 + ((a_1x+a_3)\psi_2^2(\underline{\psi}''(x)\psi'(x) - \underline{\psi}'''(x)\psi(x)) \\ &\quad + (a_1\psi_2^2 - 3(a_1x+a_3)(6x^2+b_2x+b_4))\underline{\psi}''(x)\psi(x) \\ &\quad + (a_1x^3 + 3a_3x^2 + (2a_2a_3 - a_1a_4)x + (a_3a_4 - 2a_1a_6))\psi'(x)^2 \\ &\quad + (-(3a_1x^2 + 6a_3x + (-a_1a_4 + 2a_2a_3)) \\ &\quad + (a_1x+a_3)(dx - 2s_1))\psi'(x)\psi(x) + \ (a_1s_1 + a_3n)\psi(x)^2)\psi(x).\end{aligned}$$

The functions $x_G$ and $y_G$ then satisfy the following equation of Velu [33].

$$y_G^2 + a_1x_Gy_G + a_3y_G = x_G^3 + a_2x_G^2 + (a_4 - 5t)x_G + (a_6 - b_2t - 7w), \tag{2.4}$$

where, in terms of the coefficients of $\psi(x)$,

$$\begin{aligned} t &= 6(s_1^2 - 2s_2) + b_2s_1 + nb_4, \quad \text{and} \\ w &= 10(s_1^3 - 3s_1s_2 + 3s_3) + 2b_2(s_1^2 - 2s_2) + 3b_4s_1 + nb_6. \end{aligned}$$

## Isogenies of even degree

Now suppose that the subgroup $G$ defined by $\psi_G(x)$ has elements of order 2. We will first determine the isogeny corresponding to the subgroup $H$ of degree 2 or of degree 4 defined by $\psi_H(x) = \gcd(\psi_G(x), 4x^3 + b_2x^2 + 2b_4x + b_6)$.
If $\psi_H(x) = x - x_0$ is linear the degree two isogeny of $E$ to a curve $E_H$ determined by $\psi_H(x)$ as

$$\begin{aligned} x_H &= x + \frac{3x_0^2 + 2a_2x_0 + a_4 - a_1y_0}{x - x_0} \\ y_H &= y - (3x_0^2 + 2a_2x_0 + a_4 - a_1y_0)\frac{a_1(x-x_0) + (y-y_0)}{(x-x_0)^2} \end{aligned}$$

where $y_0$ is defined by the equations

$$\begin{aligned} y_0^2 + (a_1x_0 + a_3)y_0 - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0, \\ 2y_0 + a_1x_0 + a_3 = 0. \end{aligned}$$

Thus $y_0$ is a square root of $x_0^3 + a_2x_0^2 + a_4x_0 + a_6$ in characteristic 2 and equals $-(a_1x_0 + a_3)/2$ otherwise.

If $\psi_H(x)$ has degree three, corresponding to the subgroup $H = E[2] \subset G$, then the resulting isogeny is given as follows.

$$(x, y) \longmapsto (x_H, y_H) = (\frac{\phi(x)}{\psi(x)^2}, \frac{\omega(x, y)}{\psi(x)^3}),$$

where $\psi(x) = \psi_H(x)$ and $\phi(x)$ is given by

$$\phi(x) = \psi'(x)^2 - 2\psi''(x)\psi(x) + (4x - s_1)\psi(x)^2),$$

and $\omega(x, y)$ by

$$\omega(x, y) = \psi_2(x, y)(\phi'(x)\psi(x) - \phi(x)\psi'(x))/2 - (a_1\phi(x) + a_3\psi(x))\psi(x)/2.$$

Since $\psi_H(x)$ determines a separable isogeny, the characteristic is necessarily different from 2 and the equation for $\omega(x, y)$ is well-defined.

In each case, the equation for the image curve is determined as above by (2.4), with the following values of $t$ and $w$. If $\psi_H(x) = x - x_0$, then $t = 3x_0^2 + 2a_2x_0 + a_4 - a_1y_0$, and $w = x_0t$. Otherwise set

$$\begin{aligned} t &= 3(s_1^2 - 2s_2) + b_2s_1/2 + 3b_4/2, \\ w &= 3(s_1^3 - 3s_1s_2 + 3s_3) + b_2(s_1^2 - 2s_2)/2 + b_4s_1/2. \end{aligned}$$

## Invariance under composition

The Weierstrass equation of the image curve $E_G$ and isogeny $f_G$ are uniquely determined by the choice of coordinates $x_G$ and $y_G$. We define a function $T_G$ on functions with no poles on $G - \{\mathbf{O}\}$ to be $T_G(t) = t_G$, where

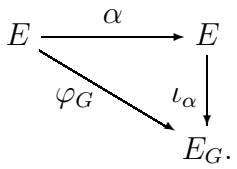
$$t_G(P) = t(P) + \sum_{Q \in G - \{\mathbf{O}\}} \left(t(P + Q) - t(Q)\right),$$

for all points $P$ in $E(\overline{k})$. Then $T_G(t + s) = T_G(t) + T_G(s)$ and $T_G(\alpha) = \alpha$ for all $\alpha$ in $k$. By rearranging sums, one verifies that $T_{G/H} \circ T_H = T_G$. Since we defined the coordinate functions of equations (2.3) on $E_G$ by $x_G = T_G(x)$ and $y_G = T_G(y)$, this proves that the isogenies determined by the equations of Vélu are independent of the decomposition into isogenies of smaller degree.

## Isogenies of Vélu versus endomorphisms

In general the separable isogeny defined by Vélu will not be an endomorphism, even if the group $G$ is the kernel of an endomorphism. Let $\mathcal{O}$ be the endomorphism ring

of $E$, and $K = \mathcal{O} \otimes \mathbb{Q}$. Let $\mathfrak{p}$ be the kernel of the map $\mathcal{O} \to \overline{k}$ which is defined by the action of $\mathcal{O}$ on the sheaf of differentials. For each endomorphism $\alpha$ defined over $k$ having kernel $G$, there is a unique isomorphism of curves $\iota_\alpha : E_G \to E$ such that the following diagram commutes:




Let the Weierstrass equation of $E_G$ be

$$y_G^2 + \widetilde{a_1} x_G y_G + \widetilde{a_3} y_G = x_G^3 + \widetilde{a_2} x_G^2 + \widetilde{a_4} x_G + \widetilde{a_6},$$

then $\widetilde{a_1} = a_1$, $\widetilde{a_2} = a_2$, $\widetilde{a_3} = a_3$, and $\widetilde{a_4}$ and $\widetilde{a_6}$ can be described by

$$\widetilde{a_4} = a_4 + \left[\frac{\alpha^4 - 1}{48\alpha^4}\right](-b_2^2 + 24b_4) \quad \text{and,}$$
$$\widetilde{a_6} = a_6 + \left[\frac{(\alpha^2-1)^2(\alpha^2+1)}{12^3\alpha^6}\right] b_2^3 - \left[\frac{\alpha^2-1}{24\alpha^6}\right] b_2 b_4 + \left[\frac{\alpha^6-1}{4\alpha^6}\right] b_6,$$

where the expression in braces should be evaluated in $K$ before reducing modulo $\mathfrak{p}$ to obtain an element of $k$. One can easily verify that each such expression lies in the localization of $\mathcal{O}$ at $\mathfrak{p}$.

## 2.5 Reduction and lifting of curves

The following theorems of Deuring describe the structures which are preserved in passing between curves in characteristic zero and finite characteristic.

**Theorem 11** *Let $\widetilde{E}/\overline{\mathbb{Q}}$ be an elliptic curve with endomorphism ring $\mathrm{End}(\widetilde{E}) = \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic extension $K$ of $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of $\overline{\mathbb{Q}}$, over a prime number $p$, at which $\widetilde{E}$ has nondegenerate reduction $E$. The curve $E$ is supersingular if and only if $p$ has only one prime of $K$ above it. If $p$ splits in $K$, then let $m$ be the conductor of $\mathcal{O}$, so that $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$. Write $m = p^r m_0$, where $p^r$ is the largest power of $p$ dividing $m$. Then the endomorphism ring of $E$ is as follows.*

1. *$\mathrm{End}(E) = \mathbb{Z} + m_0\mathcal{O}_K$ is the order in $K$ with conductor $m_0$.*
2. *If $(p, m) = 1$ then the map $\varphi \mapsto \widehat{\varphi}$ is an isomorphism of $\mathrm{End}(\widetilde{E})$ onto $\mathrm{End}(E)$.*

**Proof.** Lang [16, Theorem 13.4.12].

**Theorem 12** *Let $E$ be an elliptic curve over a finite field $k$ of characteristic $p$ and let $\varphi$ be an endomorphism of $E$. Then there exists an elliptic curve $\widetilde{E}$ defined over a number field $H$, an endomorphism $\widetilde{\varphi}$ of $\widetilde{E}$, and a prime $\mathfrak{p}$ over $p$ in $H$ such that $E$ is isomorphic to the reduction of $\widetilde{E}$ at $\mathfrak{p}$, and $\varphi$ corresponds to the reduction of $\widetilde{\varphi}$ under this isomorphism.*

**Proof.** Lang [16, Theorem 13.5.14].

# Chapter 3

# Complex multiplication

## 3.1 Elliptic and modular functions

Elliptic functions are meromorphic functions on the complex plane which are invariant under translation by a lattice $\Lambda$. As such, elliptic functions are well defined on the complex torus $\mathbb{C}/\Lambda$ and give us a means of parametrizing elliptic curves over $\mathbb{C}$. With proper normalizations, these functions give us integral models for elliptic curves. The relations between elliptic functions, derived in the setting of complex analysis, are equally valid over any field.

Modular functions, and more generally modular forms, are functions on the lattices themselves. Using the complex analytic isomorphisms associating an elliptic curve to a lattice in $\mathbb{C}$ via elliptic functions, we may view modular functions as parametrizing the set of elliptic curves as a whole. With this perspective we can reinterpret elliptic functions as functions on the space of lattices.

### Weierstrass $\wp$-function

The classical elliptic function of study is the Weierstrass $\wp$-function. For a lattice $\Lambda$, the Weierstrass $\wp$-function is defined as follows:

$$\wp(z;\Lambda) = z^{-2} + \sum_{\omega\in\Lambda}{}' \left((z-\omega)^{-2} - \omega^{-2}\right),$$

where the sum is restricted to nonzero $\omega$ in $\Lambda$. From the definition, one sees that $\wp$ is a meromorphic function on $\mathbb{C}$ with double poles at the lattice points and holomorphic elsewhere. The following theorem provides justification for the study of $\wp(z;\Lambda)$.

**Theorem 13** *The field of elliptic functions with respect to $\Lambda$ is generated by $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$.*

From the definition of the Weierstrass $\wp$-function, one can show that for any lattice $\Lambda' \supseteq \Lambda$,

$$\wp(z;\Lambda') = \wp(z;\Lambda) + \sum_{\omega'} \left(\wp(z+\omega';\Lambda) - \wp(\omega';\Lambda)\right), \tag{3.1}$$

where $\omega'$ runs over a set of representatives for the nonzero cosets of $\Lambda'/\Lambda$.

## Eisenstein series

Given a lattice $\Lambda$ and an integer $k > 2$ we define the Eisenstein series $G_k$ with respect to $\Lambda$ to be

$$G_k(\Lambda) = \sum_{\omega\in\Lambda}{}' \omega^{-k}.$$

Note that $G_k(\Lambda) = 0$ is $k$ is odd. We can express the coefficients of $\wp$ in terms of the $G_k(\Lambda)$ as follows:

$$\wp(z;\Lambda) = z^{-2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

The utility of this expression is due to the fact that each Eisenstein series $G_k(\Lambda)$ can be expressed as a polynomial in $G_4(\Lambda)$ and $G_6(\Lambda)$ with positive rational coefficients. Specifically, for $m > 3$, the Eisenstein series $G_{2m}(\Lambda)$ can be expressed in terms of the $G_{2r}(\Lambda)$ with $r < m-1$ by the following equation:

$$(2m+1)(m-3)(2m-1)G_{2m}(\Lambda) = 3\sum_{r=2}^{m-2}(2r-1)(2m-2r-1)G_{2r}(\Lambda)G_{2m-2r}(\Lambda).$$

## A classical equation

One can now verify the classical equation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - 60G_4(\Lambda)\wp(z;\Lambda) - 140G_6(\Lambda),$$

relating $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$. The discriminant of this curve is

$$\Delta(\Lambda) = (60G_4(\Lambda))^3 - 27(140G_6(\Lambda))^2,$$

and this value is nonzero [29, Theorem VI.3.6(a)]. Thus the elliptic curve $E$ given by the above Weierstrass equation is parametrized by the functions $\wp(z;\Lambda)$, and $\wp'(z;\Lambda)$:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & E, \\ z & \longmapsto & (\wp(z;\Lambda), \wp'(z;\Lambda)) \end{array}$$

and the map is an isomorphism of groups [29, Theorem VI.3.6(b)]. Moreover the following categories are equivalent [29, Theorem VI.5.3]:

1. The category $\mathcal{L}$ of lattices in $\mathbb{C}$ with morphisms given by homothety maps:
$$\mathrm{Mor}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}.$$
2. The category $\mathcal{T}$ of complex tori $\mathbb{C}/\Lambda$ with holomorphic maps taking 0 to 0 for morphisms.
3. The category $\mathcal{E}$ of elliptic curves over $\mathbb{C}$ with isogenies as morphisms.

## Eisenstein series revisited

We now consider Eisenstein series as functions on lattices in $\mathbb{C}$. From the definition of $G_k(\Lambda)$ it is clear that $G_k(\lambda\Lambda) = \lambda^{-k}G_k(\Lambda)$. Eisenstein series, and modular forms in general, are naturally viewed as functions on the set of lattices but for doing work on these functions, we translate to the setting of the upper half plane $\mathfrak{H}$ as follows. Let $\{\omega_1, \omega_2\}$ be a basis for $\Lambda$, and let $\tau$ be $\omega_1/\omega_2$. We define
$$G_k(\tau) = G_k(\langle\tau, 1\rangle) = G_k(\omega_2^{-1}\Lambda) = \omega_2^k G_k(\Lambda).$$
It is standard to choose an orientation $(\omega_1, \omega_2)$ on the basis such that $\Im(\omega_1/\omega_2) > 0$, and to study $G_k(\tau)$ on the upper half plane $\mathfrak{H}$. The action of $SL_2(\mathbb{Z})$ on the set of bases for $\Lambda$, given by
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\omega_1, \omega_2) = (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$
is transitive on the set of bases for $\Lambda$ oriented such that $\Im(\omega_1/\omega_2) > 0$.
We thus let $SL_2(\mathbb{Z})$ be the induced left action on $\mathfrak{H}$ given by
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = \frac{a\tau + b}{c\tau + d}.$$
Then $G_k : \mathfrak{H} \to \mathbb{C}$ is a holomorphic function such that
$$G_k(\alpha\tau) = (c\tau + d)^k G_k(\tau),$$
for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$.

**Theorem 14** *The ring of modular forms for $SL_2(\mathbb{Z})$ is $\mathbb{C}[G_4(\tau), G_6(\tau)]$.*

Return to modular forms as functions on lattices. Let $\mathfrak{a}$ be a projective ideal for an order $\mathcal{O}$ in an imaginary quadratic extension of $\mathbb{Q}$. The condition that $\mathfrak{a}$ is projective over $\mathcal{O}$ is equivalent to the condition that $\mathcal{O}$ is precisely the order ring of elements $\{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$. From the equivalence of categories of lattices and elliptic curves, this implies that the elliptic curve $E(\mathfrak{a})$ has ring of endomorphisms isomorphic to $\mathcal{O}$.

## Fourier series expansions

The element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ acts on $\mathfrak{H}$ by translation by 1, and a modular form $f(\tau)$ for $SL_2(\mathbb{Z})$ is left invariant under this action. Thus $f(\tau)$ has a Fourier series expansion

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^n,$$

where $q = e^{2\pi i\tau}$. The condition that $f(\tau)$ be meromorphic at the at $\infty$ says that all but finitely many of the coefficients $a_n$ for $n < 0$ are zero.

The Eisenstein series have particularly nice Fourier series expansions

**Proposition 15** *Let $G_k(\tau)$ be the Eisenstein series of weight $k$ and let $q = e^{2\pi i}$. Then $G_k(\tau)$ can be expessed as a series in $q$ by*

$$G_k(\tau) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

*where $\sigma_r(n) = \sum_{d|n} d^r$.*

Recall that the Riemann zeta function, at positive even values $k$, is equal to $\zeta(k) = -\frac{(2\pi i)^k}{2(k!)} B_k$, where $B_k$ is the $k$-th Bernoulli number. Recall that the Bernoulli numbers are defined by the equation

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

The first few Bernoulli numbers are:

$$B_0 = 1, \qquad B_1 = -\frac{1}{2}, \qquad B_2 = \frac{1}{6}, \qquad B_4 = -\frac{1}{2},$$

$$B_6 = \frac{1}{42}, \qquad B_8 = -\frac{1}{30}, \qquad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730},$$

and $B_k = 0$ for odd $k$ greater than 1.

This motivates us to define a normalized Eisenstein series by

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum \sigma_{k-1}(n) q^n.$$

The series $E_k(\tau)$ has an equivalent series expansion of the form

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum \frac{n^{k-1} q^n}{1 - q^n}.$$

We also have nice series expansions for $\Delta(\tau)$:

$$\begin{aligned}\Delta(\tau) &= (2\pi)^{12}\frac{(E_4(\tau)^3 - E_6(\tau)^2)}{12^3} \\ &= (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}.\end{aligned}$$

Hereafter we will define $\Delta(\tau)$ to be the normalized version $\Delta(\tau) = q\prod(1-q^n)^{24}$. We can now express $j(\tau)$ as

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots .$$

Consider also the Fourier series development for $\wp$:

$$\wp(z;\tau) = (2\pi i)^2\left[\frac{1}{12} - 2\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty}\frac{q^n q_z}{(1-q^n q_z^n)^2}\right].$$

where $q = e^{2\pi i\tau}$ as before and $q_z = e^{2\pi iz}$.
Returning to the modular parametrization of $E$, define

$$\widetilde{\wp}(z;\tau) = \frac{\wp(z;\tau)}{(2\pi i)^2} \quad \text{and} \quad \widetilde{\wp}'(z;\tau) = \frac{\wp'(z;\tau)}{2(2\pi i)^3}.$$

Then the following relation holds.

$$\widetilde{\wp}'(z;\tau)^2 = \widetilde{\wp}(z;\tau)^3 - \frac{E_4(\tau)}{48}\widetilde{\wp}(z;\tau) - \frac{E_6(\tau)}{864}.$$

## Higher levels

We have reviewed modular forms viewed as functions on the space of lattices, and their use to parametrize the collection of elliptic curves over $\mathbb{C}$. We wish to extend this idea to achieve parametrizing spaces for elliptic curves with additional structure. As a principal example, we consider pairs of lattices $(\Lambda, \Lambda')$ such that $\Lambda \subseteq \Lambda'$ and the quotient of $\Lambda'$ by $\Lambda$ is a cyclic subgroup of order $N$. From the equivalence of categories such an inclusion of lattices corresponds to an isogeny of elliptic curves $E(\Lambda) \to E(\Lambda')$ with cyclic kernel of order $N$. Translating the setting of lattices back to our working environment in $\mathfrak{H}$, we find that the pair $(\Lambda, \Lambda')$ gives us a pair $(\tau, \tau/N)$ and that the subgroup fixing such pairs is the group $\Gamma_0(N)$ defined by

$$\Gamma_0(N) = \{\alpha \in SL_2(\mathbb{Z}) : \alpha \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod N\}.$$

We say that $\Gamma_0(N)$ corresponds to the moduli problem of classifying cyclic isogenies of elliptic curves. The other two main subgroups of interest are

$$\begin{aligned}\Gamma_1(N) &= \{\alpha \in SL_2(\mathbb{Z}) : \alpha \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \bmod N\},\\ \Gamma(N) &= \{\alpha \in SL_2(\mathbb{Z}) : \alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N\}.\end{aligned}$$

The subgroups $\Gamma_1(N)$ and $\Gamma(N)$ of $SL_2(\mathbb{Z})$ correspond to the moduli problems of classifying elliptic curves with a cyclic point of order $N$ and of classifying elliptic curves with an oriented basis of the full group of $N$-torsion points.

Corresponding to the inclusions of groups

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z}),$$

there are corresponding maps of the modular curves

$$X(N) \to X_1(N) \to X_0(N) \to X(1),$$

which can be interpreted as forgetful maps.

## Generating modular forms

To introduce the "tools of the trade" we present the following modular forms and constructions by which we produce elements of the function fields of the modular curves $X_0(N)$, $X_1(N)$, and $X(N)$.

If $X' \to X$ is any map of curves then we have an inclusion of $K(X)$ in $K(X')$. Similarly we have an inclusion of $M_n(\Gamma)$ in $M_n(\Gamma')$ for any congruence subgroup $\Gamma' \subseteq \Gamma$.

The modular interpretation of $X_0(N) \to X(1)$ which we interpret as the map

$$\varphi : (E \to E') \longmapsto E$$

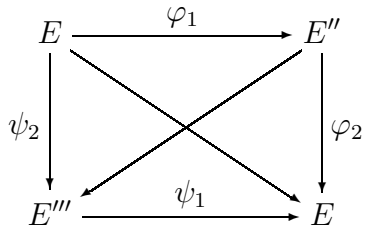
suggests the possibility of projecting onto the image curve $E'$. This would give a second embedding of $K(X(1))$ in $K(X_0(N))$. Indeed the map sending $\varphi$ to its dual $\widehat{\varphi}$ gives an involution of the curve $X_0(N)$ which exchanges these projections. More generally, suppose that $N = pq$ is the product of two primes. An isogeny $\varphi : E \to E'$ of degree $N$ decomposes as

$$E \xrightarrow{\varphi_1} E'' \xrightarrow{\varphi_2} E'$$

where $\varphi_1$ has degree $p$ and $\varphi_2$ has degree $q$. Similarly we may decompose $\varphi$ as

$$E \xrightarrow{\psi_2} E''' \xrightarrow{\psi_1} E'$$

where $\psi_2$ has degree $q$ and $\psi_1$ has degree $p$. By means of combinations of $\varphi_1, \varphi_2, \psi_1, \psi_2$ and their duals, we could imagine that there should be an involution of $X_0(N)$ exchanging $\varphi$ with any of the diagonal maps or its dual diagram below.




Indeed, we arrive at the definition of the Atkin-Lehner involution via this construction (see [1]).

Thus the additions to our repertoire of modular forms will be those forms $f(n\tau)$ for $n \in \mathbb{Z}$ and $f(\tau)$ a previously described form.

For a moment let us return to the definition of the Eisenstein series $G_k(\tau)$. Recall that

$$G_k(\tau) = \sum_{(n,m)\in\mathbb{Z}^2}{}' (m\tau + n)^{-k}.$$

We observed that for $k$ odd $G_k(\tau)$ is zero and only for $k > 2$ does $G_k(\tau)$ converge. In order to salvage $k = 2$ we must separate the sums as follows.

$$G_2(\tau) = \sum_{m\in\mathbb{Z}} \sum_{n\in\mathbb{Z}}{}' (m\tau + n)^{-2},$$

where the sum is restricted to $n \neq 0$ when $m = 0$. The series $G_2(\tau)$ defined in this manner is a convergent holomorphic function. As before, we obtain a Fourier series expansion

$$G_2(\tau) = 2\zeta(2)\left(1 - 24\sum_{n\in\mathbb{Z}} \sigma_1(n)q^n\right),$$

and normalize to get $E_2(\tau) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n$. The holomorphic function $E_2(\tau)$ is almost but not quite a modular form, transforming according to the following rules [13, Theorem III.2.7].

$$\begin{aligned} E_2(-1/\tau) &= \tau^2 E_2(\tau) + \frac{12\tau}{2\pi i}, \\ E_2(\tau + 1) &= E_2(\tau) \end{aligned}$$

For a positive integer $N$, the following function

$$\begin{aligned} E_2^*(\tau) &= \frac{NE_2(N\tau) - E_2(\tau)}{24} \\ &= \frac{N-1}{24} + \sum_{n=1}^{\infty} \sigma_1^*(n)q^n, \end{aligned}$$

where

$$\sigma_1^*(n) = \begin{cases} \sigma_1(n) \text{ if } n \not\equiv 0 \bmod N \\ \sigma_1(n/N) \text{ otherwise} \end{cases}$$

is a modular form. The modular interpretation for $E_2^*(\tau)$ stems from the following formula [28]:

$$NE_2^*(\tau) = -\frac{1}{2}\sum_{i=1}^{N-1} \wp(i\tau/N;\tau).$$

Thus it gives the first symmetric function in the $x$-values of the points of a cyclic subgroup of order $N$ on $E_\Lambda(\mathbb{C})$, where $x(P)$ and $x(-P)$ are counted once and $x(Q)$ is counted with multiplicity $1/2$ for all $Q$ in $E_\Lambda[2]$.

Next we define $\eta(\tau) = q^{1/24}\prod(1-q^n)$, a 24-th root of $\Delta(\tau)$. Then $\eta(\tau)$ is holomorphic on $\mathfrak{H}$ and transforms as follows [30, Theorem I.8.3] under the generators for $SL_2(\mathbb{Z})$:

$$\begin{aligned} \eta(-1/\tau) &= \sqrt{-i\tau}\,\eta(\tau), \text{ and} \\ \eta(\tau+1) &= e^{2\pi i/24}\,\eta(\tau), \end{aligned}$$

where $\sqrt{\ }$ is a branch of the square root which is positive on the positive real axis.

While $\eta(\tau)$ is not a modular form we use $\eta(\tau)$ to construct modular forms. For instance, set

$$u = 13\left(\frac{\eta(13\tau)}{\eta(\tau)}\right)^2.$$

Then $u$ is a modular form for $\Gamma_0(13)$ and the Atkin-Lehner operator acts in a particularly simple fashion on $u$.

$$u|_{W_{13}} = \left(\frac{\eta(\tau)}{\eta(13\tau)}\right)^2 = \frac{13}{u}.$$

## Theta functions

Theta functions associated to positive definite quadratic forms over $\mathbb{Z}$ provide an abundant source of modular forms. This will be particularly useful when applied with the binary and quaternary quadratic forms associated to ideal classes of orders in complex imaginary extensions of $\mathbb{Q}$ and of orders in quaternion algebras over $\mathbb{Q}$.

Let $\mathbf{q} : V \to \mathbb{Q}$ be a positive definite quadratic form of even dimension $n = 2k$ over $\mathbb{Q}$ with integral lattice $\Lambda$ of determinant $\det(\Lambda)$. Then we can form a holomorphic function on $\mathfrak{H}$

$$\theta_\Lambda(\tau) = \sum_{\omega\in\Lambda} q^{\mathbf{q}(\omega)},$$

where $q = e^{2\pi i\tau}$, and the transformation of $\theta_\Lambda(\tau)$ under elements of the modular group $SL_2(\mathbb{Z})$ is well understood (see Chapter IX of Schoeneberg [26]). In the special case that $n = 4$ and $\det(\Lambda) = N^2$ then $\theta_\Lambda(\tau)$ is a modular form of weight 2 for $\Gamma_0(N)$.

## Models for modular curves

We can now make use of the above constructions for modular forms to produce models for modular curves, in particular for $X_0(N)$. Classically one uses the functions $j = j(\tau)$ and $j_N = j(N\tau)$ to construct the field of modular functions on $X_0(N)$. By the following theorem, this gives us all functions on $X_0(N)$.

**Theorem 16** *The field of modular functions for* $\Gamma_0(N)$ *is* $\mathbb{C}(j, j_N)$.

The modular functions $j$ and $j_N$ satisfy the classical *modular equation* $\Phi_N(j, j_N) = 0$, where $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. While this gives an aesthetically pleasing relation between the $j$-invariant of a curve $E$ and the $j$-invariants of the curves, $\Phi_N(X, Y)$ is a singular model for $X_0(N)$ and has many singularities over $\mathrm{Spec}(\mathbb{Z})$. As a result, the coefficients of $\Phi_N(X, Y)$ can be quite large. For instance for the first few values of $N$, we have

$$\begin{aligned}\Phi_2(X,Y) &= (X+Y)^3 - X^2Y^2 + 1485XY(X+Y) - 162000(X+Y)^2 \\ &\quad + 41097375XY + 8748000000(X+Y) - 157464000000000,\end{aligned}$$

$$\begin{aligned}\Phi_3(X,Y) &= (X+Y)^4 - X^3Y^3 + 2232X^2Y^2(X+Y) + 36864000(X+Y)^3 \\ &\quad - 1069960XY(X+Y)^2 + 2590058000X^2Y^2 \\ &\quad + 8900112384000XY(X+Y) + 452984832000000(X+Y)^2 \\ &\quad - 771751936000000000XY + 1855425871872000000000(X+Y),\end{aligned}$$

$$\begin{aligned}\Phi_4(X,Y) &= (X+Y)^6 - X^4Y^4(X+Y) + 1488X^4Y^4 + 2976X^3Y^3(X+Y)^2 \\ &\quad - 2533680X^2Y^2(X+Y)^3 + 561444603XY(X+Y)^4 \\ &\quad - 8507430000(X+Y)^5 + 80975207520X^3Y^3(X+Y) \\ &\quad - 120497741069824X^3Y^3 + 1425218210971653X^2Y^2(X+Y)^2 \\ &\quad + 1194227286647130000XY(X+Y)^3 \\ &\quad + 24125474716854750000(X+Y)^4 \\ &\quad - 9179452324809702900000X^2Y^2(X+Y) \\ &\quad + 13627503572259970080000000X^2Y^2 \\ &\quad + 12519709864947556179750000XY(X+Y)^2 \\ &\quad - 228051803515480321950000000000(X+Y)^3 \\ &\quad + 25707218051964255186928710937 5XY(X+Y) \\ &\quad + 15801023694795376772418750000000 0(X+Y)^2 \\ &\quad - 41028705695913093857569921875000 0XY \\ &\quad - 36493632779675765840437500000000000 0(X+Y) \\ &\quad + 28094937472219537210964062500000000000,\end{aligned}$$

and the modular polynomial of level 13 is

$$\begin{aligned}\Phi_{13}(X,Y) &= (X+Y)^{14} - X^{13}Y^{13} + 9672(X+Y)X^{12}Y^{12} \\ &\quad - 40616316(X+Y)^2X^{11}Y^{11} + 97116140576(X+Y)^3X^{10}Y^{10} \\ &\quad - 145742356534710(X+Y)^4X^9Y^9 \\ &\quad + 142727120530755696(X+Y)^5X^8Y^8 \\ &\quad + 63336131453363537808X^{12}Y^{12} \\ &\quad + \cdots \\ &\quad \cdots + 2^{182}\,3^{61}\,5^{33}\,11^{15}\,13^3\,23^6\,180347944559(X+Y)^3 \\ &\quad - 2^{184}\,3^{61}\,5^{35}\,11^{15}\,13{\cdot}23^6\,209767{\cdot}6780941(X+Y)XY \\ &\quad - 2^{200}\,3^{63}\,5^{38}\,7^2\,11^{18}\,23^9\,XY \\ &\quad + 2^{198}\,3^{63}\,5^{36}\,11^{18}\,13^3\,23^9(X+Y)^2,\end{aligned}$$

a polynomial whose expanded coefficients, if included herein, would constitute a significant increase in the length of this document.

The modular curve $X_0(13)$ has genus zero, and its function field is generated by the function the function $u = 13(\eta(13\tau)/\eta(\tau))^2$ defined earlier. In contrast to the enormous coefficients in the expression relating $j$ and $j_{13}$, we find that $j$ can be simply expressed in terms of $u$ with relatively small coefficients as follows.

$$\begin{aligned}j(\tau) &= (u^{14} + 26u^{13} + 325u^{12} + 2548u^{11} + 13832u^{10} + 54340u^9 \\ &\quad +157118u^8 + 333580u^7 + 509366u^6 + 534820u^5 + 354536u^4 \\ &\quad +124852u^3 + 15145u^2 + 746u + 13)/u.\end{aligned}$$

## 3.2 Class fields and complex multiplication

Among elliptic curves over $\mathbb{C}$, those possessing "extra" endomorphisms are exceptional. Typically, an elliptic curve $E$ has $\mathrm{End}(E) \cong \mathbb{Z}$, but up to isomorphism there are countably many curves such that the endomorphism rings have rank 2 over $\mathbb{Z}$. In terms of the equivalent category of lattices in $\mathbb{C}$, if the endomorphism ring of a lattice is not $\mathbb{Z}$, then it is equal to an order $\mathcal{O}$ in a quadratic imaginary extension $K$ of $\mathbb{Q}$ in $\mathbb{C}$. An elliptic curve with $\mathrm{End}(E) \otimes \mathbb{Q} \cong K$ is said to have *complex multiplication* by $K$. When we wish to be more restrictive, we will say that $E$ has complex multiplication by $\mathcal{O}$. Elliptic and modular functions, evaluated at the "special values" corresponding to elliptic curves with complex multiplication and at the torsion points on such curves, generate abelian extensions of $K$. The use of these functions to generate abelian extensions of quadratic fields $K$ is analogous to the use of the exponential function at points corresponding to torsion in $\mathbb{G}_m(\mathbb{C})$ to generate abelian extensions of $\mathbb{Q}$.

We recall some definitions and results from class field theory. Let $L/K$ be a finite abelian extension, and $D_{L/K}$ the discriminant of $L$ over $K$. We write $\mathcal{O}_K$ for the maximal order of $K$ and $\mathcal{O}_L$ for the maximal order of $L$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. We define $I_K$ to be the group of fractional ideals of $\mathcal{O}_K$, and let $I(\mathfrak{m})$ be the subgroup

freely generated as an abelian group by the prime ideals relatively prime to $\mathfrak{m}$. We denote by $P(\mathfrak{m})$ the subgroup of principal fractional ideals in $I(\mathfrak{m})$. For an integer $m$ we write $I(m) = I(m\mathcal{O}_K)$, and similarly write $P(m)$ for $P(m\mathcal{O}_K)$. For each prime $\mathfrak{p}$ relatively prime to $D_{L/K}$ there exists a unique element $\sigma_\mathfrak{p}$ in the Galois group $\mathrm{Gal}(L/K)$ such that $\sigma_\mathfrak{p}(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{p}\mathcal{O}_L$ for all $x$ in the maximal order $\mathcal{O}_L$ of $L$. The map $\mathfrak{p} \mapsto [\mathfrak{p}, L/K] = \sigma_\mathfrak{p}$ extends multiplicatively to all of $I(D_{L/K})$. We call the homomorphism

$$[\,\cdot\,, L/K] : I(D_{L/K}) \longrightarrow \mathrm{Gal}(L/K)$$

the *Artin map*. A result of class field theory says that the Artin map is surjective.

The Hilbert class field $H$ of $K$ is defined to be the largest unramified abelian extension of $K$. The kernel of the Artin map of $H/K$ consists of the principal fractional ideals in $\mathcal{O}_K$. For imaginary quadratic extensions over $\mathbb{Q}$, we have a beautiful description of $H$ in terms of the modular function $j$ defined on lattices.

**Theorem 17** *Let $K/\mathbb{Q}$ be a quadratic imaginary field with ring of integers $\mathcal{O}_K$, then $j(\mathcal{O}_K)$ is an algebraic integer which generates the Hilbert class field over $K$. The Galois conjugates of $j(\mathcal{O}_K)$ are the values $j(\mathfrak{a}_i)$, where $\{\mathfrak{a}_i\}$ is a complete set of representatives of the ideal classes of $\mathcal{O}_K$. The Artin map defines an isomorphism of $\mathrm{Cl}(\mathcal{O}_K)$ with $\mathrm{Gal}(H/K)$ such that $[\mathfrak{p}, H/K](j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$.*

**Proof.** Silverman [30, Theorem II.4.3] or Lang [16, Chapter 10, §1, Theorem 1].

We would like to consider extensions of $H$ by adjoining torsion points of an elliptic curve $E$ with complex multiplication by $\mathcal{O}_K$. We first need to define a *Weber function* $h : E \to \mathbb{P}^1$ to be a quotient of $E$ by its automorphism group. In terms of a Weierstrass equation for $E$, a Weber function for $E$ is given as follows:

$$h(x) = \begin{cases} c_4c_6x/\Delta & \text{if} \quad j_E \neq 0, 1728, \\ c_4^2x^2/\Delta & \text{if} \quad j_E = 1728, \\ c_6x^3/\Delta & \text{if} \quad j_E = 0. \end{cases}$$

where $x$, $c_4$, and $c_6$ are defined as in Chapter 2. Alternatively, with respect to a lattice $\Lambda$, we can construct an analytic Weber function on $\mathbb{C}$. Let $\Lambda \subseteq \mathbb{C}$ be a lattice such that

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \\ z & \longmapsto & (\widetilde{\wp}(z;\Lambda), \widetilde{\wp}'(z;\Lambda)) \end{array}$$

gives an analytic isomorphism. A Weber function for $E$ is given as follows.

$$h(z;\Lambda) = \begin{cases} E_4(\Lambda)E_6(\Lambda)\widetilde{\wp}(z;\Lambda)/\Delta(\Lambda) & \text{if} \quad j(\Lambda) \neq 0, 1728, \\ E_4(\Lambda)^2\widetilde{\wp}(z;\Lambda)^2/\Delta(\Lambda) & \text{if} \quad j(\Lambda) = 1728, \\ E_6(\Lambda)\widetilde{\wp}(z;\Lambda)^3/\Delta(\Lambda) & \text{if} \quad j(\Lambda) = 0. \end{cases}$$

These three cases correspond to $\mathrm{Aut}(E)$ having $2, 4$, and $6$ elements, respectively. The weights of the numerators and denominators of the Weber functions above are each 12, in the sense that the map $(z;\Lambda) \mapsto (\lambda z;\lambda\Lambda)$ multiplies both numerator and denominator by $\lambda^{-12}$. Thus up to some change of variable $z \mapsto \lambda z$, the Weber function is an invariant of the homothety class of $\Lambda$.

Before stating the next results, we define *ray class fields* and *ring class fields* over $K$. For any integral ideal $\mathfrak{m}$ of $\mathcal{O} = \mathrm{End}(E)$ we define $E[\mathfrak{m}] = \{P \in E(\mathbb{C}) : \varphi(P) = \mathbf{O} \text{ for all } \varphi \in \mathfrak{m}\}$. Let $\Lambda$ be a lattice such that, as before, $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. The torsion points $E[\mathfrak{m}]$ corresponds to $\mathfrak{m}^{-1}\Lambda/\Lambda \subseteq \mathbb{C}/\Lambda$. Thus in terms of our Weber functions on $E$ and on $\mathbb{C}$, we have $h(E[\mathfrak{m}]) = h(\mathfrak{m}^{-1}\Lambda;\Lambda)$. For $\alpha \in K^*$ by $\alpha \equiv 1 \bmod^* \mathfrak{m}$ we mean that $v_{\mathfrak{p}}(\alpha - 1) \geq r$ for every prime power $\mathfrak{p}^r$ dividing $\mathfrak{m}$ with positive exponent. We define

$$\begin{aligned} P_1(\mathfrak{m}) &= \{(\alpha) \in P(\mathfrak{m}) : \alpha \equiv 1 \bmod^* \mathfrak{m}\} \text{ and,} \\ P_{\mathbb{Z}}(\mathfrak{m}) &= \{(\alpha) \in P(\mathfrak{m}) : \alpha/n \equiv 1 \bmod^* \mathfrak{m} \text{ for some } n \in \mathbb{Z}\}. \end{aligned}$$

Note that $(\alpha) \in P_1(\mathfrak{m})$ does not imply that $\alpha \equiv 1 \bmod^* \mathfrak{m}$, only that there exists a unit $\mu \in \mathcal{O}_K^*$ such that $\mu\alpha \equiv 1 \bmod^* \mathfrak{m}$. Also note that if $m$ is the largest integer such that $\mathfrak{m}$ is contained in $(m)$, then $P_{\mathbb{Z}}(m\mathcal{O}_K) = P_{\mathbb{Z}}(\mathfrak{m})$. Thus we assume $\mathfrak{m} = (m)$ and write $P_{\mathbb{Z}}(m)$ for $P_{\mathbb{Z}}(m\mathcal{O}_K)$.

The ray class field modulo $\mathfrak{m}$, denoted $K_{\mathfrak{m}}$, is defined to be the largest unramified abelian extension $L$ of $K$ such that the Artin map $[\,\cdot\,, L/K] : I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ contains $P_1(\mathfrak{m})$ in its kernel.

The ring class field of conductor $m$ is defined to be the largest abelian extension $L$ of $K$ such that the Artin map $[\,\cdot\,, L/K] : I(m) \to \mathrm{Gal}(L/K)$ contains $P_{\mathbb{Z}}(m)$ in its kernel. To justify the nomenclature for the definition of the ring class field, we first recall that an order $\mathcal{O}$ in $K$ has the form $\mathbb{Z} + m\mathcal{O}_K$, for a unique positive integer $m$, the *conductor* of $\mathcal{O}$. The ideal class group $\mathrm{Cl}(\mathcal{O})$ of projective ideals of $\mathcal{O}$ is isomorphic to $I(m)/P_{\mathbb{Z}}(m)$. We call the ring class field of conductor $m$ the ring class field for $\mathcal{O}$ and denote it by $K_{\mathcal{O}}$.

We can now state the main theorems of this section.

**Theorem 18** *Let $K/\mathbb{Q}$ be a quadratic imaginary extension of $\mathbb{Q}$, let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$, and let $\mathfrak{a}$ be any fractional ideal for $\mathcal{O}_K$. Then*

$$K_{\mathfrak{m}} = K(j(\mathfrak{a}), h(\mathfrak{m}^{-1}\mathfrak{a};\mathfrak{a}))$$

*is the ray class field modulo $\mathfrak{m}$.*

**Proof.** Silverman [30, Theorem II.5.6] or Lang [16, Chapter 10, §1, Theorem 2].

**Theorem 19** *Let $K/\mathbb{Q}$ be a quadratic imaginary extension of $\mathbb{Q}$ and let $\mathcal{O}$ be an order of conductor $m$ in $K$. Then $j(\mathcal{O})$ is an algebraic integer which generates the ring class field for $\mathcal{O}$ over $K$. The Galois conjugates for $j(\mathcal{O})$ are $j(\mathfrak{a}_i)$, where $\{\mathfrak{a}_i\}$ is a complete set of coset representatives for the projective ideal classes of $\mathcal{O}$. The Artin map defines an isomorphism of* $\mathrm{Cl}(\mathcal{O})$ *with* $\mathrm{Gal}(K_{\mathcal{O}}/K)$ *such that* $[\mathfrak{p}\mathcal{O}_K, K_{\mathcal{O}}/K](j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$*, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ not dividing $m$.*

**Proof.** Lang [16, Chapter 10, §3, Theorem 5]

As an application we can now define the class polynomial $H_D(X)$. Let $\mathcal{O}$ be an order of discriminant $D$ in an imaginary quadratic extension of $\mathbb{Q}$, and let $\{\mathfrak{a}_i\}$ be a complete set of coset representatives of the $h(\mathcal{O})$ projective ideal classes of $\mathcal{O}$. The above theorem implies that

$$H_D(X) = \prod_{i=1}^{h(\mathcal{O})} (X - j(\mathfrak{a}_i))$$

is an irreducible polynomial in $\mathbb{Z}[X]$.

For example, if we take $D = -71$, the class polynomial $H_{-71}(X)$ is

$$\begin{aligned} X^7 + 313645809715X^6 - 3091990138604570X^5 + 9839403881004781204930 2X^4 \\ - 8235342634397307799680913 89X^3 + 5138800366453976780323726329446X^2 \\ - 4253194739461396032746051511876 59X + 11^9 \cdot 17^6 \cdot 23^3 \cdot 41^3 \cdot 47^3 \cdot 53^3. \end{aligned}$$

As with the modular equation, the coefficients grow rapidly with the size of the discriminant. And as with the modular equations, one can try to deduce simpler expressions for the class polynomial using different modular functions. For instance, Yui and Zagier [37] use special values of certain classical Weber functions to find a reduced class equation

$$W_{-71}(t) = t^7 - t^6 - t^5 + t^4 - t^3 - t^2 + 2t + 1,$$

for the discriminant $-71$, where $t$ and $X$ satisfy the relation $(t^{24} - 16)^3 = t^{24}X$.

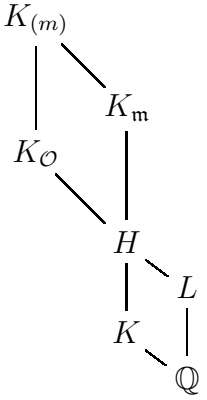
The following commutative diagram of exact sequences summarizes the ideal class

relations for an ideal $\mathfrak{m}$ and integer $m$ in $\mathfrak{m}$.

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G & \longrightarrow & \dfrac{(\mathbb{Z}/m\mathbb{Z})^*}{\{\pm 1\}} & \longrightarrow & \dfrac{(\mathcal{O}_K/\mathfrak{m})^*}{\mathcal{O}_K^* \bmod \mathfrak{m}} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \dfrac{\mathcal{O}_K^* + \mathfrak{m}}{\mathcal{O}_K^* + (m)} & \longrightarrow & \dfrac{I(m)}{P_1(m)} & \longrightarrow & \dfrac{I(\mathfrak{m})}{P_1(\mathfrak{m})} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \dfrac{(\mathcal{O}_K/m\mathcal{O}_K)^*}{\overline{\mathcal{O}_K^*}(\mathbb{Z}/m\mathbb{Z})^*} & \longrightarrow & \mathrm{Cl}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

We define $\mathfrak{m}$ to be *primitive* if $\mathfrak{m}$ is contained in no proper ideal $n\mathcal{O}_K$ for an integer $n$ in $\mathbb{Z}$. In the case of principal interest, $\mathfrak{m}$ is primitive and $m = \mathrm{N}(\mathfrak{m})$. In this case the cokernel of $(\mathcal{O}_K/\mathfrak{m})^*/\overline{\mathcal{O}_K^*}$ by $(\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$ is trivial. In particular, we will be interested in the case that $\mathfrak{m}$ is a power of a splitting prime $\mathfrak{p}$ of $\mathcal{O}_K$.

The class fields corresponding to the above Galois groups are as follows, where $H$ is the Hilbert class field, $L$ is the subfield generated by $j(\mathcal{O}_K)$ over $\mathbb{Q}$, and $m$ is an integer in the ideal $\mathfrak{m}$.




To put the class field theory in context with the elliptic curves having complex multiplication, we summarize the class field theory through the following dictionary with elliptic curves with complex multiplication. In the glossary below, let $E$ be an elliptic curve defined over the field generated by its $j$-invariant $j_E$ with endomorphism ring equal to the maximal order in $K$.

| | |
|---|---|
| $L = \mathbb{Q}(j_E)$ | Field of definition of $E$. The endomorphisms ring of $E$ over $L$ is $\mathrm{End}_L(E) = \mathbb{Z}$. |
| $H = K(j_E)$ | Field of definition of $\mathrm{End}(E)$, and all isogenies $E \to E'$ for a complete set of representatives $\{E'\}$ of the isomorphism classes of elliptic curves with endomorphism ring equal to $\mathcal{O}_K$. |
| $K_{\mathfrak{m}}/H$ | Splitting field for cyclic points $E[\mathfrak{m}]$ modulo $\mathrm{Aut}(E)$. The group $E[\mathfrak{m}]$ is the kernel of the isogeny $E \to E'$ corresponding to $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{m}^{-1}\Lambda$ where $\mathcal{O}_K \cong \mathrm{End}(\Lambda) \subseteq \mathbb{C}$. |
| $K_{\mathcal{O}}/H$ | Splitting field for all isogenies of $E' \to E''$, for a complete set of representatives of $\{E'\}$ and $\{E''\}$ of the isomorphism classes of elliptic curves with complex multiplication by orders $\mathcal{O}'$ and $\mathcal{O}''$ contained in $\mathcal{O}_K$ and containing $\mathcal{O}$. |
| $K_{(m)}/H$ | Complete splitting field for $E[m]$ modulo $\mathrm{Aut}(E)$. |

## 3.3 The main theorem of complex multiplication

Theorems 17, 18, and 19 constitute the main theorem of complex multiplication. In this section we would like to combine the three theorems into one using the idele group of $K$. First we must recall the necessary definitions from class field theory.

Let $K$ be a field and $M_K$ be the set of places of $K$. The adele ring $A_K$ of a field $K$ is defined to be the restricted product $\prod' K_v$ of the completions $K_v$ of $K$ at each of the places $v$ of $K$ with respect to the local rings of integers $\mathcal{O}_v$. Let $S$ be a finite set of places of $K$ including the infinite places. Define $A_S$ by

$$A_S = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v,$$

with the product topology. Then each $A_S$ is a locally compact topological ring. $A_K$ is defined as the union of $A_S$ for all finite subsets $S$ of $M_K$ containing the infinite places. Defining each $A_S$ to be open topological subrings induces a topology on $A_K$ as a topological ring.

Next we define the idele group $J_K$ of $K$. This will be a subgroup of the adeles consisting of the invertible elements $A_K^*$. The induced subset topology is insufficient to give $J_K$ the structure of a topological group. Instead we enlarge the topology on $J_K$ so that the map $x \mapsto x^{-1}$ is continuous. The topology on $J_K$ is defined to be that for which the homomorphism of $J_K$ to $A_K \times A_K$ given by $x \mapsto (x, x^{-1})$ is a homeomorphism of $J_K$ onto its image.

*Definition of Artin map not yet stated in general.*

Let $K \subseteq \mathbb{C}$ be a quadratic imaginary extension of $\mathbb{Q}$. Let $t$ be an idele for $K$, and let $\Lambda$ be a lattice in $K$. As a special case, assume that $\mathrm{End}(\Lambda) = \mathcal{O}_K$. For any prime $\mathfrak{p}$ of $\mathcal{O}_K$, define $\Lambda_{\mathfrak{p}}$ to be the closure of $\Lambda$ in the completion of $K$ at $\mathfrak{p}$. From the

local-global correspondence of lattices, there is a well-defined lattice $t\Lambda$ defined by

$$t\Lambda = \bigcap_{\mathfrak{p}\in M_K} K \cap t_{\mathfrak{p}}\Lambda_{\mathfrak{p}}.$$

Moreover, there are natural isomorphisms

$$K/\Lambda \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\Lambda_{\mathfrak{p}} \text{ and } K/t\Lambda \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/t_{\mathfrak{p}}\Lambda_{\mathfrak{p}}.$$

This allows us to define an isomorphism $t : K/\Lambda \to K/t\Lambda$ by multiplication by $t_{\mathfrak{p}}$ on the $\mathfrak{p}$-primary component.

For the general case, we have an identification of adele rings $A_K = K \otimes A_{\mathbb{Q}}$, from which we have a decomposition of rings $A_K = \prod_p' K \otimes \mathbb{Q}_p$, restricted with respect to the rings $\mathcal{O}_K \otimes \mathbb{Z}_p$. For a prime $p$ in $\mathbb{Z}$, let $\Lambda_p = \Lambda \otimes \mathbb{Z}_p$. Then we can write an idele $t \in J_K$ as $(t_p)_{p\in M_{\mathbb{Q}}}$, and $t$ acts on $\Lambda$ by

$$t\Lambda = \bigcap_{p\in M_{\mathbb{Q}}} K \cap t_p\Lambda_p.$$

Again we have natural isomorphisms

$$K/\Lambda \cong \bigoplus_{p\in M_{\mathbb{Q}}} K_p/\Lambda_p, \text{ and } K/t\Lambda \cong \bigoplus_{p\in M_{\mathbb{Q}}} K_p/t_p\Lambda_p,$$

and we define an isomorphism $t : K/\Lambda \to K/t\Lambda$ by multiplication by $t_p$ on each component $K_p/\Lambda_p$.

This definition coincides with that for the special case, and for any lattice $\Lambda$ in $K$ we note that $\mathrm{End}(\Lambda) = \mathcal{O}$ for some order $\mathcal{O}$ in $K$. If the conductor of $\mathcal{O}$ is $m$, then for all primes $\mathfrak{p}$ of $M_K$ not dividing $m$, $(\mathcal{O}_K)_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ and the lattice $\Lambda_{\mathfrak{p}}$ is well-defined. We have the liberty of decomposing an idele $t \in J_K$ as $t = (t_{\mathfrak{p}})_{\mathfrak{p}\nmid m} \times (t_q)_{q|m})$, and view $t$ as acting locally at $\mathfrak{p}$ as in the previous case.

Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Corresponding to the automorphism of fields $\mathbb{C} \xleftarrow{\sigma} \mathbb{C}$ there is a morphism $\sigma^* : \mathrm{Spec}(\mathbb{C}) \longrightarrow \mathrm{Spec}(\mathbb{C})$. For any elliptic curve $E/\mathbb{C}$ we define $E^\sigma/\mathbb{C}$ to be the elliptic curve $E$ base extended by $\sigma^*$.

We can now state the main theorem of complex multiplication, in its idelic version.

**Theorem 20** *Let $K \subseteq \mathbb{C}$ be a quadratic imaginary extension of $\mathbb{Q}$, and let $\Lambda$ be a lattice in $K$. Let $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ be a complex analytic isomorphism to an elliptic curve $E$. Let $s$ be an idele of $K$ and let $\sigma$ be an automorphism of $\mathbb{C}$ such that $[s, K] = \sigma|_{K^{\mathrm{ab}}}$. Then there exists a unique complex analytic isomorphism*

$$\psi : \mathbb{C}/s^{-1}\Lambda \to E^\sigma(\mathbb{C})$$

*such that the following diagram is commutative.*

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\phi} & E(\mathbb{C}) \\ \Big\downarrow{\scriptstyle s^{-1}} & & \Big\downarrow{\scriptstyle \sigma} \\ K/s^{-1}\Lambda & \xrightarrow{\psi} & E^{\sigma}(\mathbb{C}) \end{array}$$

**Proof.** Lang [16, Chapter 10, §2, Theorem 3]. See also Silverman [30, Theorem II.8.2].

## 3.4 Actions of ideles

The above theorem suggests that we should study the action of $J_K$ on the collection of elliptic curves over $K^{\mathrm{ab}}$, given by $s \cdot E = E^{\sigma}$, where $\sigma = [s, K]$. On Weierstrass equations, this is the expected operation, taking a Weierstrass equation with coefficients $\{a_i\}$ to the Weierstrass equation with coefficients $\{a_i^{\sigma}\}$. Let $\mathcal{E}(K)$ be the category of elliptic curves over $K^{\mathrm{ab}}$ having complex multiplication by $K$. For each $s \in J_K$ this gives a functor of $\mathcal{E}(K)$ to itself, and we say that $J_K$ acts on the category $\mathcal{E}(K)$, and call this the arithmetic action of $J_K$. In our applications, this action will be unsatisfactory, since the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ does not act on elliptic curves over finite fields.

Consider the action we described on the set of lattices in $\mathbb{C}$, which for $s \in J_K$ takes $\Lambda$ to $s^{-1}\Lambda$. Let $\Lambda$ be one such lattice and let $\mathcal{O} = \mathrm{End}(\Lambda)$. If $s\mathcal{O}$ is an integral ideal of $\mathcal{O}$, then $s^{-1}\Lambda$ is properly contained in $\Lambda$. Then we have a canonical quotient map

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\varphi} \mathbb{C}/s^{-1}\Lambda \\ z \bmod \Lambda &\longmapsto z \bmod s^{-1}\Lambda \end{aligned}$$

If we use the Weierstrass parametrization of elliptic curves, for every elliptic curve $E_\Lambda$ and complex analytic isomorphism

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E_\Lambda, \\ z &\longmapsto (\widetilde{\wp}(z;\Lambda), \widetilde{\wp}'(z;\Lambda)) \end{aligned}$$

we can associate a curve $E_{s^{-1}\Lambda} = s \cdot E$ such that

$$\begin{aligned} \mathbb{C}/s^{-1}\Lambda &\longrightarrow E_{s^{-1}\Lambda}, \\ z &\longmapsto (\widetilde{\wp}(z;s^{-1}\Lambda), \widetilde{\wp}'(z;s^{-1}\Lambda)) \end{aligned}$$

In order to define this map independent of any Weierstrass equations we recall that

$$\begin{aligned}\widetilde{\wp}(z;\Lambda') &= \widetilde{\wp}(z;\Lambda) + \sum_{\omega'} \left(\widetilde{\wp}(z+\omega';\Lambda) - \widetilde{\wp}(\omega',\Lambda)\right),\\ \widetilde{\wp}'(z;\Lambda') &= \widetilde{\wp}'(z;\Lambda) + \sum_{\omega'} \left(\widetilde{\wp}'(z+\omega';\Lambda) - \widetilde{\wp}'(\omega',\Lambda)\right),\end{aligned}$$

where $\Lambda' = \mathfrak{a}^{-1}\Lambda \subseteq \Lambda$ and notice that for $G = E[\mathfrak{a}]$, and $x = \widetilde{\wp}(z,\Lambda)$ and $y = \widetilde{\wp}'(z,\Lambda)$, the functions $x_G$ and $y_G$ defined by

$$\begin{aligned}x_G(P) &= x(P) + \sum_{Q\in G-\{0\}} (x(P+Q) - x(Q)),\\ y_G(P) &= y(P) + \sum_{Q\in G-\{0\}} (y(P+Q) - y(Q)),\end{aligned}$$

correspond to $x_G = \widetilde{\wp}(z,\Lambda')$ and $y_G = \widetilde{\wp}'(z,\Lambda')$. This is precisely the isogeny we defined in § 2.4.

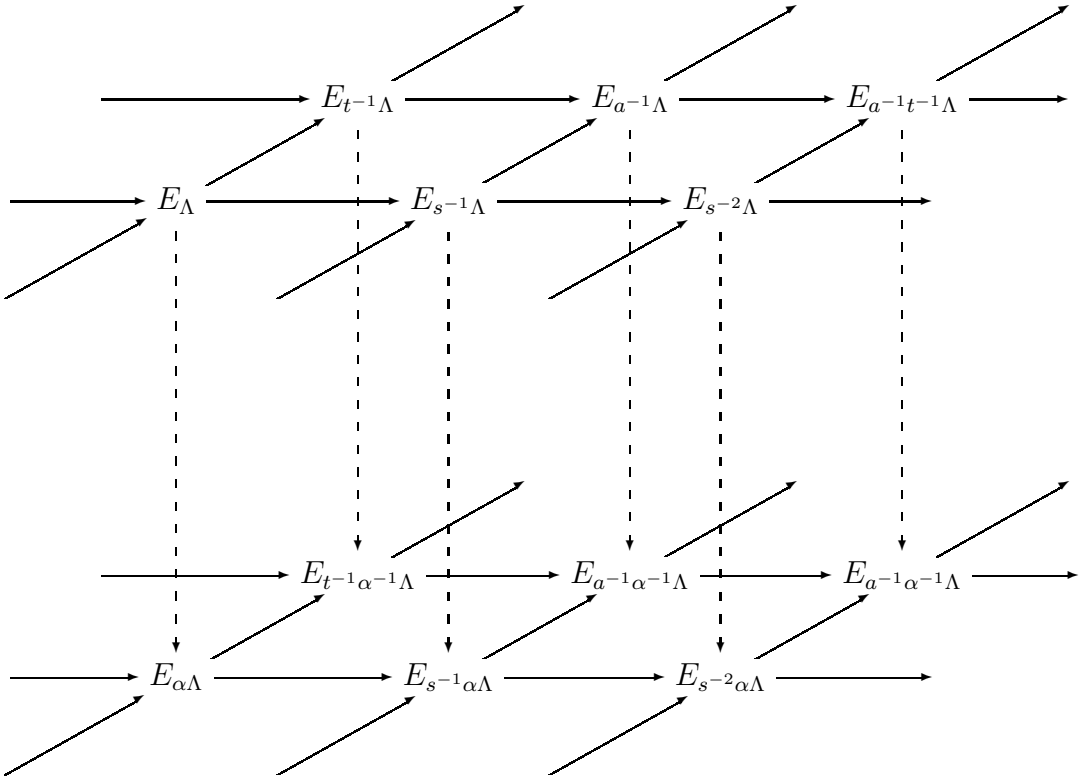
For an arbitrary idele $s$ and order $\mathcal{O}$, the lattice $s\mathcal{O}\mathfrak{b}$ is a fractional ideal of $\mathcal{O}$, which we may write as $n^{-1}\mathfrak{b}$ for some integer $n$ and integral ideal $\mathfrak{b}$. We have canonical isogenies

$$\mathbb{C}/\Lambda \xrightarrow{\quad\varphi\quad} \mathbb{C}/\mathfrak{b}^{-1}\Lambda \xleftarrow{\quad\psi\quad} \mathbb{C}/n\mathfrak{b}^{-1}\Lambda,$$

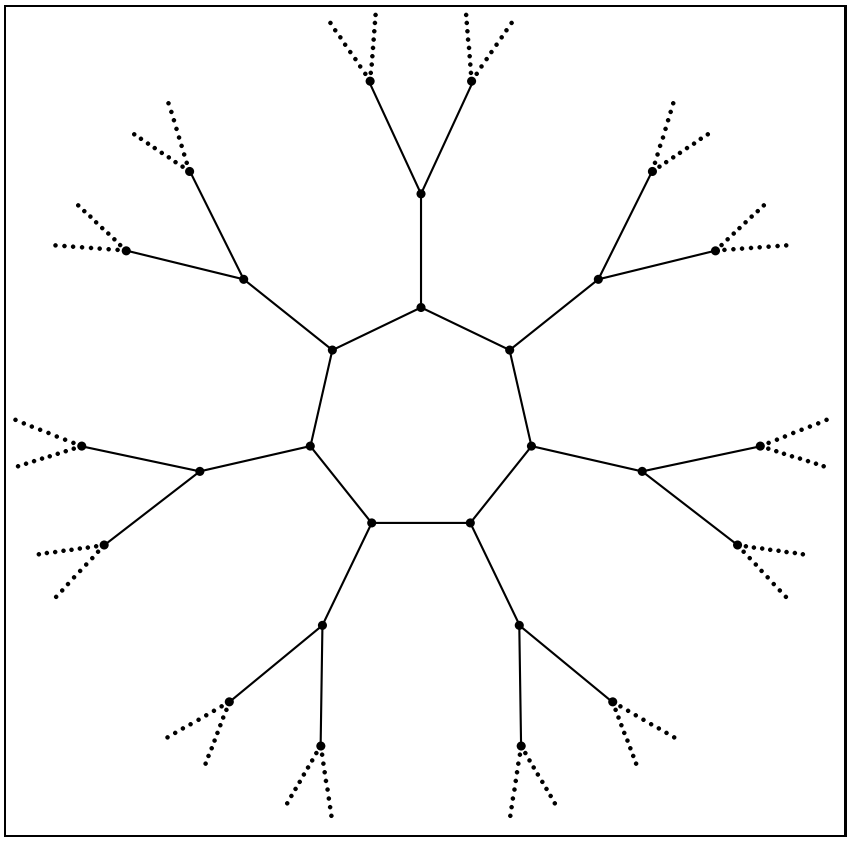
which serve to define an elliptic curve $E' = s\cdot E$. Namely, write $s\mathcal{O} = n^{-1}\mathfrak{a}$, and set $G = E[\mathfrak{a}]$. Given any Weierstrass equation for $E$, in § 2.4 we described an explicit Weierstrass equation for $E_G$. And in the end of that section, we give the equation of the curve $E'$ mapping to $E_G = E'_{E[n]}$. This serves to define $s\cdot E = E'$.

This gives an action on the set of Weierstrass equations of elliptic curves over a finite field. The above construction is valid for all ideles which are trivial at the prime of reduction. In an ad hoc fashion we can extend the action to all ideles by letting the prime of reduction act by the Frobenius isogeny. Note that only the decomposition group of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ at a place $\mathfrak{p}$ acts on the reduced curve at $\mathfrak{p}$, and that the image curve of the Frobenius automorphism is defined to be the same as for the Frobenius isogeny.

**Example** Suppose $s \in J_K$ and $s\Lambda \subseteq \Lambda$, so that $s\mathcal{O} = \mathfrak{a}$ is an integral ideal. Let $t = \overline{s}$ and $a = st = \mathrm{N}(\mathfrak{a}) \in \mathbb{Z}$. Let $\alpha$ be a generator for $\mathfrak{a}^h$, where $h$ is the order of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$. Consider the following diagram, where the solid arrows are the canonical quotient isogenies, shown for those isogenies induced by $s$ and $t$. The dotted lines down indicate the isomorphisms obtained by multiplication by $\alpha$ on lattices.




If we quotient out by isomorphisms, $J_K$ acts on the finitely many isomorphism classes in particular, on their $j$-invariants. Below we represent isomorphism classes for those elliptic curves (equivalently lattices) with endomorphism rings equal to orders $\mathcal{O}_K \supseteq \mathcal{O}_1 \supseteq \mathcal{O}_2 \supseteq \cdots$ where each $\mathcal{O}_i$ has index $2^i$ in the maximal order $\mathcal{O}_K$ of discriminant $-71$. A vertex of the graph represents an isomorphism class of elliptic curve, a line between them represents the existence an isogeny of degree two between members of the classes.



Graph of isogenies of degree two.

Through the arithmetic action of $J_K$ on $\mathcal{E}(K)$ of the previous section, only a subgroup of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ – the decomposition group of a prime $\mathfrak{p}$ – acts on the set of reduced curves at $\mathfrak{p}$. In contrast, reduction of elliptic curves is injective on the set of isogenies so the full idele group acts on the image of the reduction map via these fractional isogenies. Thus there exist fractional isogenies of elliptic curves giving an automorphism of the above diagram in any characteristic.

# Chapter 4

# The ordinary case

Throughout this section $E$ will denote an ordinary elliptic curve over a finite field $k$ of $q$ elements and characteristic $p$. Let $\pi$ be the Frobenius endomorphism relative to $k$. Recall that $E$ is ordinary if it satisfies any of the following equivalent conditions.

1. $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all positive integers $r$.
2. $\mathrm{End}(E)$ is an order in a complex imaginary extension of $\mathbb{Q}$.
3. The dual of the Frobenius endomorphism is separable.
4. The trace of the Frobenius endomorphism is relatively prime to $q$.

For an ordinary elliptic curve $E$ over a field $k$, the full endomorphism ring $\mathrm{End}(E)$, which we denote by $\mathcal{O}$, is equal to $\mathrm{End}_k(E)$. For a rational integer $l$ we denote $\mathbb{Z}[\pi] \otimes \mathbb{Z}_l$ by $\mathbb{Z}[\pi]_l$ and $\mathcal{O} \otimes \mathbb{Z}_l$ by $\mathcal{O}_l$.

The objective of this chapter is to describe methods by which to determine the isomorphism type of the endomorphism ring $\mathcal{O}$, which we refer to as the endomorphism type of $E$. We refer to the subset of curves in the isogeny class of $E$ with endomorphism type $\mathcal{O}$ as the endomorphism class of $E$. The algorithm of Schoof [27] is a polynomial time algorithm for determining the trace $t$ of Frobenius relative to $k$ on $E$, so we may assume that we know the subring $\mathbb{Z}[\pi]$ of $\mathcal{O} = \mathrm{End}(E)$. The methods described here will comprise elements of an algorithm for computing the endomorphism type of a given ordinary elliptic curve $E$. We synthesize the various components into an algorithm in the last section. We may let $\mathcal{O}_K$ be the maximal order in the formal field of fractions $K = \mathbb{Z}[\pi] \otimes \mathbb{Q}$ of discriminant $D_K$, and let $m$ be the conductor of $\mathbb{Z}[\pi]$. Then there exists an integer $a$ such that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - a}{m}\right].$$

The integer $a$ has the property that that $(X-a)^2 = X^2 - tX + q \bmod m$, and is determined by the conditions that $2a \equiv t \bmod m$ and $q - ta + a^2 \equiv 0 \bmod m^2$.

In particular, the integers $a = (t + m)/2$ and $a = t/2$ satisfy these conditions if $D_K \equiv 1 \bmod 4$, and $D_K \equiv 0 \bmod 4$, respectively.

Let $\kappa/k$ be a finite extension of degree $r$. For integers $a_r$ and $m_r$ we write

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi^r - a_r}{m_r}\right],$$

and let $t_r$ be the trace of the Frobenius endomorphism $\pi^r$ relative to $\kappa$. Recall the result of Lenstra [18] that

$$E(\kappa) \cong \frac{\mathcal{O}}{(\pi^r - 1)},$$

as a module over $\mathcal{O}$. It follows that the group structure of $E(\kappa)$ is $\mathbb{Z}/l_r\mathbb{Z} \times \mathbb{Z}/n_r\mathbb{Z}$, for $l_r | n_r$ and $l_r n_r = q^r - t_r + 1$, and where $l_r$ is the largest integer dividing $\gcd(a_r - 1, m_r)$.

Notice that the integers $t_r$ and $m_r$ are completely determined by the trace of $\pi$. They are respectively

$$\begin{aligned} t_r &= \sum_{i=0}^{[r/2]} (-1)^i b_i(r) t^{r-2i} q^i = \sum_{i=0}^{[r/2]} (-1)^i \binom{r-i-1}{i} t^{r-2i} q^i, \quad \text{and} \\ m_r &= m \sum_{i=0}^{[r/2]} (-1)^i c_i(r) t^{r-2i-1} q^i = m \sum_{i=0}^{[r/2]} (-1)^i \frac{r}{r-i} \binom{r-i}{i} t^{r-2i-1} q^i, \end{aligned}$$

where the coefficients $b_i(r)$ and $c_i(r)$ are determined by the recursions

$$b_i(r) = b_i(r-1) + b_{i-1}(r-2) \quad \text{and} \quad c_i(r) = c_i(r-1) + c_{i-1}(r-2).$$

subject to the boundary conditions $b_0(r) = 1$, $b_i(2i) = 2$, $c_0(r) = 1$, and $c_i(2i) = 0$.

To emphasize that the group structure of $E(k)$ alone is not the appropriate $k$-isomorphism invariant to be studied, consider the following example. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^2 - \alpha + 5 = 0$ and let $\mathcal{O}_K$ be the maximal order in $K$. Let $\pi = 9 + 5\alpha$, a prime element of norm 251. Then both $\mathcal{O}_K/(\pi - 1)$ and $\mathbb{Z}[\pi]/(\pi - 1)$ are isomorphic to $\mathbb{Z}/229\mathbb{Z}$ as groups, or as modules over $\mathbb{Z}[\pi]$. But the group structure fails to capture the fact that

$$\frac{\mathcal{O}_K}{(\pi^2 - 1)} \cong \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{12595\mathbb{Z}} \quad \text{and} \quad \frac{\mathbb{Z}[\pi]}{(\pi^2 - 1)} \cong \frac{\mathbb{Z}}{62975\mathbb{Z}}.$$

So the group structure of $E(k)$ is a weaker invariant of study. As a point of record, it should be pointed out that neither determination of the endomorphism type nor of generators for $\mathcal{O}$ produces generators for the group and except in incidental cases, actual generators for the endomorphism ring are not determined in this document.

The goal of the algorithm is to determine for each prime divisor $l$ of the conductor of $\mathbb{Z}[\pi]$, the largest power which divides $\pi - a$ in $\mathrm{End}(E)$. The isogeny class of $E$ contains

$h(\mathcal{O})$ curves with endomorphism ring $\mathcal{O}$ for each of the orders $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. From the exact sequence of class groups

$$1 \longrightarrow \frac{(\mathcal{O}_K/m\mathcal{O}_K)^*}{\overline{\mathcal{O}_K^*}(\mathbb{Z}/m\mathbb{Z})^*} \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \tag{4.1}$$

derived in the Chapter 3, we can express the class number of $\mathcal{O}$ as

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]}\, m \prod_{\substack{l|m \\ prime}} \left(1 - \left(\frac{D_K}{l}\right) l^{-1}\right). \tag{4.2}$$

In particular at each prime $l|m$ the probability that $\mathcal{O} \otimes \mathbb{Z}_l$ is equal to $\mathbb{Z}[\pi] \otimes \mathbb{Z}_l$ is at least $(l-1)/3$ times as great as $\mathcal{O} \otimes \mathbb{Z}_l$ being larger. Thus one expects the endomorphism ring of $E$ to contain $\mathbb{Z}[\pi]$ with small index.

Moreover, if one assumes that the discriminants $t^2 - 4q$ of the rings $\mathbb{Z}[\pi]$ generated by the Frobenius endomorphism are in some sense random, the typical ring $\mathbb{Z}[\pi]$ is expected to have discriminant equal to a small square multiple of the fundamental discriminant of the field $K$, and $\mathbb{Z}[\pi]$ itself has small index in the maximal order. A general algorithm for computing the isormorphism type of $\mathrm{End}(E)$ must treat the exceptional cases in which the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ is large and possibly divisible by a large prime. However, methods will be described which are not applicable in such exceptional cases, but reflect the needs of treating typical curves.

Throughout this chapter we will refer to the following examples of elliptic curves.

**Example 1.**

Let $E/\mathbb{F}_p$ be the elliptic curve given by Weierstrass equation

$$Y^2 = X^3 - \frac{j_E}{48(j_E - 12^3)}X - \frac{j_E}{864(j_E - 12^3)}$$

with $j$-value $j_E = 889825141831795296744553987 0 \bmod p$ over the field of $p$ elements, where $p$ is the prime

$$1774720755003177239886849307 3.$$

The trace $t$ of Frobenius is equal to 81759951888758, so that

$$\mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4p = -2^5 \cdot 3^2 \cdot 41 \cdot 97 \cdot 16366333369 \cdot 3430358152087.$$

The index of $\mathbb{Z}[\pi]$ in the maximal order of $K = \mathbb{Z}[\pi] \otimes \mathbb{Q}$ is 6.

**Example 2.**

Let $\mathbb{F}_p$ be the same field as in Example 1, and let $E/\mathbb{F}_p$ be the elliptic curve given by Weierstrass equation

$$Y^2 = X^3 - \frac{j_E}{48(j_E - 12^3)}X - \frac{j_E}{864(j_E - 12^3)}$$

with $j$-value $j_E = 172312560560722443619199908 86 \bmod p$.
The Frobenius endomorphism $\pi$ has trace $t$ equal to 145933714622674, hence

$$\mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4p = -2^{22} \cdot 3^3 \cdot 7^{12} \cdot 547^2 \cdot 105953.$$

The index of $\mathbb{Z}[\pi]$ in the maximal order of $K = \mathbb{Z}[\pi] \otimes \mathbb{Q}$ is $2^{11} \cdot 3 \cdot 7^6 \cdot 547$.

**Example 3.**

Let $E/\mathbb{F}_q$ be the elliptic curve of Atkin (see Schoof [28]) having Weierstrass equation

$$Y^2 = X^3 - 105X - 78153$$

over the field of $q$ elements, where $q$ is the 200 digit prime

$$\begin{gathered}
10000000000000000000000000000000000000000000000000 \\
00000000000000000000000000000000000000000000000000 \\
00000000000000000000000000000000000000000000000000 \\
00000000000000000000000000000000000000000000000153.
\end{gathered}$$

Atkin determined the trace $t$ of the Frobenius endomorphism to be

$$\begin{gathered}
-67897502880042241180803143654602776419280496418 88 \\
39991591392960032210630561760029050858613689631599.
\end{gathered}$$

Thus the discriminant of $\mathbb{Z}[\pi]$ is equal to

$$t^2 - 4p = -3 \cdot 4621 \cdot 5783 \cdot 15667 \cdot 23251 \cdot 2580042061 \cdot n_1,$$

where $n_1$ is a composite integer of 174 decimal digits. Provided $n_1$ is square free, then $\mathbb{Z}[\pi]$ is the maximal order, hence also the full endomorphism ring of $E$.

Example 3 demonstrates that while one can expect a random elliptic curve to have endomorphism ring containing $\mathbb{Z}[\pi]$ with small index, even if $\mathbb{Z}[\pi]$ is maximal, this fact can not be recognized in polynomial time.

## 4.1 Explicit kernels

Let $E/k$ be an elliptic curve defined by a Weierstrass equation $F_E(x, y) = 0$. As in the previous section we denote the conductor of $\mathbb{Z}[\pi]$ by $m$ and let $a$ be an integer such that $\pi - a \equiv 0 \bmod m\mathcal{O}_K$. We observe that since $E$ is ordinary, the trace of Frobenius is relatively prime to $q$, thus $m$ is relatively prime to $q$ and $\pi$ determines a linear automorphism

$$\pi : \mathcal{O}/m\mathcal{O} \to \mathcal{O}/m\mathcal{O},$$

and the integer $a$ is is the double eigenvalue modulo $m$ of $\pi$. The objective is to find the largest $n$ for which $\pi - a$ is the zero map on $\mathcal{O}/n\mathcal{O}$. The most direct way to determine if a divisor $n$ of $m$ divides $\pi - a$ in $\mathcal{O}$ is by comparing the homomorphisms induced by $\pi$ and $[a]$ on the ring

$$\frac{k[X,Y]}{(F_E(X,Y), \psi_n(X,Y))},$$

where $\psi_n(X,Y)$ is the division polynomial for $n$. The endomorphism $\pi - a$ is equal to $n\alpha$ for some $\alpha$ in $\mathrm{End}(E)$ if and only if the kernel of $\pi - a$ contains $E[n]$. Let $\mathbb{P}^1 = E/\{[\pm 1]\}$, let $\pi_{\mathbb{P}^1}$ and $[a]_{\mathbb{P}^1}$ be the maps induced on $\mathbb{P}^1$ by $\pi$ and $[a]$, and let $\psi_n(X)$ be a generator for $(\psi_n(X,Y)) \cap k[X]$. Since

$$[a]_{\mathbb{P}^1}(X) = \frac{\phi_a(X)}{\psi_a(X,Y)^2} \in k(X), \text{ and } \pi_{\mathbb{P}^1}(X) = X^q,$$

one computes $X^q \psi_a(X,Y)^2 - \phi_a(X) \bmod \psi_n(X)$, which equals zero if and only if $n$ divides $\pi - a$ in $\mathcal{O}$. Note that we can take for $a$ any of its coset representatives modulo $n$, and all calculations are carried out modulo the polynomial $\psi_n$ of degree $\mathrm{O}(n^2)$. By taking $n = l, l^2, \ldots$ up to the highest power of a prime $l$ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$, we find the exponent of $l$ in the index $[\mathcal{O} : \mathbb{Z}[\pi]]$.

**Example 4.** We now return to our examples for this chapter.

In Example 1, we observe that the largest prime powers dividing the $m$ are 2 and 3. We find that 1 is a coset representative for $a \bmod 6$, so $\pi$ acts as the identity on $E[n]$ for $n|6$ if and only if $\pi - 1$ is divisible by $n$ in $\mathcal{O}$. One finds that the 2-torsion group is contained in $E(k)$, but that the 3-torsion group is not. Thus $\mathbb{Z}[\pi]$ is contained in $\mathrm{End}(E)$ with index 2.

In Example 2, we would need to consider the action of $\pi$ on the torsion groups

$$E[2], E[2^2], \ldots, E[2^{11}], \text{ on } E[3], \text{ on } E[7], E[7^2], \ldots, E[7^6], \text{ and on } E[547].$$

As we have noted, it is likely that the endomorphism ring contains $\mathbb{Z}[\pi]$ with small index, and thus we are likely to find that $E[l^r] \not\subseteq \ker(\pi - a)$ well before treating the largest power of $l$ dividing the conductor of $\mathbb{Z}[\pi]$. However, *a priori* we may have to calculate the action of Frobenius on the subgroup of order $7^6 = 117649$. In the following section we describe a practical method for determining the index of $\mathbb{Z}[\pi]_l$ in $\mathcal{O}_l$ when a large power of $l$ divides the conductor.

## 4.2 Probing the depths

The direct approach described above makes use of the decomposition of the conductor of $\mathbb{Z}[\pi]$ into prime powers $n = l^r$. However, it fails to further exploit the decomposition

of $n$, if we find that a large power of $l$ divides $[\mathcal{O} : \mathbb{Z}[\pi]]$. Here we describe how to construct isogenies, using a factoring algorithm in $k[X]$, in order to *probe the depths* at which $E$ lies relative to $l$.

First we make explicit the terminology which we use in this section. If $\mathcal{O}$ is maximal at $l$, we say that $E$ lies at the surface relative to $l$, where we may drop the qualification relative to $l$ if the prime $l$ is understood. If the index $[\mathcal{O}_K : \mathcal{O}]$ is divisible by $l^r$ but not $l^{r+1}$, we say that $E$ lies at depth or level $r$. If $\mathcal{O}_l = \mathbb{Z}[\pi]_l$, we say that $E$ lies at the floor of rationality.

Let $\varphi : E \to E'$ be an isogeny of degree $n$. We define $K = \mathrm{End}(E) \otimes \mathbb{Q}$. Then $\varphi$ determines a homomorphism

$$\iota : \mathcal{O}' \to K$$

sending $\psi$ to $\varphi^{-1}\psi\varphi = \widehat{\varphi}\psi\varphi \otimes n^{-1}$. Given any other isogeny $\eta : E \to E'$ with $\deg(\eta) = k$, the induced homomorphism $\mathcal{O}' \to K$ gives the same embedding:

$$\begin{aligned} \widehat{\eta}\psi\eta \otimes k^{-1} &= \widehat{\eta}(\varphi\widehat{\varphi})\psi(\varphi\widehat{\varphi})\eta \otimes k^{-1}n^{-2} \\ &= (\widehat{\eta}\varphi)\widehat{\varphi}\psi\varphi(\widehat{\varphi}\eta) \otimes k^{-1}n^{-2} \\ &= \widehat{\varphi}\psi\varphi(\widehat{\eta}\varphi)(\widehat{\varphi}\eta) \otimes k^{-1}n^{-2} \\ &= \widehat{\varphi}\psi\varphi \otimes n^{-1}, \end{aligned}$$

where the next to last step relies on the commutativity of $\mathcal{O}'$. In general, as we will see with supersingular elliptic curves, the induced embedding of $\mathrm{End}(E')$ in a ring $\mathrm{End}(E)\otimes\mathbb{Q}$ depends on the isogeny $\varphi$. For ordinary elliptic curves, we view all elliptic curves in an isogeny class as embedded in a field $K$ isomorphic to $\mathcal{O} \otimes \mathbb{Q}$, where $\mathcal{O}$ is any endomorphism ring of a curve in the isogeny class.

**Proposition 21** *Let $E/k$ be an ordinary elliptic curve over the finite field $k$. Let $\varphi : E \to E'$ be an isogeny of prime degree $l$ different from the characteristic of $k$. Then $\mathcal{O}$ contains $\mathcal{O}' = \mathrm{End}(E')$ or $\mathcal{O}'$ contains $\mathcal{O}$ in $K$ and the index of one in the other divides $l$.*

**Proof.** The proposition follows from the observation that

$$\mathbb{Z} + l^2\mathcal{O} \subseteq \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq \mathcal{O},$$

where $\mathbb{Z} + l^2\mathcal{O}$ has index $l^2$ in $\mathcal{O}$. If equality holds nowhere this translates into the equality of $\mathcal{O}$ and $\mathcal{O}'$ in $K$. If $\mathbb{Z} + l^2\mathcal{O} = \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi$ then $\mathcal{O}'$ has index $l$ in $\mathcal{O}$ and if $\mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi = \mathcal{O}$ then $\mathcal{O}$ is contained in $\mathcal{O}'$ with index $l$.

**Proposition 22** *Let $\varphi : E \to E'$ be an isogeny of ordinary elliptic curves over $k$ and let $\mathcal{O} = \mathrm{End}(E)$ and $\mathcal{O}' = \mathrm{End}(E')$. Then the following conditions are equivalent.*

1. *The orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic.*

2. *The left ideal* $I(\ker(\varphi)) = \{\psi \in \mathcal{O} : \psi(\ker(\varphi)) = \mathbf{O}\}$ *is a projective ideal of norm equal to* $\deg(\varphi)$.

3. *There exists an isogeny* $\psi : E \to E'$ *of degree relatively prime to* $\deg(\varphi)$.

**Proof.** We could deduce this result from the results of Chapter 3 and the Deuring lifting theorem. Instead we take the approach of Tate. Let $\phi$ be the Frobenius automorphism of $\overline{k}/k$. Then Tate [31] has shown that for every prime $l$ different from the characteristic $p$ of $k$, that

$$\mathrm{Hom}(E', E) \otimes \mathbb{Z}_l \cong \mathrm{Hom}_{\mathbb{Z}[\phi]}(T_l(E'), T_l(E)),$$

where $T_l(E)$ and $T_l(E')$ are the Tate modules at $l$. Both sides have the structure of left $\mathcal{O}_l$-modules, and $\mathbb{Z}_l[\phi]$ and $\mathbb{Z}_l[\pi]$ have the same representations on the Tate modules. Moreover $\mathbb{Q}_l[\pi] = \mathcal{O} \otimes \mathbb{Q}_l$. Since $\mathrm{End}_{\mathbb{Z}_l[\phi]}(T_l(E)) \cong \mathcal{O}_l$ and $\mathrm{End}_{\mathbb{Z}_l[\phi]}(T_l(E')) \cong \mathcal{O}'_l$, the Tate modules $T_l(E)$ and $T_l(E')$ are isomorphic as $\mathbb{Z}_l[\phi]$-modules if and only if $\mathcal{O}_l \cong \mathcal{O}'_l$. This is equivalent to $\mathrm{Hom}(E', E) \otimes \mathbb{Z}_l$ being a free $\mathcal{O}_l$-module. If these conditions hold for all $l \neq p$, since $\mathcal{O}_p$ is maximal at $p$, this is equivalent to $\mathrm{Hom}(E', E)$ being projective as a left $\mathcal{O}$-module. Observing that $I(\ker(\varphi)) = \mathrm{Hom}(E', E)\varphi$, this proves the equivalence of the first two conditions. The degree map on isogenies of $\mathcal{O}$ equals the norm map on the ring $\mathcal{O}$. If the ideal $I(\ker(\varphi)) = \mathrm{Hom}(E', E)\varphi$ has norm $\deg(\varphi)$ then it follows that there exists an isogeny of degree relatively prime to $\deg(\varphi)$. By decomposing an isogeny into isogenies of prime degrees, from condition 3 we deduce that the orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic by the previous proposition.

The ideal $I(\ker(\varphi))$ is called the *kernel ideal* for $\varphi$.

**Proposition 23** *Let* $E/k$ *be an ordinary elliptic curve with endomorphism ring* $\mathcal{O}$ *of discriminant* $D$*, let* $l$ *be a prime, and let* $\left(\frac{D}{l}\right)$ *be the Legendre symbol.*

1. *If* $\mathcal{O}_l$ *is maximal then there are* $\left(\frac{D}{l}\right) + 1$ *isogenies of degree* $l$ *to curves with endomorphism ring isomorphic to* $\mathcal{O}$.

2. *If* $\mathcal{O}_l$ *is nonmaximal, then there are no isogenies of degree* $l$ *to curves with endomorphism ring* $\mathcal{O}$.

3. *If there exist more than* $\left(\frac{D}{l}\right) + 1$ *isogenies of degree* $l$*, up to isomorphism, then all isogenies of degree* $l$ *are defined over* $k$*, and up to isomorphism of the pairs* $(E, E')$ *there are exactly*

$$\left(l - \left(\frac{D}{l}\right)\right)[\mathcal{O}^* : \mathcal{O}'^*]^{-1}$$

*elliptic curves* $E'$ *and isogenies* $E \to E'$ *of degree* $l$ *such that the endomorphism ring* $\mathcal{O}'$ *of* $E'$ *is properly contained in* $\mathcal{O}$.

**Proof.** Statements 1 and 2 follow by counting the number of projective ideals of norm $l$. The final statement follows by enumeration of the remaining elliptic curves, up to isomorphism, and applying the class number relations of equation (4.2). The factor $[\mathcal{O}^* : \mathcal{O}'^*]$ is the size of the orbits of the action of automorphisms of $E$ on the set of cyclic subgroups of $E[l]$.

Let $E/k$ be an ordinary elliptic curve over the finite field $k$. We use this proposition as follows.

If $E$ lies at the floor of rationality, we can recognize this fact easily as follows. Since $\mathbb{Z}_l[\pi] = \mathcal{O}_l$, there are no elliptic curves in the isogeny class of $E$ at depth greater than $E$ at $l$. By proposition 23, of the $l+1$ isogenies of degree $l$ over $\overline{k}$, exactly $\left(\frac{D}{l}\right)+1$ are defined over $k$. If $l$ divides the index $m$ of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$ then by assumption $E$ is not at the surface and this number is 1. The remaining $l$ curves which are $l$-isogenous to $E$ over $\overline{k}$ are not defined over $k$. Thus we would like to use $l$-isogenies to probe the depths for the floor of rationality, as we describe below.

Suppose that $l$ is a prime dividing the conductor of $\mathbb{Z}[\pi]$, and $E$ does not lie at the floor of rationality. We construct an isogeny $\varphi : E \to E'$ of degree $l$. At the surface, the number of isogenies to curves at greater depth is at least $\max((l-1)/3, 1)$, and at greater depth $l$ of the $l+1$ isogenies lead down. If we choose an isogeny such that $E'$ lies at a greater depth than $E$, then all isogenies except the dual to $\varphi$ continue our descent. Thus we construct $l$-isogenies until we reach a curve at the floor of rationality. Counting the number of levels down to a curve at the floor of rationality gives the exponent of $l$ in the index $n = [\mathcal{O} : \mathbb{Z}[\pi]]$.

In the unfortunate event that our initial choice of $l$-isogeny did not begin this descent, we overestimate the index $n$. For that reason we perform a second probe. By the proposition, if $E$ does not lie at the surface, one $l$-isogeny leads up and $l$ isogenies of degree $l$ lead down to greater depth. If we begin our second probe along a different $l$-isogeny, one path is certain to lead down, and we conclude that the exponent of $l$ in $n$ is the minimum of the lengths of the two probes.

Finally, if we begin at the surface with respect to $l$, there are $\left(\frac{D}{l}\right)+1$ isogenies of degree $l$ to curves having the same endomorphism type. If $l$ splits in $\mathcal{O}$, we may have the misfortune of floating indefinitely along the surface before beginning our descent. However, we know that the maximum exponent of $l$ to be that in the conductor of $\mathbb{Z}[\pi]$. If the length of both probes exceeds this bound, then we conclude that $E$ lies at the surface.

In practice this method is good for small primes for which we have a good model of $X_0(l)$. The $j$-value of the isogenous curve $E'$ is sufficient to determine whether $E'$ is defined over $k$.

We can now treat our examples.

**Example 5.** Let $E/\mathbb{F}_p$ be the elliptic curve

$$Y^2 = X^3 - \frac{j_E}{48(j_E - 12^3)}X - \frac{j_E}{864(j_E - 12^3)}$$

of Example 2 over the field of

$$177472075500317723988684930 73$$

elements and $j$-invariant $j_E = j_0 = 172312560560722443619199908 86 \bmod p$. The discriminant of $\mathbb{Z}[\pi]$ can be verified to be

$$\mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4p = -2^{22} \cdot 3^2 \cdot 7^{12} \cdot 547^2 \cdot 105953.$$

Hence $\mathbb{Z}[\pi]$ is nonmaximal at the primes $2, 3, 7$, and $547$, and a curve at the floor of rationality lies at depth $11, 1, 6$, and $1$ respectively with respect to $2, 3, 7$, and $547$.

By means of explicitly constructed sequences of isogenous curves, we can prove that the index $[\mathcal{O}_l : \mathbb{Z}[\pi]_l]$ is $2^2$ at $l = 2$, is $1$ at $l = 3$, and is $7$ at $l = 7$.

**Index at 2.** Let $\Phi_2(X, Y)$ be the modular equation of level 2. Let $E = E_0$ and let $j_0$ be the $j$-invariant of the elliptic curve $E$. We can construct a sequence of $j$-invariants $j_i$ of elliptic curves $E_i$ by successively solving for a root $j_{i+1}$ of $\Phi_2(X, j_i)$, where $j_{i+1} \neq j_{i-1}$. Then each $j_i$ is the $j$-invariant of a curve $E_i$ such that there exists an 2-isogeny $\varphi_i : E_{i-1} \to E_i$ over $k$. The first such sequence of curves, with $j$-values given below, terminates after four isogenies in a curve at the floor of rationality.

$$\begin{aligned}
j_0 &= 172312560560722443619199908 86 \bmod p,\\
j_1 &= 116783496993645786327741928 46 \bmod p,\\
j_2 &= 174908099099881991696854280 \bmod p,\\
j_3 &= 174167927365859179881009527 3 \bmod p,\\
j_4 &= 859284985375096729566308140 \bmod p.
\end{aligned}$$

A second sequence of isogenies of degree two, represented by $j$-values below, terminates after just two isogenies in a curve at the floor of rationality.

$$\begin{aligned}
j_0 &= 172312560560722443619199908 86 \bmod p,\\
j_1' &= 107085662263845853030859187 97 \bmod p,\\
j_2' &= 104684922354215671407893729 59 \bmod p.
\end{aligned}$$

In the first sequence, then, the first choice of isogeny above was to the unique curve having endomorphism ring which contains $\mathcal{O}$ with index 2. Since the shortest sequence of isogenies to the floor of rationality is of length 2, the index of $\mathbb{Z}[\pi]_2$ in $\mathrm{End}(E)_2$ is $2^2$.

**Index at 3.** Let $\Phi_3(X, Y)$ be the modular equation of level 3. Then $\Phi_3(X, j_E)$ has exactly one root, hence $E$ lies at the floor of rationality with respect to 3. Thus the index of $\mathbb{Z}[\pi]_3$ in $\mathrm{End}(E)_3$ is 1.

**Index at 7.** Let $\Phi_7(X, Y)$ be the modular equation of level 7. Then $\Phi_7(X, j_E)$ splits completely, so $E$ does not lie at the floor of rationality, but $E$ is 7-isogenous to a curve with $j$-value $676210665078371289572567543 1 \bmod p$ which does lie at the floor of rationality, as do 5 of the other 6 curves 7-isogenous to $E$.

In order to determine the index of $\mathbb{Z}[\pi]_l$ in $\mathrm{End}(E)_l$ at $l = 547$, we could look at the splitting of the division polynomial $\psi_{547}$ of degree $(547^2 - 1)/2 = 149604$, or contruct equations for the modular curve $X_0(547)$ and determine the number of $\mathbb{F}_p$-rational points lying over $j_E$ under the map $X_0(547)/\mathbb{F}_p \to X_0(1)/\mathbb{F}_p$. However, in the next section we will describe another method by which we can treat such large factors.

## 4.3 Isolated endomorphism classes

In this section we describe how to make use of the existence of large prime divisors of the conductor of $\mathbb{Z}[\pi]$. The techniques described here will be the only methods by which we may construct endomorphisms of $E$ not lying in $\mathbb{Z}[\pi]$. This will not be the motivating goal however, and we will incidentally produce such endomorphims only when the endomorphism ring is unexpectedly large. If one takes a constructive approach to the problem the methods outlined here can be applied to build generators for $\mathcal{O}$, but the computational complexity is significantly worse than that obtainable for the determination of the endomorphism type of $E$.

By decomposition into prime degree isogenies, and application of proposition 21, we see that an isogeny between elliptic curves of endomorphism types $\mathcal{O}_1$ and $\mathcal{O}_2$ must have degree divisible by the integer

$$[\mathcal{O}_1\mathcal{O}_2 : \mathcal{O}_1] \cdot [\mathcal{O}_1\mathcal{O}_2 : \mathcal{O}_2] = [\mathcal{O}_1 : \mathcal{O}_1 \cap \mathcal{O}_2] \cdot [\mathcal{O}_2 : \mathcal{O}_1 \cap \mathcal{O}_2].$$

Moreover, every elliptic curve in the isogeny class of $E$ over $k$ has endomorphism ring containing $\mathbb{Z}[\pi]$. Thus for any isogeny $\varphi : E \to E'$ of degree relatively prime to the conductor of $\mathbb{Z}[\pi]$, the image curve $E'$ also has endomorphism type $\mathcal{O}$. By proposition 22 the kernel ideal for $\varphi$ is projective, and $\varphi$ is principal if and only if $E'$ is isomorphic to $E$. This gives us the bijection of the endomorphism class of $E$, up to isomorphism, with the class group of $\mathcal{O}$ as described in section 3.4 of Chapter 3.

This suggests two approaches which we might exploit for the determination of the endomorphism type of $E$. The first is to enumerate all of the $h(\mathcal{O})$ elliptic curves in the endomorphism class of $E$. This involves choosing a set of small prime generators for the class group and using these to construct the corresponding endomorphisms of elliptic curves. The second involves computation of principal ideals of smooth norm

in a possible endomorphism ring $\mathcal{O}$, and then determining the corresponding isogeny to determine whether the image curve is isomorphic to $E$.

First we explore the possibilities of the enumeration approach. The class number of $\mathbb{Z}[\pi]$ and the orders containing it can be exceedingly large. The discriminant of $\mathcal{O}$ divides $D = t^2 - 4q$, and the class number has bound $O(\sqrt{|D|}\log(|D|))$. By the Brauer-Siegel Theorem [4, Theorem 4.9.15], the growth of $\log(\mathcal{O}_K)$ is asymptotically $\log(|D_K|^{1/2})$, but the result is noneffective, and few absolute bounds on $h(\mathcal{O}_K)$ from below are known.

However, if the conductor of $\mathbb{Z}[\pi]$ is divisible by a large prime $l$, then the orders containing

$$\mathcal{O}_1 = \mathbb{Z}\left[\frac{\pi - a}{l}\right]$$

have discriminants dividing $(t^2 - 4q)/l^2$ and class numbers of these orders divide the class number $h(\mathcal{O}_1)$. Thus if we can enumerate the elliptic curves, up to isomorphism, in the endomorphism class of $E$ until we exceed $h(\mathcal{O}_1)$, we can conclude that $E$ lies at the floor of rationality with respect to $l$.

Such a calculation presupposes that we have determined $h(\mathcal{O}_1)$ and that we have small splitting primes in $\mathcal{O}_1$ from which we can feasibly construct sequences of isogenies of small degree to all members of the endomorphism class. In the last section we will deal with the existence questions and the bounds necessary to derive complexity bounds on this method.

In order to enumerate the curves in the endomophism class of $E$, up to isomorphism, we blindly explore the bounds of the class until we have determined the size of the world to which $E$ is confined. This fails to exploit the considerable knowledge we have of the ideal group acting on the endomorphism class of $E$. Instead we can build on the algorithms for ideal class groups to find class group relations among small splitting primes $\mathfrak{r}_1, \ldots, \mathfrak{r}_c$ in the order $\mathcal{O}_1$. In doing so we obtain a principal ideal $(\beta) = \mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c} \subseteq \mathcal{O}_1$, with exponent sum $u = s_1 + \cdots + s_c$ and let $\mathfrak{b} = \beta\mathcal{O} \cap \mathcal{O}$. By constructing the sequence of isogenies:

$$E_0 = E \to E_1 = E/E[\mathfrak{r}_1] \to E_2 = E/E[\mathfrak{r}_1^2] \to \cdots \to E_u = E/E[\mathfrak{b}],$$

each of small degree, we obtain a curve $E_u = E/E[\mathfrak{b}]$ which is isomorphic to $E$ if and only if $\mathfrak{b}$ is principal. Typically we find $\beta$ in a ring $\mathcal{O}_1$ containing $\mathbb{Z}[\pi]$ with large index, and we expect $\mathfrak{b}$ to be nonprincipal in $\mathcal{O} = \mathrm{End}(E)$. In the incidental case that $\mathcal{O} \supsetneq \mathcal{O}_1$ we have constructed a new endomorphism $E \longrightarrow E' \cong E$.

We now recap the procedure for constructing the isogeny with kernel ideal $\mathfrak{r}$. We note that any prime ideal $\mathfrak{r}$ of $\mathcal{O}$ which does not divide the discriminant of $\mathbb{Z}[\pi]$ can be written in the form $(r, \pi - b)$ for $r = N(\mathfrak{r})$ and $b \in \mathbb{Z}$. Let $F_E(X, Y)$ be a Weierstrass equation for $E$ and let $\psi_r(X, Y)$, $\psi_b(X, Y)$, and $\phi_b(X)$ be the division polynomials on $E$ in the notation of § 2.2. The kernel of the isogeny $E \to E' = E/E[\mathfrak{r}]$ is determined

by the ideal

$$I = (\psi_r(X,Y), X^q\psi_b(X,Y)^2 - \phi_b(X)) \subseteq \frac{k[X,Y]}{(F_E(X,Y))}.$$

We let $\psi(X)$ be a generator for $I \cap k[X]$, and construct $E/E[\mathfrak{r}]$ using the formulas of § 2.4.

We can now complete the determination of the endomorphism type of the curve $E$ of Example 2. We return to the complexity issues in the following section, in which we synthesize an algorithm.

**Example 6.** Now we can complete the calculation of the index of $\mathbb{Z}[\pi]$ in $\mathcal{O} = \mathrm{End}(E)$ for the curve of Example 2. In order to have class group of the smallest possible size, it will be useful to have an isogenous curve near the surface for each of the primes 2, 3 and 7. It is easy to find a curve one level above the floor of rationality for $l$ since the unique isogeny of degree $l$ over $\mathbb{F}_p$ from a curve at the floor of rationality is to a curve with larger endomorphism ring. Finding a curve at the surface, however, involves a random search for one lying at the surface. Of the $l+1$ elliptic curves isogenous to $E$ via an isogeny of degree $l$, only one lies at a depth less than $E$. At each depth above the floor of rationality one must calculate up to $l+1$ isogenies and determine the depth of each by the methods of the previous section. By means of such a search we identify an elliptic curve $E_0$ with $j$-invariant

$$j_0 = 580821385975059568086463192 \bmod p$$

at the surface with respect to 2, 3, and 7. We know then that the endomorphism ring has either discriminant $-3 \cdot 547^2 \cdot 105953$ or is maximal with discriminant $-3 \cdot 105953$. In the maximal order there exists a principal ideal $\mathfrak{p}_{13}\mathfrak{p}_{19}^3$ of norm $13 \cdot 19^3$. Since 13 and 19 do not divide the conductor of $\mathbb{Z}[\pi]$, in any order $\mathcal{O}_1$ containing $\mathbb{Z}[\pi]$, the primes $\mathfrak{p}_{13}$ and $\mathfrak{p}_{19}$ restrict to primes $\mathfrak{q}_{13} = (13, \pi - 3)\mathcal{O}_1$ and $\mathfrak{q}_{19} = (19, \pi + 3)\mathcal{O}_1$ in $\mathcal{O}_1$.

The curve $E_0/E_0[\mathfrak{q}_{13}]$ isogenous to $E_0$ via the isogeny of degree 13 induced by the ideal $\mathfrak{q}_{13}$ has the following $j$-value:

$$j_1 = 491225607620541146270113976 3 \bmod p.$$

Further, constructing isogenies induced by the ideal $\mathfrak{q}_{19}$, we get a sequence of elliptic curves having $j$-invariants as follows.

$$\begin{aligned} j_2 &= 669576847411527478166178236 6 \bmod p, \\ j_3 &= 100139838059437636125606584 88 \bmod p, \\ j_4 &= 763088943985577825880020317 6 \bmod p. \end{aligned}$$

Since the final curve has $j$-value $j_4 \neq j_0$, we can conclude that $\mathfrak{q}_{13}\mathfrak{q}_{19}^3$ is not principal in the endomorphism ring of $E_0$, so it has discriminant $-3 \cdot 547^2 \cdot 105953$. Combining the index calculations done in Example 5, we conclude that the endomorphism ring $\mathcal{O}$ of $E$ has discriminant $-2^{18} \cdot 3^2 \cdot 7^{10} \cdot 547^2 \cdot 105953$.

## 4.4 Computation of the endomorphism type

The objective of this section is to prove the following theorem.

**Theorem 24** *There exists a deterministic algorithm that given an elliptic curve $E$ over a finite field $k$ of $q$ elements, computes the isomorphism type of the endomorphism ring of $E$ and if a certain generalization of the Riemann hypothesis holds true, for any $\varepsilon > 0$ runs in time $\mathrm{O}(q^{1/3+\varepsilon})$.*

The algorithm combines the methods of the previous sections to produce a deterministic algorithm. Throughout this section, $B$ will be a positive integer. We refer to primes or prime powers less than or equal to $B$ as small, and those greater than $B$ as large. The notation for the endomorphism ring $\mathcal{O}$, the field of fractions $K = \mathcal{O} \otimes \mathbb{Q}$, and the discriminant $D$ and the conductor $m$ of $\mathbb{Z}[\pi]$ remain as previously defined. The maximal order of $K$ is the order

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - a}{m}\right].$$

The proposed algorithm uses the calculation of explicit kernels from § 4.1 to test the index of $\mathbb{Z}[\pi]$ in $\mathcal{O}$ for all integers $n|m$ up to the bound $B$. Larger primes and prime powers will be treated using class group calculations as in § 4.3. While the method of probing the depths of § 4.2 provides a practical method for handling small primes dividing the conductor, for lack of a fast, deterministic factorization algorithm for polynomials over finite fields, it will not play a role in the complexity analysis. Moreover, in the final analysis, a worst case scenario in which no powers of small primes occur in the index $m$ renders this additional tool inapplicable. Although we do maintain the restriction to deterministic algorithms, for the sake of exhibiting small splitting primes, we venture into conjectural territory and assume a certain generalized Riemann hypothesis.

**Proof of Theorem 24.** The first step in the determination of the endomorphism type of $E$ is to calculate the trace $t$ of the Frobenius endomorphism, and second, to factor its discriminant $t^2 - 4q$ to discover $m$, and determine $a$. As noted in Example 3, the factorization step can be an obstacle to the endomorphism type computation for $E$ even when the ring $\mathbb{Z}[\pi]$ itself is maximal. Existing factoring algorithms perform better than the result of the theorem, in fact we can find all square factors in time $\mathrm{O}(q^{1/6+\varepsilon})$.

Next we consider the divisors of $m$ below the bound $B$. As we have noted, it suffices to consider prime power divisors. For any prime power divisor $n \leq B$, we apply the explicit kernel calculation of § 4.1. The following lemma gives the complexity of the computation.

**Lemma 25** *There exists an algorithm to calculate the kernel of $\pi - a$ on $E[n]$ in time $\mathrm{O}(n^2 \log n \log q)$.*

**Proof.** Let $\psi_n(X,Y)$ be the $n$-th division polynomial, and let $\psi_n(X)$ be a generator for $(\psi_n(X,Y)) \cap k[X]$. Then $\psi_n(X)$ defines the $n$-torsion points of $E$. As observed in § 4.1 it suffices to compute

$$X^q \psi_a(X,Y)^2 - \phi_a(X) \bmod \psi_n(X),$$

and let

$$\psi_0(X) = \gcd(X^q \psi_a(X,Y)^2 - \phi_a(X), \psi_n(X)).$$

Then $\psi_0(X)$ defines the kernel of $\pi - a$ on $E[n]$. Since the degree of $\psi_n(X)$ is $O(n^2)$, using fast multiplication and fast gcd algorithms, this can be achieved in time $\mathcal{O}(n^2 \log n \log q)$.

Thus we can apply explicit kernel calculations to determine if $n$ divides $[\mathcal{O} : \mathbb{Z}[\pi]]$ for all of the $\mathrm{O}(\log q)$ divisors up to $B$ in time $\mathcal{O}(B^2 \log B (\log q)^2)$.

At this point we need to make use of the conjectural existence of many small primes. Lagarias and Odlyzko [14] prove that a result of this sort follows from the truth of a generalized Riemann hypothesis. First we need to introduce some notation. Let

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)} \sim \frac{x}{\log(x)},$$

and for any Galois extension $L/F$ of number fields, we can define the Artin symbol $[\mathfrak{p}, L/F]$ on primes of $F$ as a conjugacy class of $G = \mathrm{Gal}(L/F)$. For each conjugacy class $C$ of $G$, define

$$\pi_C(x, L/F) = \left|\{\mathfrak{p} : \mathfrak{p} \text{ is unramified in } L, [\mathfrak{p}, L/F] = C, \text{ and } \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{p}) \leq x\}\right|,$$

and let $n_L$ be the degree of the extension $L/\mathbb{Q}$ and $D_L$ be its discriminant. The theorem of Lagarias and Odlyzko is as follows.

**Theorem 26** *There exists an effectively computable positive absolute constant $c_1$ such that if the generalized Riemann hypothesis holds for the Dedekind zeta function of $L$, then for every $x > 2$ and conjugacy class $C$ of $\mathrm{Gal}(L/F)$*

$$\left|\pi_C(x, L/F) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leq c_1 \left(\frac{|C|}{|G|} x^{1/2} \log(|D_L| x^{n_L}) + \log(|D_L|)\right).$$

**Proof.** [14, Theorem 1.1].

We apply this theorem with $L = K$ and $F = \mathbb{Q}$, and $C = \{1\}$. Lagarias and Odlyzko observe that the crossover point for $\mathrm{Li}(x)$ and their bound occurs below

$$x_0 = c_2 (\log |D_L|)^2 (\log\log |D_L|)^4,$$

for some effectively computable constant $c_2$. If we set a smoothness bound $S$ at some value greater than $x_0$ we are guaranteed to have an effectively computable positive fraction of $\mathrm{Li}(S)$ splitting primes in $\mathcal{O}_K$ with norm less than $S$. We state this as a corollary of the theorem.

**Corollary 27** *For every $\varepsilon > 0$ and $t > 2$ there exists an effectively computable real number $d$ such that if $K$ is a quadratic extension of $\mathbb{Q}$ with $|D_K| > d$ then for $S = (\log |D_K|)^t$,*

$$\left|\pi_{\{1\}}(S, K/\mathbb{Q})\right| \geq \frac{(1-\varepsilon)\,\mathrm{Li}(S)}{2}.$$

Hereafter we assume we have fixed an order $\mathcal{O}_1$ such that $[\mathcal{O}_1 : \mathbb{Z}[\pi]] = n_1$ is a large prime power. Also let $S$ be a fixed smoothness bound, and let $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$ be a set of primes of $\mathcal{O}_1$, relatively prime to $D = t^2 - 4q$ and bounded in norm by $S$. We further assume that $\mathrm{N}(\mathfrak{r}_i) \neq \mathrm{N}(\mathfrak{r}_j)$ for $i \neq j$, so that for positive integers $s_i$ and $t_i$, if

$$\overline{\mathfrak{r}}_1^{s_1} \cdots \overline{\mathfrak{r}}_c^{s_c} \mathfrak{r}_1^{t_1} \cdots \mathfrak{r}_c^{t_c}$$

is principal and generated by $\beta \in \mathcal{O}_1$, then $\beta \notin \mathcal{O}_1^* \mathbb{Z}$, as long as not all $s_i = t_i$. We refer to such a set of primes $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$ as a *factor base*.

In practice the calculation proceeds by first using the exact sequence (4.1) of class groups to find relations in the class group of $\mathcal{O}_K$, then to determine relations in the kernel

$$\frac{(\mathcal{O}_K/m_1\mathcal{O}_K)^*}{\mathcal{O}_K^*(\mathbb{Z}/m_1\mathbb{Z})^*}$$

of the surjection $\mathrm{Cl}(\mathcal{O}_1) \to \mathrm{Cl}(\mathcal{O})$. In the complexity analysis, this separation is suppressed. Thus the first step is to determine enough ideals $\mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c}$ over the factor base $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$ to guarantee that the map of these ideals to $\mathrm{Cl}(\mathcal{O}_1)$ is not injective. Thus we fix an exponent bound $u$ and form a list of product ideals $\mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c}$ in the factor base with $\sum s_i \leq u$ until the number of ideals exceeds the class number of $\mathcal{O}_1$. The number of ideals over the factor base of size $c$ with total exponent bounded by $u$ is $\binom{u+c}{c}$. The following combinatorial lemma will be useful to choose appropriate values of $u$ and $c$.

**Lemma 28** *The binomial coefficient $\binom{u+c}{c}$ satisfies the following bounds.*

$$\frac{\left(\frac{u+c+1}{c+1}\right)^{c+1}\left(\frac{u+c+1}{u+1}\right)^{u+1}}{u+c+1} \leq \binom{u+c}{c} \leq \left(\frac{u+c}{c}\right)^{c}\left(\frac{u+c}{u+1}\right)^{u}.$$

**Proof.** The bounds follow from comparing the logarithm of $\binom{u+c}{c}$ to the integral of $\log(x)$.

We would like to choose $u$ and $c$ in order to bound the class number of $\mathcal{O}_1$ by the number of ideals we can produce as products of elements in the factor base $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$

having total exponent bounded by $u$. Thus we would like to have

$$h(\mathcal{O}_1) \leq \frac{\left(\frac{u+c+1}{c+1}\right)^{c+1}\left(\frac{u+c+1}{u+1}\right)^{u+1}}{u+c+1} \leq \binom{u+c}{c}. \tag{4.3}$$

We are able to satisfy these bounds, but it will not be sufficient to produce a smooth element of $\mathcal{O}_1$. We would like to produce a smooth element $\beta$ which generates $\mathcal{O}_1 \otimes \mathbb{Z}_l$ over $\mathbb{Z}_l$. As a consolation, we will obtain bounds which constrain the index $[\mathcal{O}_1 \otimes \mathbb{Z}_l : \mathbb{Z}_l[\beta]]$.

**Lemma 29** *For every $\delta > 0$ and $t > 2$ there exists a deterministic algorithm which, given a discriminant $D_1$ of an order $\mathcal{O}_1$ in a complex imaginary extension $K/\mathbb{Q}$ for which a generalized Riemann hypothesis holds, returns an element $\beta$ of $\mathcal{O}_1 - \mathbb{Z}$ such that*

1. *all prime factors of $\beta$ are bounded in norm by $\mathrm{O}((\log|D_1|)^t)$, and*
2. *the norm of $\beta$ is bounded by $\mathrm{O}(|D_1|^\gamma)$, where $\gamma = \frac{(1+\delta)t}{(t-1)}$,*

*and runs in time $\mathrm{O}(h(\mathcal{O}_1)\log|D_1|)$.*

**Proof.** Set $\gamma_0 = 1 + \delta$, then let

$$u = \frac{\gamma_0 \log|D_1|}{(t-1)\log\log|D_1|} \text{ and set } c = u^t - 1.$$

Choose a factor base $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$ consisting of one prime lying over each of the first $c$ primes of $\mathbb{Z}$ which split in $\mathcal{O}_1$. The number of ideals $\mathfrak{a} = \mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c}$ with $\sum s_i \leq u$ is then $\binom{u+c}{c}$, which is bounded below by

$$\frac{\left(\frac{u^t+u}{u^t}\right)^{u^t}\left(\frac{u^t+u}{u+1}\right)^{u}}{u+1} \sim \frac{e^u\left(\frac{u^t+u}{u+1}\right)^{u}}{u+1},$$

by Lemma 28 and the observation that for fixed $t > 2$, the term $\left(\frac{u^t+u}{u^t}\right)^{u^t} \sim e^u$.

From the bound $h(\mathcal{O}_1) = \mathrm{O}(|D_1|^{1/2}\log|D_1|)$, we find that for the choice of $u$ and $c$ above, and for all $|D_1|$ sufficiently large, that $\binom{u+c}{c}$ exceeds $h(\mathcal{O}_1)$. Once we have listed a number of ideals in excess of the class number of $\mathcal{O}_1$, we find two ideals $\mathfrak{a} = \mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c}$ and $\mathfrak{b} = \mathfrak{r}_1^{t_1} \cdots \mathfrak{r}_c^{t_c}$ lying in the same class. Thus there exists $\beta$ in $\mathcal{O}_1$ such that

$$(\beta) = \overline{\mathfrak{a}}\mathfrak{b} = \overline{\mathfrak{r}}_1^{s_1} \cdots \overline{\mathfrak{r}}_c^{s_c}\mathfrak{r}_1^{t_1} \cdots \mathfrak{r}_c^{t_c},$$

and the running time is dominated by the calculation of reduced ideal classes for up to $h(\mathcal{O}_1)$ ideals. Since we can find a reduced binary quadratic form representing the class of an ideal $\mathfrak{r}_1^{s_1} \cdots \mathfrak{r}_c^{s_c}$ in time $O(\log |D_1|)$, this gives the stated complexity bound.

We now apply Corollary 27 to conclude that for $|D_1|$ sufficiently large, if the generalized Riemann hypothesis for $K$ holds, then the maximum norm of a prime in the factor base $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_c\}$ is bounded by $S = (\log |D_1|)^t$. Note that we must exclude from the first splitting primes of $K$ at most $\log |D_1|$ primes dividing the conductor of $\mathcal{O}_1$. Thus we conclude that

$$\log \mathrm{N}(\beta) \leq \sum_{i=1}^{c} (s_i + t_i) \log \mathrm{N}(\mathfrak{r}_i) \leq 2u \log S = \frac{t\gamma_0}{t-1} \log |D_1| = \gamma \log |D_1|.$$

This completes the proof of the lemma.

For each prime power $n_1 > B$, we construct $\beta \in \mathcal{O}_1$ as above. The computation of the isogeny with kernel $E[\mathfrak{b}]$, where $\mathfrak{b} = \beta\mathcal{O} \cap \mathcal{O}$ can be done in polynomial time. If $\mathfrak{b}$ is not principal, then $\mathcal{O}_1$ is not contained in $\mathcal{O}$ and the conductor of $\mathcal{O}$ does not divide $m_1 = m/n_1$. If $\beta$ lies in $\mathcal{O}$, then we have constructed an entirely new endomorphism which, much as $\pi$, has a compact representation. By the bound on $\mathrm{N}(\beta)$, the discriminant of $\mathbb{Z}[\beta]$ satisfies

$$|\operatorname{disc}(\mathbb{Z}[\beta])| \leq 4\mathrm{N}(\beta) = \mathrm{O}(|D_1|^{\gamma}),$$

where $\gamma = (1+\delta)t/(t-1)$, and the index of $\mathbb{Z}[\beta]$ in $\mathcal{O}_1$ is bounded by $\mathrm{O}(|D_1|^{(\gamma-1)/2})$. Thus we have constructed an endomorphism $\beta : E \to E$ as an element of $\mathcal{O}_K$, about which we know the following data.

1. A representation $\beta = a_1 + b_1\omega$ in $\mathcal{O}_K$, where $\omega = (\pi - a)/m$; thus in particular we know the conductor $b_1$ of $\mathbb{Z}[\beta]$ and an integer $a_1$ such that $\beta - a_1 \equiv 0 \bmod b_1\mathcal{O}_K$.
2. Rational functions $\alpha_i : E_{i-1} \to E_i$ for $1 \leq i \leq u$, such that $E = E_0 = E_u$, such that $\beta$ is the composite of the $\alpha_i$, and such that each $\alpha_i$ has degree bounded by $S$.

We call such an isogeny an explicit $S$-smooth isogeny for $E$. We now adapt the explicit kernel calculations of § 4.1 to $\mathbb{Z}[\beta]$.

**Lemma 30** *There exists a deterministic algorithm which takes an explicit $S$-smooth isogeny $\beta : E \to E$ and a divisor $n$ of the conductor of $\mathbb{Z}[\beta]$, and which determines if $n$ divides $[\mathcal{O} : \mathbb{Z}[\beta]]$ in $\mathrm{O}(n^2(n^2 \log S + S \log n)u)$ polynomial time operations in $k$.*

**Proof.** As with the algorithm of § 4.1 it will suffice to determine the action of $\beta$ on the image of $E[n]$ in $E/\{[\pm 1]\} = \mathbb{P}^1$, and compare this with the action of $[a_1]$. Let $\beta$ be the composite

$$E = E_0 \xrightarrow{\alpha_1} E_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_u} E_u = E,$$

and the map induced by $\alpha_i$ on $\mathbb{P}^1$ be $\alpha_i|_{\mathbb{P}^1}(x) = \varphi_i(x)/\chi_i(x)$. For each $i$ let $\psi_n^{(i)}(X,Y)$ be the $n$-th division polynomial on $E_i$, and let $\psi_n^{(i)}(X)$ be a generator for $(\psi_n^{(i)}(X,Y))\cap k[X]$. We are interested in the induced maps:

$$\frac{k[X]}{(\psi_n(X))} = \frac{k[X_u]}{(\psi_n^{(u)}(X_u))} \longrightarrow \cdots \longrightarrow \frac{k[X_1]}{(\psi_n^{(1)}(X_1))} \longrightarrow \frac{k[X_0]}{(\psi_n^{(0)}(X_0))} = \frac{k[X]}{(\psi_n(X))}.$$

Rather than concerning ourselves with inverting elements in the above rings, we express a quotient

$$\frac{\sigma(X)}{\tau(X)} \in \frac{k[X]}{(\psi_n(X))}$$

as $(\sigma(X) : \tau(X))$. In order to compose maps, we denote the homogenization of $(\sigma(X) : \tau(X))$ by $(\widetilde{\sigma}(X,Z) : \widetilde{\tau}(X,Z))$, where

$$\widetilde{\sigma}(X,Z) = \sigma(\frac{X}{Z})Z^d \quad \text{and} \quad \widetilde{\tau}(X,Z) = \tau(\frac{X}{Z})Z^d,$$

for $d = \max(\deg(\sigma(X)), \deg(\tau(X)))$.

We can then compute the map $X_i = (X_i : 1) \longmapsto (\sigma_i(X) : \tau_i(X))$ given by $\alpha_i \circ \cdots \circ \alpha_1$, by setting $(\sigma_0(X) : \tau_0(X)) = (X : 1)$ and recursively calculating

$$(\sigma_i(X) : \tau_i(X)) = (\widetilde{\sigma}_{i-1}(\varphi_i(X), \chi_i(X)) : \widetilde{\tau}_{i-1}(\varphi_i(X), \chi_i(X))),$$

where $\sigma_i(X)$ and $\tau_i(X)$ are calculated modulo the polynomial $\psi_n(X)$. This gives

$$\beta_{\mathbb{P}^1}(X) \equiv \frac{\sigma_u(X)}{\tau_u(X)} \bmod \psi_n(X).$$

In order to determine if $\beta$ and $[a_1]$ agree on $E[n]$ it remains only to calculate

$$\sigma_u(X)\psi_{a_1}(X,Y)^2 - \phi_{a_1}\tau_u(X) \bmod \psi_n(X),$$

for the division polynomials $\phi_{a_1}(X)$ and $\psi_{a_1}(X,Y)$. The result is zero if and only if $E[n] \subseteq \ker(\beta - [a_1])$, and thus $n$ divides the index $[\mathcal{O} : \mathbb{Z}[\beta]]$.

The complexity of the calculation is dominated by the calculations of the composites

$$\widetilde{\sigma}_{i-1}(\varphi_i(X), \chi_i(X)) \quad \text{and} \quad \widetilde{\tau}_{i-1}(\varphi_i(X), \chi_i(X)).$$

For this computation, we need $\deg \sigma_{i-1} + \deg \tau_{i-1} = \mathrm{O}(n^2)$ multiplications of polynomials of degrees $n^2$ and $S$. Using fast multiplication methods, this gives a complexity of $\mathrm{O}(n^2(n^2 \log S + S \log n))$ for each of the $u$ compositions of isogenies. This proves the stated complexity for the algorithm.

**Note.** In our application, we have bounds $S = \mathrm{O}(n)$, and $\log(\deg \beta) \leq u \log S$. Thus the complexity is $\mathrm{O}(n^4 \log(\deg \beta))$. A much better complexity bound can be obtained if we compute each of the polynomials $\psi_n^{(i)}(X)$ and compute the image of

$$X = (X : 1) \longmapsto (\sigma_i(X_{u-i}) : \tau(X_{u-i}))$$

induced by $\alpha_u \circ \cdots \circ \alpha_{u-i}$ by setting $(\sigma_0(X_u) : \tau_0(X_u)) = (X_u : 1)$, recursively calculating the composites

$$(\sigma_i(X_{u-i}) : \tau_i(X_{u-i})) = (\widetilde{\varphi}_{u-i}(\sigma_{i-1}(X_{u-i}), \tau_{i-1}(X_{u-i})) : \widetilde{\chi}_{u-i}(\sigma_{i-1}(X_{u-i}), \tau_{i-1}(X_{u-i})))$$

modulo $\psi_n^{(i)}$, and making use of the fact that the degrees of $\varphi$ and $\chi$ remain bounded by $S$. The improved complexity is not necessary since we are able to control the size of $n$ by selecting a larger value of $t$ in Lemma 29.

We apply this lemma with $n$ equal to the greatest common divisor of $[\mathcal{O}_1 : \mathbb{Z}[\beta]]$ and $n_1$ to decide if $n_1$ divides $[\mathcal{O} : \mathbb{Z}[\pi]]$. Thus Lemma 25, Lemma 29, and Lemma 30 complete the index calculation for all prime powers dividing the conductor of $\mathbb{Z}[\pi]$. By choosing $B = q^{1/6}$, all prime powers less than or equal to $B$ can be determined in time $\mathrm{O}(q^{1/3}(\log q)^2)$ by Lemma 25. We apply Lemma 29 to orders $\mathcal{O}_1$ with $[\mathcal{O}_1 : \mathbb{Z}[\pi]]$ equal to a prime power greater than $B$. Then the discriminant of $\mathcal{O}_1$ satisfies $|D_1| = \mathrm{O}(q^{2/3})$, and so the running time is $\mathrm{O}(q^{1/3}(\log q)^2)$, where we use the bound $h(\mathcal{O}_1) = \mathrm{O}(|D_1|^{1/2} \log |D_1|)$. If we set $\delta = 1/80$ and $t = 10$, then we apply Lemma 30 with $S = \mathrm{O}((\log q)^{10})$, with $\log(\deg \beta) = \mathrm{O}(u \log S) = \mathrm{O}(\log q)$, and $n = \mathrm{O}(|D_1|^{1/4})$ to obtain a complexity bound of $\mathrm{O}(q^{1/3}(\log q)^6)$. All of the $\log q$ factors, polynomial time calculations in $k$, and treatment of the $\mathrm{O}(\log q)$ divisors of the conductor of $\mathbb{Z}[\pi]$ are subsumed under the factor $q^{\varepsilon}$ in the complexity for the final algorithm, with the bounding constant appropriately adjusted. This completes the proof of Theorem 24.

# Chapter 5

# Arithmetic of quaternion algebras

In this chapter we introduce the arithmetic of quaternion algebras which we need in order to understand the endomorphism rings and arithmetic of supersingular elliptic curves.

## 5.1 Introduction to quaternions

A quaternion algebra $\mathfrak{A}$ over a field $F$ is defined to be a central simple algebra of dimension four over $F$, that is, $\mathfrak{A}$ is a ring with no nontrivial two-sided ideals, equipped with a homomorphism of rings $F \to \mathfrak{A}$ which is an isomorphism with the center of $\mathfrak{A}$ and which gives $\mathfrak{A}$ the structure of a vector space of dimension four over $F$. We identify $F$ with its image in $\mathfrak{A}$ under this homomorphism. We consider only quaternion algebras over $\mathbb{Q}$, or over one of the completions $\mathbb{Q}_p$ or $\mathbb{R}$ at a place of $\mathbb{Q}$. We define a lattice in a quaternion algebra $\mathfrak{A}$ over $\mathbb{Q}$ to be a finitely generated $\mathbb{Z}$-module which contains a basis for $\mathfrak{A}$ over $\mathbb{Q}$, and adopt the notation $\Lambda$ for such a lattice. A lattice in a quaternion algebra over $\mathbb{Q}_p$ is a finitely generated $\mathbb{Z}_p$-module containing a $\mathbb{Q}_p$-basis. We denote an order of a quaternion algebra, defined to be a lattice which is a subring containing 1, by $\mathcal{O}$. Moreover, for a finite prime $p$ or the infinite prime $\infty$ of $\mathbb{Q}$, we make the following definitions:

$$\mathfrak{A}_p = \mathfrak{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p \quad \text{and} \quad \mathfrak{A}_\infty = \mathfrak{A} \otimes_{\mathbb{Q}} \mathbb{R},$$

$$\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \quad \text{and} \quad \Lambda_p = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

The Wedderburn structure theorem [25, Chapter 1, Theorem 7.4] implies that a quaternion algebra over a field $F$ is either a central division algebra over $F$ or isomorphic to the matrix algebra $\mathbb{M}_2(F)$. If $\mathfrak{A}$ is a quaternion algebra over $\mathbb{Q}$ then a prime $p$ is said to *ramify* if $\mathfrak{A}_p$ is a division algebra or *split* if $\mathfrak{A}_p$ is isomorphic to $\mathbb{M}_2(\mathbb{Q}_p)$. The ramification index of $p$ is defined to be 2 is $p$ ramifies in $\mathfrak{A}$ and equal to 1 otherwise.

A quaternion algebra which ramifies at infinity is called definite, and one which splits at infinity is called indefinite.

As a consequence of the Wedderburn theorem, for any $\alpha$ in $\mathfrak{A}$ not in the center $F$, the commutative ring $K = F[\alpha]$ is of dimension two over $F$. This follows easily if $\alpha$ is a unit in $\mathfrak{A}$ for then $K$ is a field extension of $F$, and $\mathfrak{A}$ is a vector space and noncentral algebra over $K$, hence $K/F$ is necessarily quadratic. If $\alpha$ is not invertible, then $\mathfrak{A}$ must be isomorphic to $\mathbb{M}_2(F)$, and so $\alpha$ satisfies its characteristic equation of degree two. Thus every noncentral element generates a quadratic extension of the center, and the maximal commutative subrings of $\mathfrak{A}$ are quadratic extensions over $F$. The quaternion algebras which arise from supersingular elliptic curves are division algebras over $\mathbb{Q}$, and the maximal subfields of $\mathfrak{A}$ are imaginary quadratic extensions of $\mathbb{Q}$.

To each $\alpha$ in $\mathfrak{A}$ we can associate its conjugate $\overline{\alpha}$ in $F[\alpha]$. The map $\mathfrak{A} \longrightarrow \mathfrak{A}$ taking $\alpha$ to $\overline{\alpha}$ gives an involution of $\mathfrak{A}$. We define the reduced norm $\mathrm{N} : \mathfrak{A} \longrightarrow F$ and the reduced trace $\mathrm{Tr} : \mathfrak{A} \longrightarrow F$ by $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ and $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$. Hereafter we refer to these maps as the norm and trace, respectively, which should not be confused with the norm and trace of the vector space endomorphism of $\mathfrak{A}$ given by left multiplication by $\alpha$.

The Brauer group of a field $F$ provides a means of classifying the central simple algebras over $F$. We define a relation $\sim$ on the set of central simple algebras over $F$ by the definition that $\mathfrak{A} \sim \mathfrak{B}$ if and only if there exist finite dimensional vector spaces $V$ and $W$ over $F$ such that

$$\mathfrak{A} \otimes_F \mathrm{End}(V) \cong \mathfrak{B} \otimes_F \mathrm{End}(W),$$

as algebras over $F$. Denote by $[\mathfrak{A}]$ the equivalence class of $\mathfrak{A}$ under this relation. For two central simple algebras $\mathfrak{A}$ and $\mathfrak{B}$ over $F$, the tensor product $\mathfrak{A} \otimes \mathfrak{B}$ is again $F$-central and simple [15, Chapter 4, Theorem 1.2], so we define a semigroup operation on the set of equivalence classes by $[\mathfrak{A}] \cdot [\mathfrak{B}] = [\mathfrak{A} \otimes_F \mathfrak{B}]$ with $[F]$ as the identity element. Denote this semigroup by $\mathrm{Br}(F)$.

For each algebra $\mathfrak{A}$ we can construct its opposite algebra $\mathfrak{A}^{\mathrm{op}}$ as the algebra with the same underlying $F$-vector space and multiplication defined by $a^{\mathrm{op}} \cdot b^{\mathrm{op}} = (ba)^{\mathrm{op}}$. Then there exists an isomorphism:

$$\theta : \mathfrak{A} \otimes_F \mathfrak{A}^{\mathrm{op}} \longrightarrow \mathrm{End}_F(\mathfrak{A})$$

defined by $\theta\left(a \otimes b^{\mathrm{op}}\right)(c) = acb$. It follows that $[A^{\mathrm{op}}] = [A]^{-1}$ and therefore $\mathrm{Br}(F)$ is a group.

The conjugation involution defines an isomorphism between a quaternion and its opposite algebra, thus quaternion algebras have order 2 in the Brauer group of $F$. By the Wedderburn theorem [25] every central simple algebra over $F$ has the form $\mathbb{M}_n(D)$ for a central division algebra $D$ over $F$. As a consequence, we state the following classification theorem for classes of the Brauer group.

**Theorem 31** *The elements of* $\mathrm{Br}(F)$ *are in one to one correspondence with the isomorphism classes of central division algebras over* $F$*, by the map* $D \mapsto [D]$*.*

**Proof.** [15, Chapter 4, Proposition 1.4].

Finally we recall a fundamental exact sequence from class field theory [32]. A central result from local class field theory states that there exists a canonical isomorphism $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ for all finite $p$, and Frobenius proved in 1878 that $\mathrm{Br}(\mathbb{R})$ has order two, which by analogy we embed in $\mathbb{Q}/\mathbb{Z}$ by a homomorphism which we denote $\mathrm{inv}_\infty$. Then there exists an exact sequence of groups:

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where $\mathrm{Br}(\mathbb{Q})$ maps diagonally to $\bigoplus_p \mathrm{Br}(\mathbb{Q}_p)$ via $[\mathfrak{A}] \mapsto \bigoplus_p [\mathfrak{A}_p]$, and the surjection on $\mathbb{Q}/\mathbb{Z}$ is given by $\mathrm{inv} = \sum \mathrm{inv}_p$. Necessarily the number of primes ramifying in a quaternion algebra over $\mathbb{Q}$, including the infinite prime, is finite and even in number. Moreover, the image of the quaternion algebras in the Brauer group of $\mathbb{Q}$ equals the 2-torsion subgroup of $\mathrm{Br}(\mathbb{Q})$. The quaternion algebras which arise from endomorphism rings of supersingular elliptic curves are ramified at the characteristic $p$ and at $\infty$, thus form a set of generators for the two torsion subgroup of $\mathrm{Br}(\mathbb{Q})$.

Before moving on to the study of orders and ideals, we give the following examples of quaternion algebras.

1. Over the real numbers, the algebra

   $$\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij,$$

   defined by the relations $i^2 = -1$, $j^2 = -1$, and $ij = -ji$, generates the Brauer group of $\mathbb{R}$. This is Hamilton's classical ring of quaternions.

2. For any prime $p$ there is up to isomorphism a unique quaternion algebra over $\mathbb{Q}$ ramified at $p$ and $\infty$. For instance the algebra

   $$\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$$

   satisfying $i^2 = -3$, $j^2 = -1223$, and $ij = -ji$ defines the algebra ramified at 1223 and $\infty$.

## 5.2 Orders, ideals, and class groups

The purpose of this section is to present the main results of the integral arithmetic of quaternion algebras over $\mathbb{Q}$. The material is primarily drawn from the articles of

Pizer [23], [24] and the definitive book on the subject by Vignéras [34]. For simplicity of presentation the focus will be on the maximal orders in a quaternion algebra $\mathfrak{A}$ over $\mathbb{Q}$. Most of the results in this section hold for the nonmaximal orders of a certain associated level which is analogous to the conductor of an order in an imaginary quadratic extension of $\mathbb{Q}$.

The following propositions will provide the main tools for working with quaternions.

**Proposition 32** *Let $\mathfrak{A}$ be a quaternion algebra over $\mathbb{Q}$. Let $M$ be a lattice in $\mathfrak{A}$. There exists a bijection between lattices $\Lambda$ and collections of lattices $(\Lambda(p))_{p<\infty}$ such that $\Lambda(p)$ is a lattice in $\mathfrak{A}_p$ and $\Lambda(p) = M_p$ for almost all primes $p$, and the inverse bijections are given by:*

$$\Lambda \longmapsto (\Lambda_p)_{p<\infty} \quad \textit{and} \quad (\Lambda(p))_{p<\infty} \longmapsto \bigcap_{p<\infty} (\mathfrak{A} \cap \Lambda(p)).$$

**Proof.** Vignéras [34, Proposition 5.1]

To show the necessity of the condition that the local data agree almost everywhere with a globally defined lattice, consider the following example. Let $\mathfrak{A} = \mathbb{M}_2(\mathbb{Q})$ and let $(\Lambda(p)) = (\alpha_p^{-1}\mathbb{M}_2(\mathbb{Z}_p)\alpha_p)$, where

$$\alpha_p = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}.$$

Then the intersection of the $\Lambda(p)$ inside of $\mathfrak{A}$ is equal to the ring of upper triangular matrices in $\mathbb{M}_2(\mathbb{Q})$, hence does not have full rank.

**Proposition 33** *Let $\mathfrak{A}$ be a quaternion algebra over $\mathbb{Q}$, let $p$ be a finite prime of $\mathbb{Q}$, and let $e$ be the ramification index of $p$ in $\mathfrak{A}$.*

1. *If $\mathfrak{A}_p$ is a division algebra over $\mathbb{Q}_p$, then there is a unique maximal order*

$$\mathcal{O}_p = \{\alpha \in \mathfrak{A}_p : \mathrm{N}(\alpha) \in \mathbb{Z}_p\}.$$

2. *If $\mathfrak{A}_p$ is isomorphic to $\mathbb{M}_2(\mathbb{Q}_p)$, then all maximal orders are conjugate to $\mathbb{M}_2(\mathbb{Z}_p)$ under this isomorphism.*
3. *A maximal order $\mathcal{O}_p$ of $\mathfrak{A}_p$ has a unique maximal two-sided ideal $\mathfrak{P}$. Every two-sided ideal of $\mathcal{O}_p$ is of the form $\mathfrak{P}^m$ for an integer $m$, and $\mathfrak{P}^e = (p)$.*

**Proof.** Reiner [25, Theorems 12.8 and 17.3].

**Proposition 34** *Let $\mathcal{O}$ be a maximal order of $\mathfrak{A}$. Then every left ideal of $\mathcal{O}_p$ is principal at all finite primes $p$. A left ideal $I$ of $\mathcal{O}$ is projective if and only if it is locally free at all finite primes $p$.*

**Proof.** The first statement is Theorem 17.3 of [25]. It follows that $I$ is projective if and only if at $I_p = \mathcal{O}_p\alpha_p$ for an invertible element $\alpha_p$ in $\mathfrak{A}_p^*$ at each finite prime $p$.

**Definition.** Let $\mathcal{O}$ be a maximal order in $\mathfrak{A}$. We define a fractional ideal $I$ of $\mathcal{O}$ to be a lattice in $\mathfrak{A}$ such that $\alpha I \subseteq I$ for all $\alpha$ in $\mathcal{O}$. Throughout this section we make the convention of referring to fractional ideals as ideals, and reserve integral ideal for a fractional ideal of $\mathcal{O}$ which is contained in $\mathcal{O}$. Two left ideals $I$ and $J$ of $\mathcal{O}$ are said to belong to the same *class* if $I = J\beta$ for some $\beta$ in $\mathfrak{A}^*$. The *class number* of $\mathcal{O}$, denoted $H$, is the number of distinct classes of projective left ideals. Two maximal orders $\mathcal{O}$ and $\mathcal{O}'$ belong to the same *type* if $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$ for some $\alpha$ in $\mathfrak{A}^*$. As a consequence of the theorem of Skolem–Noether [25, Theorem 7.21], a maximal order type coincides with an isomorphism class of orders. The *type number* $T$ is defined to be the number of distinct types of maximal orders.

As with number fields, we can define a ring of adeles for $\mathfrak{A}$. For any order $\mathcal{O}$ of $\mathfrak{A}$, we define the adele ring $A_{\mathfrak{A}}$ of $\mathfrak{A}$ to be the restricted product of the localizations $\mathfrak{A}_p$ with respect to the rings $\mathcal{O}_p$. If $S$ is a finite set of places of $\mathbb{Q}$ including infinity, then we let

$$A_S = \prod_{p\in S} \mathfrak{A}_p \times \prod_{p\notin S} \mathcal{O}_p,$$

endowed with the product topology. Each $A_S$ is a locally compact topological ring, and we define $A_{\mathfrak{A}}$ to be the union of the $A_S$ inside of $\prod_p \mathfrak{A}_p$, with each $A_S$ embedded as an open topological subring. Note that any two orders of $\mathfrak{A}$ differ at only finitely many primes, hence $A_{\mathfrak{A}}$ is independent of the order $\mathcal{O}$ in the above definition.

The group of ideles $J_{\mathfrak{A}}$ is defined to be the group of units in $A_{\mathfrak{A}}$, with the topology such that the homomorphism $J_{\mathfrak{A}} \longrightarrow A_{\mathfrak{A}} \times A_{\mathfrak{A}}$ given by $x \mapsto (x, x^{-1})$ is a homeomorphism onto its image.

For each $p$ we introduced the reduced norm map $\mathrm{N} : \mathfrak{A}_p \longrightarrow \mathbb{Q}_p$, which we can use to define a norm map on the ideles. Let $|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{Q}$ be the absolute value, normalized as usual so that $|p|_p = p^{-1}$. We define

$$\begin{aligned} \mathrm{N} : J_{\mathfrak{A}} &\longrightarrow \mathbb{Q}^* \\ s = (\alpha_p) &\longmapsto \prod_p |\mathrm{N}(\alpha_p)|_p . \end{aligned}$$

Define $J^1_{\mathfrak{A}}$ to be the kernel of the norm map in $J_{\mathfrak{A}}$. By means of the diagonal embedding, $\mathfrak{A}^*$ embeds in $J^1_{\mathfrak{A}}$. Define also $\mathcal{U}(\mathcal{O}) = \{s = (\alpha_p) \in J^1_{\mathfrak{A}} : \alpha_p \in \mathcal{O}_p^* \text{ for all } p < \infty\}$.

**Proposition 35** *Let $\mathfrak{A}$ be a quaternion algebra over $\mathbb{Q}$ and $\mathcal{O}$ a maximal order in $\mathfrak{A}$. Then the following results hold.*

1. *$\mathfrak{A}^*$ is a discrete subgroup of $J^1_{\mathfrak{A}}$.*
2. *$J^1_{\mathfrak{A}}/\mathfrak{A}^*$ is compact.*
3. *$\mathcal{U}(\mathcal{O})$ is an open compact subgroup of $J^1_{\mathfrak{A}}$.*

**Proof.** Weil [36].

From the correspondence between global lattices and collections of local lattices, for every left ideal $I$ of an order $\mathcal{O}$ and every idele $s = (\alpha_p)$, there exists a left ideal $J$ such that $J_p = I_p\alpha_p$ for all $p$, and we define $J = Is$. Under the action of $J^1_{\mathfrak{A}}$ on the set of left projective ideals given by $I \mapsto Is$, the isotropy group is $\mathcal{U}(\mathcal{O})$.

**Proposition 36** *The double cosets $\mathcal{U}(\mathcal{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*$ are in bijective correspondence with the ideal classes of projective left ideals of $\mathcal{O}$ via the map $s \mapsto \mathcal{O}s$.*

**Proof.** Let $I$ and $J$ be projective left ideals for $\mathcal{O}$. By Proposition 34, for each prime $p$ there are elements $\alpha_p$ and $\beta_p$ in $\mathfrak{A}^*_p$ such that $I_p = \mathcal{O}_p\alpha_p$ and $J_p = \mathcal{O}_p\beta_p$. By Proposition 32, for almost all primes $\alpha_p$ and $\beta_p$ lie in $\mathcal{O}^*_p$. Then $s = (\alpha_p^{-1}\beta_p)$ lies in $J^1_{\mathfrak{A}}$ and $J = Is$. Thus the action is $J^1_{\mathfrak{A}}$ is transitive, and the result follows.

We define the normalizer $\mathbf{N}(\mathcal{O})$ of $\mathcal{O}$ to be

$$\mathbf{N}(\mathcal{O}) = \{\alpha \in \mathfrak{A}^* : \alpha^{-1}\mathcal{O}\alpha = \mathcal{O}\},$$

and define the normalizer $\mathbf{N}(\mathcal{O}_p)$ of the order $\mathcal{O}_p$ in $\mathfrak{A}_p$ similarly. Then let $\mathfrak{N}(\mathcal{O})$ to be the restricted product of $\mathbf{N}(\mathcal{O}_p)$ with respect to the local units $\mathcal{O}^*_p$.

**Proposition 37** *Conjugation by $J^1_{\mathfrak{A}}$ defines a transitive action on the set of maximal orders of $\mathfrak{A}$. The isomorphism classes of maximal orders are in bijective correspondence with the set of double cosets $\mathfrak{N}(\mathcal{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*$ by the map $s \mapsto s^{-1}\mathcal{O}s$.*

**Proof.** Let $\mathcal{O}$ and $\mathcal{O}'$ be two maximal orders of $\mathfrak{A}$. By Proposition 33 at each prime $p$, the orders $\mathcal{O}_p$ and $\mathcal{O}'_p$ are conjugate: $\mathcal{O}'_p = \alpha_p^{-1}\mathcal{O}_p\alpha_p$. But $\mathcal{O}'_p = \mathcal{O}_p$ at almost all primes $p$ by Proposition 32, so $t = (\alpha_p)$ lies in $J^1_{\mathfrak{A}}$ and $\mathcal{O}' = t^{-1}\mathcal{O}t$. By definition, $\mathfrak{N}(\mathcal{O})$ lies is the stabilizer of $\mathcal{O}$ under the action of $J^1_{\mathfrak{A}}$ by conjugation on the set of maximal orders. All isomorphisms of maximal orders are determined globally by conjugation by $\mathfrak{A}^*$, thus the bijection follows.

**Proposition 38** *The class number $H$ and the type number $T$ are finite, and $T$ is less than or equal to $H$. For each maximal order, the number $H$ of classes of left ideals is equal to the number of classes of right ideals and is independent of the maximal order of $\mathfrak{A}$.*

**Proof.** The finiteness follows from Proposition 36 and Proposition 35 and since $\mathfrak{N}(\mathcal{O})$ contains $\mathcal{U}(\mathcal{O})$, the classes of maximal orders is a quotient of the classes of left ideals by the action of $\mathfrak{N}(\mathcal{O})$. The map $J^1_{\mathfrak{A}} \longrightarrow J^1_{\mathfrak{A}}$ sending $s \mapsto s^{-1}$ is a continuous involution of $J^1_{\mathfrak{A}}$ which restricts to continuous involutions of $\mathcal{U}(\mathcal{O})$ and $\mathfrak{A}^*$. Thus we have a bijection

$$\mathcal{U}(\mathcal{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^* \longrightarrow \mathfrak{A}^*\backslash J^1_{\mathfrak{A}}/\mathcal{U}(\mathcal{O}),$$

hence also of the left and right classes of projective ideals. Likewise, for each idele $t$ we have a homeomorphism $J^1_{\mathfrak{A}} \longrightarrow J^1_{\mathfrak{A}}$ sending $s \mapsto t^{-1}st$. This map restricts to a homeomorphism of $\mathfrak{A}^*$ and gives a homeomorphism $\mathcal{U}(\mathcal{O}) \to \mathcal{U}(t^{-1}\mathcal{O}t)$. Thus we also have a bijection

$$\mathcal{U}(\mathcal{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^* \longrightarrow \mathcal{U}(t^{-1}\mathcal{O}t)\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^*.$$

Since conjugation by $J^1_{\mathfrak{A}}$ is transitive by Proposition 37, the class number is the same for every maximal order of $\mathfrak{A}$.

As a result, we can state the following corollary.

**Corollary 39** *If $I_1, I_2, \ldots, I_H$ is a complete set of representatives of left ideal classes for any maximal order $\mathcal{O}$ of $\mathfrak{A}$, then the set of right orders of the $I_j$ represent all of the isomorphism classes of maximal orders.*

For left ideals $I$ and $J$ of an order $\mathcal{O}$, define $(I : J)_r = \{\alpha \in \mathfrak{A} : J\alpha \subseteq I\}$, and for right ideals $I$ and $J$ of $\mathcal{O}'$, define $(I : J)_l = \{\alpha \in \mathfrak{A} : \alpha J \subseteq I\}$. We define the *inverse* of a left ideal of $\mathcal{O}$ to be

$$I^{-1} = \{\alpha \in \mathcal{O} : I\alpha I \subseteq I\}.$$

The *right order* of a left ideal $I$ of $\mathcal{O}$ is defined to be $(I : I)_r$ and the *left order* of a right ideal $J$ of $\mathcal{O}'$ is defined to be $(J : J)_l$.

**Proposition 40** *Let $I$ be a projective left ideal for a maximal ideal $\mathcal{O}$. Then the right order $\mathcal{O}'$ is also maximal. Moreover, the left order of $I$ with respect to the right order $\mathcal{O}'$ is $\mathcal{O}$. The inverse of $I$ is equal to $(\mathcal{O} : I)_r$ and also to $(\mathcal{O}' : I)_l$.*

**Proof.** By Proposition 32 and Proposition 34, there exists an idele $s$ such that $I = \mathcal{O}s$. The right order is determined locally as the order $\mathcal{O}' = s^{-1}\mathcal{O}s$. Since it is conjugate to $\mathcal{O}$ at all primes $p$ and hence locally maximal, $\mathcal{O}'$ is also maximal. The left order of the projective right $\mathcal{O}'$ module $I$ is obviously $\mathcal{O}$. We can also write $I$ as $t\mathcal{O}'$ for some idele $t$, so that $I = t\mathcal{O}' = \mathcal{O}s$. Then

$$(\mathcal{O} : I)_r = s^{-1}\mathcal{O} = \mathcal{O}'t^{-1} = (\mathcal{O}' : I)_l.$$

To prove the identity of $(\mathcal{O} : I)_r$ with $I^{-1}$, we verify locally that

$$I\alpha I = \mathcal{O}s\,\alpha\,\mathcal{O}s \subseteq I = \mathcal{O}s$$

if and only if $\alpha \in s^{-1}\mathcal{O}$.

The set of left ideals of all the various maximal orders forms the *Brandt groupoid* of $\mathfrak{A}$. For two ideals $I$ and $J$ such that the right order of $I$ is equal to the left order of $J$, the composite $IJ = \{\sum_k i_k j_k : i_k \in I, j_k \in J\}$ is a well-defined ideal with left order equal to the left order of $I$ and right order equal to the right order of $J$.

Define a bilinear form $\Phi : \mathfrak{A} \times \mathfrak{A} \longrightarrow \mathbb{Q}$ by means of the norm

$$\Phi(x, y) = \mathrm{N}(x + y) - \mathrm{N}(x) - \mathrm{N}(y) = \mathrm{Tr}(x\overline{y}).$$

The *different* $\mathfrak{D}$ of an order $\mathcal{O}$ is the ideal inverse of the dual lattice of $\mathcal{O}$ with respect to the bilinear form $\Phi$. For each finite prime $p$ let $\mathrm{N}(I_p)$ be the ideal of $\mathbb{Z}_p$ generated by the set $\{\mathrm{N}(x) : x \in I_p\}$. Define the reduced norm of the ideal $I$ to be the positive integer

$$\mathrm{N}(I) = \prod_p \left|\mathbb{Z}_p/\mathrm{N}_p(I_p)\right|.$$

The *reduced discriminant* $d(\mathcal{O})$ of $\mathcal{O}$ is the norm of the different.

**Proposition 41** *If $\mathcal{O}$ is maximal, then $\mathfrak{D}$ is an integral two-sided ideal of $\mathcal{O}$, and for any basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\mathcal{O}$, we have*

$$d(\mathcal{O})^2 = \left|\det(\Phi(\alpha_i, \alpha_j))\right|.$$

*Moreover $\mathfrak{D}^2$ is the two-sided ideal of $\mathcal{O}$ generated by $d(\mathcal{O})$.*

**Proof.** All but the last statement is contained in Vignéras [34, Chapitre I, Lemme 4.7]. Since $\mathfrak{D}$ divides exactly the ramifying primes, each of which have ramification index two, its square is principal.

**Proposition 42** *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders such that $\mathcal{O} \subseteq \mathcal{O}'$. Then $d(\mathcal{O})$ divides $d(\mathcal{O}')$ and $d(\mathcal{O}) = d(\mathcal{O}')$ if and only if $\mathcal{O} = \mathcal{O}'$. An order $\mathcal{O}$ is maximal if and only if $d(\mathcal{O})$ is the product of the finite primes of $\mathbb{Q}$ ramifying in $\mathfrak{A}$.*

**Proof.** This is the content of [34, Chapitre I, Corollaire 4.8] and [34, Chapitre III, Corollaire 5.3].

Suppose $I$ and $J$ are two-sided ideals for an order $\mathcal{O}$. Then we can compose $I$ and $J$ in the Brandt groupoid of $\mathfrak{A}$ to obtain a two-sided ideal $IJ$ of $\mathcal{O}$. Suppose $I = J\alpha$ for some $\alpha$ in $\mathfrak{A}^*$. The right orders of $I$ and $J$ are equal to $\mathcal{O}$, so $\mathcal{O} = \alpha^{-1}\mathcal{O}\alpha$. Thus $\alpha$ lies in the normalizer $\mathbf{N}(\mathcal{O})$ of $\mathcal{O}$.

**Proposition 43** *Conjugation by $\mathfrak{N}(\mathcal{O})$ is trivial on the set of two-sided ideals of $\mathcal{O}$. Thus the class group $\mathrm{Cl}(\mathcal{O})$ of two-sided ideals modulo principal two-sided ideals is well-defined, and isomorphic to $\mathcal{U}(\mathcal{O})\backslash\mathfrak{N}(\mathcal{O})/\mathbf{N}(\mathcal{O})$ via the homomorphism $s \mapsto \mathcal{O}s$. The class group of $\mathcal{O}$ is a quotient of the free $\mathbb{Z}/2\mathbb{Z}$-module generated by the two-sided prime ideals lying over the finite primes of $\mathbb{Q}$ ramifying in $\mathfrak{A}$.*

**Proof.** By Proposition 33, the two-sided ideals of $\mathcal{O}_p$ are generated freely by the unique two-sided ideal $\mathfrak{P}$ lying over $p$. If $p$ splits in $\mathcal{O}$, then $\mathfrak{P}$ is generated by $p$.

Otherwise $\mathfrak{P}$ is a principal ideal with $\mathfrak{P}^2 = (p)$. If $\pi_p$ is a generator for $\mathfrak{P}$, then $\mathbf{N}(\mathcal{O}_p) = \mathbb{Q}_p^*\langle\pi_p\rangle$. In either case, the normalizer stabilizes two-sided ideals of $\mathcal{O}_p$, so the action of $\mathfrak{N}(\mathcal{O})$ is trivial. The final statement follows from the surjection

$$\bigoplus_{p|d(\mathcal{O})} \mathbb{Z}/2\mathbb{Z} \cong \mathcal{U}(\mathcal{O})\backslash\mathfrak{N}(\mathcal{O})/\mathbb{Q}^* \longrightarrow \mathcal{U}(\mathcal{O})\backslash\mathfrak{N}(\mathcal{O})/\mathbf{N}(\mathcal{O}) \cong \mathrm{Cl}(\mathcal{O}).$$

This completes the proof.

## 5.3 An equivalence of categories

In order to relate the arithmetic of quaternion algebras to supersingular elliptic curves over finite fields, we describe an explicit equivalence of two categories. One is a category of modules over a maximal order in a quaternion algebra $\mathfrak{A}$. The other is a category of supersingular elliptic curves over a finite field $k$. Let $\mathfrak{A}$ be the unique quaternion algebra over $\mathbb{Q}$, up to isomorphism, ramified exactly at one finite prime $p$ and at $\infty$. Deuring proves in his classic article [6, §10.2] a bijection between the set of two-sided ideal classes for each of the types of maximal order in $\mathfrak{A}$, and the $j$-invariants of supersingular elliptic curves in an algebraically closed field of characteristic $p$. The statement of his result is as follows.

**Theorem 44** *Given a type of maximal order, there exist one or two supersingular $j$-invariants such that the corresponding endomorphism ring is of the given type. If the prime ideal $\mathfrak{P}$ over $p$ is principal then $j$ is rational over the prime field; otherwise there are two such $j$-invariants, constituting a conjugate pair in a quadratic field extension of the prime field.*

In Waterhouse [35] one finds a description of this correspondence for finite fields in terms of kernel ideals. This correspondence has been exploited in various forms (see [20]) for computations with elliptic curves and modular forms. The purpose of this section is to describe an explicit and functorial version of this correspondence.

Throughout we fix a finite field $k$ of $q$ elements and characteristic $p$, and we let $\mathfrak{A}$ be the quaternion algebra over $\mathbb{Q}$ ramified at $p$ and $\infty$, and let $\mathcal{O}$ be a maximal order in $\mathfrak{A}$ containing an element of reduced norm $q$.

We define $\mathbf{S}_k$ to be the category of supersingular elliptic curves over $k$. The objects of $\mathbf{S}_k$ are defined to be pairs $(E, \pi)$, where $E$ is a supersingular elliptic curve over $k$ and $\pi$ is the Frobenius endomorphism relative to $k$. A morphism of objects $(E_1, \pi_1)$ to $(E_2, \pi_2)$ is defined to be a homomorphism $\psi : E_1 \longrightarrow E_2$ such that $\psi \circ \pi_1 = \pi_2 \circ \psi$.

Before proceeding, we make some algebraic definitions for modules over $\mathcal{O}$. We define the rank of a projective module $P$ over $\mathcal{O}$ to be the smallest integer $r$ such that $P$ embeds in a free $\mathcal{O}$ module of rank $r$. Let $I$ and $J$ be right projective modules over

$\mathcal{O}$ of rank one, and let $\phi : I \longrightarrow J$ be a homomorphism of right modules. Both $I$ and $J$ are locally free, so for each prime $l$ we can find $x_l \in I_l$ and $y_l \in J_l$ such that $I_l = x_l\mathcal{O}_l$ and $J_l = y_l\mathcal{O}_l$. Then the image of $x_l$ under $\phi \otimes 1_{\mathbb{Z}_l}$ is $x_l\alpha_l$ for some $\alpha_l \in \mathcal{O}_l$. Define the *reduced norm* of $\phi$ to be the product

$$\mathrm{N}(\phi) = \prod_l |\mathbb{Z}_l/\mathrm{N}(a_l)\mathbb{Z}_l| \,.$$

We now define $\mathbf{M}_{\mathcal{O},q}$ as a category of projective right modules of rank one over $\mathcal{O}$. The objects of $\mathbf{M}_{\mathcal{O},q}$ are defined to be pairs $(I, \phi)$ such that $I$ is a projective right module of rank one over $\mathcal{O}$ and $\phi$ is an endomorphism of $I$ of reduced norm $q$. A morphism of objects $(I_1, \phi_1)$ and $(I_2, \phi_2)$ is defined to be a homomorphism $\psi : I_1 \longrightarrow I_2$ such that $\psi \circ \phi_1 = \phi_2 \circ \psi$.

We define a functor $\mathbf{I}$ from $\mathbf{S}_k$ to $\mathbf{M}_{\mathcal{O},q}$ as follows. By Theorem 44, there exists an elliptic curve $E_0$ over $k$ with $\mathcal{O} \cong \mathrm{End}(E_0)$. We fix such a curve and identify its endomorphism ring with $\mathcal{O}$. The functor $\mathbf{I}$ takes an object $(E, \pi)$ to an object $(\mathbf{I}(E), \mathbf{I}(\pi))$, where $\mathbf{I}(E) = \mathrm{Hom}(E_0, E)$ and $\mathbf{I}(\pi) = \tau_\pi$ is the homomorphism of $\mathrm{Hom}(E_0, E)$ to itself given by left composition by $\pi$. For any morphism $\psi$ of objects $(E_1, \pi_1)$ to $(E_2, \pi_2)$ there is a well-defined morphism $\mathbf{I}(\psi) = \tau_\psi$ which is the right $\mathcal{O}$-module homomorphism

$$\tau_\psi : \mathrm{Hom}(E_0, E_1) \longrightarrow \mathrm{Hom}(E_0, E_2)$$

given by left composition by $\psi$, which satisfies the condition that $\tau_\psi \circ \tau_{\pi_1} = \tau_{\pi_1} \circ \tau_\psi$. The main result of this section is the following theorem.

**Theorem 45** *The functor* $\mathbf{I}$ *is an equivalence from* $\mathbf{S}_k$ *to* $\mathbf{M}_{\mathcal{O},q}$.

**Remark.** One could easily have defined the category $\mathbf{M}_{\mathcal{O},q}$ to be a category of projective *left* modules of rank one over $\mathcal{O}$. These two categories are dual to one another, in the sense that there is a contravariant equivalence of categories between the two. The definition of $\mathbf{M}_{\mathcal{O},q}$ as a category of right modules ensures that the functor $\mathbf{I}$ is a covariant functor from $\mathbf{S}_k$ to $\mathbf{M}_{\mathcal{O},q}$.

**Proof of Theorem 45.** By Theorem IV.4.1 of MacLane [19], to prove that $\mathbf{I}$ is an equivalence it is sufficient and necessary to prove that $\mathbf{I}$ is full and faithful, and each object of $\mathbf{M}_{\mathcal{O},q}$ is isomorphic to an object in the image of $\mathbf{I}$.

First we show that $\mathbf{I}$ is a full and faithful functor from $\mathbf{S}_k$ to $\mathbf{M}_{\mathcal{O},q}$.

**Definition.** Let $J$ be a set of isogenies of $E$. Then we define $E[J]$ to be the scheme theoretic intersection of the kernels of all $\alpha$ in $J$. A left $\mathcal{O}$-ideal $I$ is called a *kernel ideal* if $I = \{\alpha \in \mathcal{O} | \alpha(E[I]) = \mathrm{O}\}$.

**Theorem 46** *Every left* $\mathcal{O}$*-ideal is a kernel ideal, and every finite subgroup of* $E$ *is of the form* $E[I]$ *for some left* $\mathcal{O}$*-ideal* $I$*. The rank of* $E[I]$ *is the reduced norm of* $I$*.*

**Proof.** Waterhouse (Theorem 3.15 [35]).

We also need the following standard result.

**Lemma 47** *Let $\phi : E \to E'$ and $\psi : E \to E''$ be isogenies and suppose that $\psi \ker(\phi) = \mathbf{O}$. Then there exists an isogeny $\varrho : E'' \to E'$ such that $\psi = \varrho\phi$.*

**Proposition 48** *Let $I \subseteq \mathrm{Hom}(E', E)$ be a left module over $\mathcal{O} = \mathrm{End}(E)$, and let $J \subseteq \mathrm{Hom}(E, E')$ be a right $\mathcal{O}$-module. Then there exists an elliptic curve $E''$ and an isogeny $\varrho : E'' \to E'$ such that $I = \mathrm{Hom}(E'', E)\varrho$. Likewise there exists an elliptic curve $E''$ and an isogeny $\sigma : E'' \to E$ such that $J = \sigma \mathrm{Hom}(E, E'')$.*

**Proof** By means of any isogeny $\phi : E \to E'$, there exist embeddings of $I$ and $\mathrm{Hom}(E', E)$ in $\mathcal{O}$ as integral ideals such that

$$I\phi \subseteq \mathrm{Hom}(E', E)\phi \subseteq \mathcal{O}.$$

Let $E'' = E/E[I\phi]$ and let $\psi : E \to E''$ be the isogeny with kernel $E[I\varrho]$. By Theorem 46 and Lemma 47,

$$I\phi = \{\alpha \in \mathcal{O} : \alpha(E[I\phi]) = \mathbf{O}\} = \mathrm{Hom}(E'', E)\psi,$$

so $I = \mathrm{Hom}(E'', E)\varrho$. The result holds for $J$ by taking duals.

**Proposition 49** *The functor $\mathbf{I}$ from $\mathbf{S}_k$ to $\mathbf{M}_{\mathcal{O},q}$ is full and faithful.*

**Proof.** It is clear that $\mathbf{I}$ is faithful. To prove that $\mathbf{I}$ is full, we need to show that every right $\mathcal{O}$-module homomorphism $\psi$ of $\mathrm{Hom}(E_0, E_1)$ to $\mathrm{Hom}(E_0, E_2)$ arises by composing on the left with an isogeny $\sigma : E_1 \to E_2$. From the previous proposition, the image of $\psi$ in $\mathrm{Hom}(E_0, E_2)$ is of the form $\sigma \mathrm{Hom}(E_0, E_1)$. Comparing $\psi$ with left multiplication by $\sigma$, the two $\mathcal{O}$-module homorphisms differ only up to a unit in the left order $\mathcal{O}_1 = \mathrm{End}(E_1)$ of $\mathrm{Hom}(E_0, E_1)$. Thus by multiplying $\sigma$ by a unit $\psi = \tau_\sigma$ has the required form. The equivalence of the commutativity relations $\psi \circ \tau_{\pi_1} = \tau_{\pi_1} \circ \psi$ and $\sigma \circ \pi_1 = \pi_1 \circ \sigma$ is trivially verified.

To complete the proof of Theorem 45, it remains only to show that every object $(I, \phi)$ is isomorphic to one of the form $(\mathbf{I}(E_1), \mathbf{I}(\pi))$. First we introduce the definition of a *hereditary* ring. We define a ring $\mathfrak{O}$ to be hereditary if every one-sided ideal of $\mathfrak{O}$ is projective. Let $R$ be a Dedekind domain with field of fractions $K$, and let $\mathfrak{B}$ be an algebra over $K$, in which $\mathfrak{O}$ is an order containing $R$. Then by Theorem 40.5 of Reiner [25], the ring $\mathfrak{O}$ is hereditary if and only if $\mathfrak{O}_\mathfrak{l}$ is hereditary for all maximal ideals $\mathfrak{l}$ of $R$. Every ideal in a maximal order in a definite quaternion algebra over $\mathbb{Q}$ is locally free at all finite primes $l$ of $\mathbb{Z}$, so it follows that $\mathcal{O}$ is hereditary. Thus a module $P$ over $\mathcal{O}$ is projective of rank one if and only if $P$ is isomorphic to an ideal of $\mathcal{O}$.

Let $(I, \phi)$ be an object in $\mathbf{M}_{\mathcal{O},q}$. Since $\mathcal{O}$ is hereditary we can embed $I$ as a right ideal in $\mathcal{O} = \mathrm{End}(E_0)$. Then $I \cong \sigma \mathrm{Hom}(E_0, E'')$ by Proposition 48, and so $I \cong \mathrm{Hom}(E_0, E'')$. Under this isomorphism, $\phi : I \longrightarrow I$ induces a homomorphism of right $\mathrm{End}(E_0)$-modules

$$\mathrm{Hom}(E_0, E'') \longrightarrow \mathrm{Hom}(E_0, E'')$$

of norm $q$, and by Proposition 48 this map is given by left composition by an element $\pi_1$ of $\mathrm{End}(E'')$. A theorem of Honda [10] asserts that there exists an elliptic curve $E_1$ and an isomorphism to $E''$ over some extension of $k$ such that the Frobenius endomorphism maps to $\pi_1$ under the isomorphism of endomorphism rings. This completes the proof of Theorem 45.

# Chapter 6

# Quadratic spaces

The equivalence of categories of the preceding section carries over not only the structure of maps of objects in the respective categories, but also relates the additional structure of the degree map on isogenies to the reduced norm on morphisms of projective modules over $\mathcal{O}$. As a $\mathbb{Z}$-module, $\mathrm{Hom}(E_1, E_2)$ has rank four, and the degree map gives $V = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$ the structure of a quadratic space over $\mathbb{Q}$ in which $\mathrm{Hom}(E_1, E_2)$ is an integral lattice. In this section, we will give the necessary definitions, and consider this quadratic space structure.

## 6.1 Introduction to quadratic spaces

We recall that *quadratic space* $(V, \Phi)$ over a field $F$ of characteristic different from 2 is a finite dimensional $F$-vector space $V$ with a symmetric bilinear form $\Phi : V \times V \to F$. From the bilinear form $\Phi$ we can define a function $\mathbf{q} : V \to F$ by

$$\mathbf{q}(v) = \frac{1}{2}\Phi(v, v).$$

The symmetric bilinear form $\Phi$ can be recovered from $\mathbf{q}$ by setting

$$\Phi(u, v) = \mathbf{q}(u + v) - \mathbf{q}(u) - \mathbf{q}(v).$$

Thus we may equivalently denote the quadratic space $(V, \Phi)$ by $(V, \mathbf{q})$. For any such form $\mathbf{q}$ on $V$ we call $\Phi$ the bilinear form associated to $\mathbf{q}$, and call $\mathbf{q}$ the quadratic map associated to $\Phi$. Except where explicitly noted, we restrict to *regular* quadratic spaces. A quadratic space is said to be regular if for every $v$ in $V$, the condition that $\Phi(u, v) = 0$ for all $u$ in $V$ implies $v = 0$. Otherwise we say that $(V, \mathbf{q})$ is *singular*.

Let $R$ be an integral domain with field of fractions $F$, and let $\Lambda$ be a *lattice* over $R$ in $V$, i.e. a finitely generated $R$-submodule of $V$ containing a basis for $V$ over $F$. If $\mathbf{q}(\Lambda)$ is contained in $R$ we say that $(\Lambda, \mathbf{q})$ is a *quadratic module* over $R$. If $\Phi(\Lambda, \Lambda)$ is

contained in $R$ we say that $(\Lambda, \Phi)$ is a *bilinear module* over $R$. If, moreover, $\Phi(v, v)$ lies in $2R$ for all $v$ in $\Lambda$, we say that $(\Lambda, \Phi)$ is *even*. From the definition of the quadratic form $\mathbf{q}$ associated to $\Phi$, it is clear that there is a bijective correspondence between even bilinear modules over $R$ and quadratic modules over $R$.

A *quadratic form* is defined to be a degree two homogeneous polynomial in $n$ variables. For each choice of basis $\{v_1, v_2, \ldots, v_n\}$ for $V$ over $F$ the quadratic space determines a quadratic form $f(\mathbf{x})$ over $F$, given by

$$f(\mathbf{x}) = \mathbf{q}(x_1 v_1 + x_2 v_2 + \cdots + x_n v_n) = \sum_{i \leq j} f_{ij} x_i x_j,$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. If $\{v_1, v_2, \ldots, v_n\}$ is a basis over $R$ for a quadratic module $\Lambda$ over $R$ then $f(\mathbf{x})$ is a quadratic form over $R$. If $R$ is a principal ideal domain, then every quadratic module has a basis. The ideal $\mathfrak{a}$ generated by the coefficients of a quadratic form $f(\mathbf{x})$ is defined to be the *content* of $f(\mathbf{x})$. If $R$ is a principal ideal domain, then we will say that $f(\mathbf{x})$ has content $a$ if the ideal $\mathfrak{a}$ equals $aR$. If the content of a quadratic form $f(\mathbf{x})$ is equal to 1, then we say that $f$ is *proper*. More generally we define the content of a quadratic module $(\Lambda, \mathbf{q})$ to be the ideal $\mathfrak{a}$ generated by $\mathbf{q}(v)$ for all $v$ in $\Lambda$, and say $(\Lambda, \mathbf{q})$ has content $a$ if $\mathfrak{a}$ is generated by $a$. A quadratic module is said to be proper if it has content 1. Similarly we define the content of a bilinear module $(\Lambda, \Phi)$ to be the ideal generated by $\Phi(u, v)$ for all $u$ and $v$ in $\Lambda$, and say that $(\Lambda, \Phi)$ is proper over $R$ if it has content 1. Note that the content of a quadratic form contains the content of the associated bilinear form, and the condition that $(\Lambda, \Phi)$ is even does not imply that the content is contained in the ideal $2R$.

Let $(\Lambda_1, \mathbf{q}_1)$ and $(\Lambda_2, \mathbf{q}_2)$ be quadratic modules over an integral domain $R$. A *representation* of $(\Lambda_1, \mathbf{q}_1)$ by $(\Lambda_2, \mathbf{q}_2)$ is a homomorphism of $R$-modules

$$\sigma : \Lambda_1 \longrightarrow \Lambda_2$$

such that $\mathbf{q}_2(\sigma(v)) = \mathbf{q}_1(v)$ for all $v$ in $\Lambda_1$. If $\sigma$ is an isomorphism of the underlying $R$-modules, we call the representation an *isometry*. If a quadratic module $(\Lambda, \mathbf{q})$ contains an element $v \in \Lambda$ such that $\mathbf{q}(v) = m$, we say that $(\Lambda, \mathbf{q})$ represents $m$.

A *similitude* is a homomorphism $\sigma : \Lambda_1 \to \Lambda_2$ of $R$-modules which satisfies the weaker condition that

$$\mathbf{q}_2(\sigma(v)) = c \cdot \mathbf{q}_1(v),$$

for some $c$ in $F^*$. The factor $c$ is termed the similitude factor of $\sigma$. If there exists a similitude $\sigma : \Lambda_1 \to \Lambda_2$ which is an isomorphism of the underlying $R$-modules, then $(\Lambda_1, \mathbf{q}_1)$ and $(\Lambda_2, \mathbf{q}_2)$ are said to be *similar*. A representation or similitude $\sigma : \Lambda_1 \to \Lambda_2$ such that the $R$-module $\Lambda_2/\sigma(\Lambda_2)$ is torsion-free is said to be *primitive*.

**Example.** Let $E_1$ and $E_2$ be isogenous elliptic curves. Let $\Lambda = \mathrm{Hom}(E_1, E_2)$ with the quadratic map deg, which assigns to each isogeny its degree. The associated bilinear

map

$$\Phi(\phi, \psi) = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

on isogenies $\phi$ and $\psi$, can be extended by linearity to all of $V = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$. Then $(\Lambda, \mathbf{q}) = (\mathrm{Hom}(E_1, E_2), \deg)$ is a quadratic module over $\mathbb{Z}$ contained in $V$. Let $E_0$ be a fixed elliptic curve isogenous to $E_1$ and $E_2$. Then we define $\Lambda(E_i)$ to be $\mathrm{Hom}(E_0, E_i)$ and $V(E_i)$ to be $\mathrm{Hom}(E_0, E_i) \otimes \mathbb{Q}$. If $\psi : E_1 \to E_2$ is an isogeny, then the map $V_\psi : V(E_1) \to V(E_2)$ given by $\phi \mapsto \psi\phi$ is a $\mathbb{Q}$-vector space homomorphism $V(E_1)$ to $V(E_2)$ which takes $\Lambda(E_1)$ to $\Lambda(E_2)$ such that

$$\mathbf{q}_2(V_\psi(\phi)) = \deg(\psi) \cdot \mathbf{q}_1(\phi),$$

hence $V_\psi$ is a similitude with similitude factor $\deg(\psi)$. However the quadratic modules $(\Lambda(E_1), \mathbf{q}_1)$ and $(\Lambda(E_2), \mathbf{q}_2)$ in general are not similar.

**Definition.** Let $(\Lambda, \Phi)$ be a bilinear module over $R$, and let $\{v_1, v_2, \ldots, v_n\}$ be a basis for $\Lambda$ over $R$. Then the *determinant* of $\Lambda$, denoted $\det(\Lambda)$, is defined to be $\det(\Phi(v_i, v_j))$. The determinant of a quadratic module $(\Lambda, \mathbf{q})$ is defined to be the determinant with respect to the bilinear form $\Phi$ associated to $\mathbf{q}$. The determinant is nonzero if and only if $(\Lambda, \Phi)$ is regular. The determinant is not independent of the choice of basis. However, $\det(\Lambda)$ is well-defined modulo $R^{*2}$. Under inclusion of bilinear modules, the determinant behaves as indicated in the following proposition.

**Proposition 50** *Let* $(\Lambda_1, \mathbf{q}_1)$ *and* $(\Lambda_2, \mathbf{q}_2)$ *be regular quadratic modules over* $R$ *such that* $\Lambda_1$ *and* $\Lambda_2$ *are free of rank* $n$ *over* $R$. *If* $\Lambda_1 \subseteq \Lambda_2$ *then* $\det(\Lambda_2)$ *divides* $\det(\Lambda_1)$. *If also* $\det(\Lambda_1) = \det(\Lambda_2) \bmod R^{*2}$, *then* $\Lambda_1 = \Lambda_2$.

**Proof.** Let $\{u_1, u_2, \ldots, u_n\}$ be a basis for $\Lambda_2$ and $\{v_1, v_2, \ldots, v_n\}$ a basis for $\Lambda_1$. Then

$$v_j = \sum_i r_{ij} u_i,$$

for some $r_{ij}$ in $R$. Setting $M = (r_{ij})$, we have

$$\begin{aligned} \det(\Lambda_1) &= \det(\Phi(v_i, v_j)) = \det(\sum_l \sum_k r_{li} \Phi(u_l, u_k) r_{kj}) \\ &= \det(M^t(\Phi(u_l, u_k))M) = (\det(M))^2 \det(\Lambda_2). \end{aligned}$$

Thus $\det(\Lambda_1)$ divides $\det(\Lambda_2)$. If equality holds modulo $R^{*2}$, then $M$ is invertible and $\Lambda_1 = \Lambda_2$.

Now we specialize to the quadratic spaces and modules derived from quaternion algebras. Let $\mathfrak{A}$ be a definite quaternion algebra over $\mathbb{Q}$, and let $\mathcal{O}$ be a maximal order in $\mathfrak{A}$. For any left projective rank one module $I$ over $\mathcal{O}$ we can define a reduced norm map from the reduced norm on $\mathcal{O}$. For each finite prime $l$, fix a generator $x_l$

for $I_l$ as an $\mathcal{O}_l$ module. Then each $x$ in $I$ is of the form $\alpha_l x_l \in I_l$ for some $\alpha_l$ in $\mathcal{O}_l$. Since $x_l$ is defined only up to an element of $\mathcal{O}_l^*$, and $\mathrm{N}(\mathcal{O}_l^*) = \mathbb{Z}_l^*$, we define $\mathrm{N}(x) = \mathrm{N}(\alpha_l) \bmod \mathbb{Z}_l^*$. Since $\mathfrak{A}$ is definite, at the infinite prime, the image of the reduced norm on $\mathfrak{A} \otimes \mathbb{R}$ is contained in $\mathbb{R}_{\geq 0}$. Thus we define $\mathrm{N}(x)$ to be the unique positive generator of

$$\bigcap_l (\mathrm{N}(\alpha_l)\mathbb{Z}_l \cap \mathbb{Z}) .$$

**Proposition 51** *Let $\mathcal{O}$ be a maximal order in a definite quaternion algebra over $\mathbb{Q}$ and let $I$ be a projective rank one left module over $\mathcal{O}$ with the quadratic map defined by the reduced norm on $I$. The determinant of $I$ is $d(\mathcal{O})^2$, and any isomorphism of $I$ with an ideal $J$ of $\mathcal{O}$ determines a similitude $\sigma : I \to \mathcal{O}$ with similitude factor $\mathrm{N}(J)$.*

**Proof.** The reduced norm on $I$ is defined using the local isomorphism $I_l \cong \mathcal{O}_l$. Thus $\det(I_l) = \det(\mathcal{O}_l) \bmod \mathbb{Z}_l^{*2}$ for all $l$ and the two determinants are equal. By Proposition 41, both determinants are then equal to $d(\mathcal{O})^2$. The reduced norm on $\mathcal{O}$, restricted to elements of $J$ is $\mathrm{N}(J)$ times the reduced norm on $J$ defined via its left $\mathcal{O}$-module structure. Thus an isomorphism of $I$ with $J$ defines a similitude with factor $\mathrm{N}(J)$.

## 6.2 Clifford algebras

Let $R$ be an integral domain with field of fractions $F$. Let $(\Lambda, \mathbf{q})$ be a quadratic module over $R$, and $V = \Lambda \otimes F$ be the quadratic space containing it. An injective homomorphism of $R$-modules $\iota : \Lambda \to A$ of $\Lambda$ in an $R$-algebra $A$ is said to be *compatible* with $\mathbf{q}$ if $\iota(v)^2 = \mathbf{q}(v) \cdot 1$. An $R$-algebra $C = C(\Lambda)$ with an injection $\iota_C : \Lambda \to C$ compatible with $\mathbf{q}$ is said to be a *Clifford algebra* for $(\Lambda, \mathbf{q})$ if for any $R$-algebra $A$ and $R$-module monomorphism $\iota_A : \Lambda \to A$, there exists a unique $R$-algebra homomorphism $\phi : C(\Lambda) \to A$ such that $\phi \circ \iota_C = \iota_A$. The Clifford algebra of $(\Lambda, \Phi)$ exists and can be constructed as the quotient of the tensor algebra $\mathrm{T}(\Lambda) = \bigoplus_i \mathrm{T}^i(V)$ of $\Lambda$ by the relations $v \otimes v - \mathbf{q}(v)$, with $\iota$ defined to be the isomorphism of $\Lambda$ with $\mathrm{T}^1(\Lambda)$. Hereafter, where convenient, we will identify $\Lambda$ with its image in $C(\Lambda)$ and omit the reference to $\iota$. The relations $v \otimes v - \mathbf{q}(v)$ generating the kernel of the surjection $\mathrm{T}(\Lambda) \to C(\Lambda)$ lie in $\bigoplus_i \mathrm{T}^{2i}(\Lambda)$. Thus the $\mathbb{Z}$-grading on $\mathrm{T}(\Lambda)$ in the construction of the Clifford algebra, descends to a $\mathbb{Z}/2\mathbb{Z}$-grading on $C(\Lambda)$, and we have a decomposition of $R$-modules $C(\Lambda) = C_0(\Lambda) \oplus C_1(\Lambda)$, where $C_0(\Lambda)$ is the even part of $C(\Lambda)$ and $C_1(\Lambda)$ is the odd part. The ring $C_0(\Lambda)$ is called the even Clifford algebra of $(\Lambda, \Phi)$. The Clifford algebra of the quadratic space $(V, \mathbf{q})$ is defined to be the Clifford algebra $C(V)$ of $(V, \mathbf{q})$ as a quadratic module over $F$.

The Clifford algebra of a quadratic module is well-behaved under extension of the base ring.

**Proposition 52** *Let $(\Lambda, \mathbf{q})$ be a quadratic module over $R$ and let $C(\Lambda)$ be its Clifford algebra. Let $R \to S$ be an injection of rings. Then the Clifford algebra $C(\Lambda_S)$ of the extended quadratic module $\Lambda_S = \Lambda \otimes S$ is $C(\Lambda)_S = C(\Lambda) \otimes S$.*

**Proof.** From the inclusion $\Lambda \subseteq \Lambda_S$ there is a unique homomorphism $C(\Lambda) \to C(\Lambda_S)$. From the universal property of the tensor product, this determines a unique homomorphism $C(\Lambda)_S \to C(\Lambda_S)$. Conversely, both $C(\Lambda)_S$ and $C(\Lambda_S)$ contain $\Lambda_S$, so there is a unique map of $C(\Lambda_S)$ to $C(\Lambda)_S$. By the universal property for the Clifford algebra, the composites of these maps is the identity on each of $C(\Lambda)_S$ and $C(\Lambda_S)$.

Of particular interest is the case when $\mathfrak{p}$ is a prime and $S$ is the localization of $R$ at $\mathfrak{p}$. We will also need several results on the structure of the Clifford algebra over a field $k$ and over an integral domain $R$.

**Theorem 53** *The dimension of the Clifford algebra of a dimension $n$ quadratic space $V$ over a field $F$ is $2^n$. If $\Lambda$ is a quadratic module free of rank $n$ over $R$, then $C(\Lambda)$ is free of rank $2^n$ over $R$.*

**Proof.** This appears in Lam [15] for $R$ a field. The same argument implies that a basis for $C(\Lambda)$ over $R$ is $v_1^{e_1} v_2^{e_2} \dots v_n^{e_n}$, where $\{v_i\}$ is a basis for $\Lambda$ over $R$ and $0 \leq e_i \leq 1$.

**Corollary 54** *The dimension of $C_0(V)$ and the dimension of $C_1(V)$ are equal to $2^{n-1}$. The $R$-algebra $C(\Lambda)$ is an order in $C(V)$, and the $R$-algebra $C_0(\Lambda)$ is an order in $C_0(V)$.*

**Proof.** The dimensions of $C_0(V)$ and $C_1(V)$ are equal since $C_1(V)$ is equal to $vC_0(V)$ for any $v$ in $V$. Comparison of the ranks of the subrings $C(\Lambda)$ and $C_0(\Lambda)$ over $R$ yields the result that these are indeed orders in $C(V)$ and $C_0(V)$.

**Proposition 55** *There exists a unique algebra involution $\varepsilon : C(\Lambda) \to C(\Lambda)$ which is the identity on $\Lambda$. Moreover, $\varepsilon$ stabilizes both $C_0(\Lambda)$ and $C_1(\Lambda)$.*

**Proof.** This follows from [15, Proposition 5.1.11] for the Clifford algebra over a field.

We can also state the following structure theorem for the Clifford algebra of an even dimensional quadratic space $V$.

**Theorem 56** *Suppose* $\dim(V) = n$ *is even. Then*

1. *$C(V)$ is a central simple algebra over $F$, isomorphic to $\mathbb{M}_t(D)$ for some central division algebra $D$ over $F$.*
2. *If $d = \det(V)$ is nontrivial in $F^*/F^{*2}$ then $C_0(V)$ is a central simple algebra over $k(\sqrt{d})$.*
3. *If $\det(V)$ is trivial in $F^*/F^{*2}$, then the center of $C_0(V)$ is isomorphic to $F \times F$ and $C_0(V)$ is isomorphic to $\mathbb{M}_r(D) \times \mathbb{M}_r(D)$ where $2r = t$*

**Proof.** Lam [15, Theorem 5.2.5].

## 6.3 Quadratic modules of quaternions

Hereafter we will restrict to the study of four dimensional regular quadratic spaces $V$ over $F$ such that $\det(V)$ is trivial in $F^*/F^{*2}$. By Theorem 56, the $F$-algebra $C(V)$ is isomomorphic to a matrix algebra over a quaternion algebra $\mathfrak{A}$, which may be split, and $C_0(V)$ is isomorphic to a product of two copies of $\mathfrak{A}$. This will enable us to characterize the quadratic modules arising from projective modules over orders in $\mathfrak{A}$.

This work was inspired in part by the article of Isabelle Pays [22], in which she analyzes the integral Clifford algebra $C(\Lambda)$ in order to answer the question of whether a given quadratic module over $\mathbb{Z}$ arises as the norm form of an order in a quaternion algebra. We consider the module structure of a general quadratic module $\Lambda$ in the Clifford algebra to deduce similar results.

We continue with the dissection of the Clifford algebra. The even Clifford algebra $C_0(V)$ splits into a product of two quaternion algebras over $F$. We let $e$ and $f$ be the two nontrivial central idempotents of $C_0(V)$.

**Proposition 57** *The involution $\varepsilon$ on $C(V)$ fixing $V$ is the identity on the center of $C_0(V)$ and takes $eV$ to $Ve$. The submodules $Ve$ and $fV$ are equal, as are $eV$ and $Vf$.*

**Proof.** We follow the proof of Theorem V.2.5 of Lam [15]. Let $\{v_1, v_2, v_3, v_4\}$ be an orthogonal basis of $V$, so that $v_i$ and $v_j$ anticommute in $C(V)$ for all $i \neq j$. Set $z = v_1v_2v_3v_4$, so that $z^2 \bmod F^{*2}$ is the determinant of $V$. Since $\det(V)$ is a square, we may scale $v_1$ by an element of $F^*$ and assume that $z^2 = 1$. Then we define $e = (1+z)/2$ and $f = (1-z)/2$, and verify directly that $e$ and $f$ are the nontrivial central idempotents of $C_0(V)$. But also

$$\varepsilon(z) = v_4v_3v_2v_1 = v_1v_2v_3v_4 = z,$$

so $e$ and $f$ are fixed by $\varepsilon$. Thus the center $Fe \times Ff$ of $C_0(V)$ is fixed by $\varepsilon$. Since $\varepsilon$ is an involution, $\varepsilon(eV) = Ve$ and $\varepsilon(Vf) = fV$. Since the orthogonal element $v_i$ anticommutes with $v_j$ for $j \neq i$, from the definition of $z$, we have $v_iz = -zv_i$. Thus $ve = fv$ for all $v$ in $V$, and likewise $vf = ev$.

**Proposition 58** *The subrings $\mathfrak{A}_1 = C_0(V)e = eC_0(V)$ and $\mathfrak{A}_2 = C_0(V)f$ of $C_0(V)$ are quaternion algebras over $F$ with unity elements $e$ and $f$ respectively. Conjugation on $\mathfrak{A}_1$ and on $\mathfrak{A}_2$ are the restrictions of the involution $\varepsilon$ of $C_0(V)$. In particular the reduced norms on $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are given by $\alpha \mapsto \alpha\,\varepsilon(\alpha)$.*

**Proof.** The subrings $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are quaternion algebras over $F$ by Theorem 56. Every involution of a quaternion algebra $\mathfrak{A}$ is equivalent to the conjugation involution on $\mathfrak{A}$ up to an inner automorphism. It suffices to show that $\varepsilon$ has the additional property

that $\alpha\,\varepsilon(\alpha)$ lies in $F$ for all $\alpha$ in $\mathfrak{A}$. But this follows directly from the generating relations $v^2 = \mathbf{q}(v)$ for all $v$ in $V$ and the fact that $\varepsilon$ is the identity on $V$.

**Definition.** Let $\Lambda$ be a left module over an order $\mathcal{O}$ in a quaternion algebra $\mathfrak{A}$ with reduced norm N and let $\mathbf{q} : \Lambda \longrightarrow R$ be a quadratic map on $\Lambda$. We say that tthe left module structure of $\Lambda$ is compatible with the quadratic map $\mathbf{q}$ if $\mathbf{q}(\alpha v) = \mathrm{N}(\alpha)\,\mathbf{q}(v)$ for all $\alpha$ in $\mathcal{O}$ and all $v$ in $\Lambda$. Likewise for a left module $V$ over $\mathfrak{A}$ we say that the left module structure is compatible with a quadratic map $\mathbf{q} : V \longrightarrow F$ if $\mathbf{q}(\alpha v) = \mathrm{N}(\alpha)\,\mathbf{q}(v)$ for all $\alpha$ in $\mathfrak{A}$ and all $v$ in $V$.

**Proposition 59** *The odd part of $C_1(V)$ decomposes as $eV \oplus fV$. The quadratic space structure of the decomposition can be summarized as follows.*

1. *The composite map*

$$V \longrightarrow C_1(V) \longrightarrow eC_1(V) = eV$$

*is an isometry with the quadratic map on $eV$ defined by $\mathbf{q}(ev) = ev\,\varepsilon(ev)$, and equips $V$ with the structure of a left $\mathfrak{A}_1$-module and right $\mathfrak{A}_2$-module, compatible with the reduced norm* N.

2. *For every $u$ in $V$ there exists a similitude*

$$\sigma_u : V \longrightarrow \mathfrak{A}_1$$

*of $(V, \mathbf{q})$ to $(\mathfrak{A}_1, \mathrm{N})$ with similitude factor $\mathbf{q}(u)$, defined by $v \mapsto ev\,\varepsilon(eu)$. In particular, if $u$ represents* 1*, then $\sigma_u$ is an isometry.*

**Proof.** Under the identification of $F$ with $Fe$, the map $V \longrightarrow eV$ is a representation by the definition of the Clifford algebra, since

$$\mathbf{q}(ev) = ev\,\varepsilon(ev) = ev^2e = e\,\mathbf{q}(v).$$

The condition that $V$ is regular implies that $V \longrightarrow eV$ is an isomorphism of vector spaces over $F$. The involution $\varepsilon$ gives an isomorphism of vector spaces $eV \cong fV$. If $ev = fu$ lies in the intersection of $eV$ and $fV$, then $ev = e \cdot ev = efv = 0$. Thus by counting dimensions we find that $eV \oplus fV$ is all of $C_1(V)$. The left and right module structure of $eV$ is inherited from multiplication in $C(V)$. Left multiplication by $\mathfrak{A}_1$ is clear and right multiplication by $\mathfrak{A}_2$ follows from the equality $eV = Vf$ of Proposition 57. The compatibility with the reduced norm of $\mathfrak{A}_1$ is demonstrated using the generating relations in the Clifford algebra and the centrality of $e$ in $C_0(V)$:

$$\begin{aligned}\mathbf{q}(\alpha\,ev) &= \alpha\,ev\,\varepsilon(\alpha\,ev) = \alpha\,e\,v^2\,e\,\varepsilon(\alpha) \\ &= \alpha\,e\,\mathbf{q}(v)\varepsilon(\alpha) = e\,\mathrm{N}(\alpha)\mathbf{q}(v).\end{aligned}$$

The other representations and similitudes are likewise proved by elementary demonstrations.

Now we would like to turn from the structure of quadratic spaces to the quadratic modules contained in them. For a quadratic module $(\Lambda, \mathbf{q})$ over $R$ contained in $(V, \mathbf{q})$ there is a unique inclusion of the Clifford algebra of $C(\Lambda)$ in $C(V)$. First we prove a lemma regarding the multiplicative structure of this integral Clifford algebra.

**Proposition 60** *Let $(\Lambda, \mathbf{q})$ be a proper quaternary quadratic module over $R$ contained in $(V, \mathbf{q})$, and let $e$ be a nontrivial central idempotent of $C(V)$. Then $eC_1(\Lambda)$ is a projective module over $C_0(\Lambda)e$.*

**Proof.** Recall that we define $(\Lambda, \mathbf{q})$ to be proper if $\mathbf{q}(\Lambda)$ is contained in no proper ideal of $R$. Define $P = eC_1(\Lambda)$ and $\widehat{P} = fC_1(\Lambda)$, and let $\mathcal{O}_1 = eC_0(\Lambda)$ and $\mathcal{O}_2 = fC_0(\Lambda)$. Then $P$ has the structure of a left $\mathcal{O}_1$-module and right $\mathcal{O}_2$-module. Similarly $\widehat{P}$ has the structure of a left $\mathcal{O}_2$-module and right $\mathcal{O}_1$-module. It suffices to prove that $P \otimes \widehat{P} \cong \mathcal{O}_1$. There exists a well-defined map $P \otimes \widehat{P} \longrightarrow \mathcal{O}_1$ taking elements of the form $ev \otimes ue$ to $evu$. This extends linearly to sums and form generators for $P \otimes \widehat{P}$ over $\mathcal{O}_1$. Multiplication by $\mathcal{O}_1$ is defined in the ring $C(\Lambda)$ so the left and right module structures are compatible with multiplication in $\mathcal{O}_1$. It remains to show that the map is surjective. For this it suffices to show that 1 lies in $\mathcal{O}_1$, but this follows from the hypothesis that $\Lambda$ is proper.

The main theorem of this section follows.

**Theorem 61** *Let $(\Lambda, \mathbf{q})$ be a proper regular quaternary quadratic module over $R$ of square determinant contained in the quadratic space $(V, \mathbf{q})$. Let $e$ be a nontrivial central idempotent of $C_0(V)$. Then $(\Lambda, \mathbf{q})$ is the quadratic module associated to a projective rank one left module for an order in a quaternion algebra if and only if one of the following equivalent statements is true.*

1. *$e\Lambda = eC_1(\Lambda)$.*
2. *$e\Lambda$ is a left module for $eC_0(\Lambda)$.*
3. *$\Lambda e$ is a right module for $eC_0(\Lambda)$.*
4. *For every $u$ in $\Lambda$, $e\Lambda u$ is a left ideal of $eC_0(\Lambda)$.*
5. *For some $u$ in $\Lambda$, $e\Lambda u$ is a left ideal of $eC_0(\Lambda)$.*
6. *For some $v$ in $\Lambda$, $v\Lambda e$ is a right ideal of $eC_0(\Lambda)$.*

**Proof.** By the previous proposition, the first statement implies that $e\Lambda$ is the quadratic module associated the left projective module over $\mathcal{O}_1 = eC_0(V)$. By Proposition 59, the quadratic module $eC_1(\Lambda)u$ is similar to $eC_1(\Lambda)$ with the same left module structure over $eC_0(\Lambda)$. By Proposition 57 the involution $\varepsilon$ exchanges the modules $eV$ and $Ve$ so the conditions for right multiplicative structures hold by symmetry. Each

of the statements is then equivalent to the condition that $e\Lambda$ is closed under left multiplication by $eC_0(\Lambda)$. By Proposition 60 this gives a projective module structure on $e\Lambda = eC_1(\mathcal{O})$.

Hereafter we will be interested in quadratic modules $(\Lambda, \mathbf{q})$ which satisfy the equivalent conditions of Theorem 61. For a choice of idempotent $e$, we then define the left order of $\Lambda$ to be $\mathcal{O}_1 = eC_0(\Lambda)$ and the right order to be $\mathcal{O}_2 = fC_0(\Lambda)$. We have already proved that $\Lambda$ is projective as a left module over $\mathcal{O}_1$ and by symmetry $\Lambda$ is projective as a right module over $\mathcal{O}_2$. For any such quadratic module there are precisely two quaternion left and right module structures on $\Lambda$ compatible with $\mathbf{q}$. These structures are dual to one another in the sense that the left order $\mathcal{O}_1$ of $\Lambda$ becomes the right order of $\Lambda$ under the second structure, with the opposite ring structure on $\mathcal{O}_1$, and similarly for the right order of $\Lambda$. In particular, the pair consisting of the left and right orders of $\Lambda$ in $C(\Lambda)$ is an invariant of the quaternary quadratic module.

We can now deduce several corollaries for projective modules over orders in quaternion algebras over $\mathbb{Q}$. The first is a classic result concerning positive definite quadratic forms over $\mathbb{Z}$ of determinant equal to the square of a prime (see Eichler [7] and [8]).

**Corollary 62** *Every positive definite quadratic module $(\Lambda, \mathbf{q})$ over $\mathbb{Z}$ with determinant equal to the square of a prime $p$ is the quadratic module of a left projective module of rank one over a maximal order in the quaternion algebra ramified at $p$ and at $\infty$.*

**Proof.** The positive definite condition implies that the quaternion algebra $\mathfrak{A}_1 = eC_0(\Lambda) \otimes \mathbb{Q}$ ramifies at infinity, hence also at a finite prime. The quadratic module $e\Lambda$ is contained in the quadratic module $eC_1(\Lambda)$, and by Proposition 51 and 50, equality holds and $p$ is the unique finite ramifying prime.

From the category equivalence of Chapter 5 we can relate the theory of quadratic modules to homomorphisms of supersingular elliptic curves.

**Corollary 63** *Let $(\Lambda, \mathbf{q})$ be a positive definite quadratic module over $\mathbb{Z}$ of discriminant equal to the square of a prime. Then there exist supersingular elliptic curves $E_1$ and $E_2$ such that $(\Lambda, \mathbf{q})$ is isometric to the quadratic module associated to $\mathrm{Hom}(E_1, E_2)$ equipped with the degree map.*

**Proof.** From Corollary 62, there exists an order $\mathcal{O}$ in the quaternion algebra ramified at $p$ and $\infty$ such that $\Lambda$ has the structure of a left projective module over $\mathcal{O}$. By Theorem 44 and Theorem 45 every projective module arises as a module of homomorphisms of supersingular elliptic curves.

**Corollary 64** *Let $E_1$, $E_2$, $E_3$, and $E_4$ be supersingular elliptic curves over a finite field $k$, and set $I = \mathrm{Hom}(E_1, E_2)$ and $J = \mathrm{Hom}(E_3, E_4)$. Let $\phi$ be the $p$th power*

*Frobenius automorphism. Then $I$ is isometric to $J$ if and only if one of the following set of isomorphisms holds over an algebraic closure.*

1. $E_1 \cong E_3$ *and* $E_2 \cong E_4$.
2. $E_1 \cong E_3^{\phi}$ *and* $E_2 \cong E_4^{\phi}$.
3. $E_1 \cong E_4$ *and* $E_2 \cong E_3$.
4. $E_1 \cong E_4^{\phi}$ *and* $E_2 \cong E_3^{\phi}$.

**Proof.** Each of the four possibilities implies that $I$ is isometric to $J$. Conversely if $I$ is isometric to $J$ then the isometry determines a unique isomorphism of $C(I)$ with $C(J)$. Therefore $I$ is isomorphic to $J$ as a left $\mathcal{O}$-module, where $\mathcal{O} = eC_0(I)$. The two right quaternionic module structures on $J$ are precisely the natural ones on $J$ and the isometric module $\widehat{J}$ of dual isogenies. But $\mathcal{O} \cong \mathrm{End}(E_1)$ arises up to isomorphism only as the endomorphism ring of curves isomorphic to $E_1$ or $E_1^{\phi}$. By the equivalence of categories of § 5.3, these are the only possibilities.

**Corollary 65** *The number of positive definite quadratic modules of discriminant $p^2$ is equal to*

$$\frac{H_1(H_1+1)}{2} + H_1H_2 + H_2(H_2+1)$$

*where $H = H_1 + 2H_2$ is the class number of the quaternion algebra $\mathfrak{A}$ ramified at $p$ and at $\infty$, and $T = H_1 + H_2$ is the type number.*

**Proof.** This is just a count of the combinations of pairs $(E_1, E_2)$ under the equivalences obtained in Corollary 64. The integer $H_1$ is the number of nonisomorphic supersingular elliptic curves over $\overline{\mathbb{F}}_p$ with $j$-values lying in the base field, and the integer $H_2$ the number of conjugate pairs whose $j$-values lie in $\mathbb{F}_{p^2}$.

**Remark.** The Clifford algebra for the quadratic modules of isogenies embeds in an explicitly described matrix ring of isogenies. Let $E_1$ and $E_2$ be supersingular elliptic curves and let $I = \mathrm{Hom}(E_2, E_1)$. Then $I$ has left order $\mathcal{O}_1 = \mathrm{End}(E_1)$ and right order $\mathcal{O}_2 = \mathrm{End}(E_2)$, and we define $\widehat{I}$ to be the module $\mathrm{Hom}(E_2, E_1)$ of dual isogenies. We can define a matrix ring $S$ of isogenies by:

$$S = \begin{pmatrix} \mathcal{O}_1 & I \\ \widehat{I} & \mathcal{O}_2 \end{pmatrix},$$

with multiplication given by matrix multiplication and composition of isogenies. The homomorphism of $I$ to $S$ defined via the map

$$\varphi \longmapsto \begin{pmatrix} 0 & \varphi \\ \widehat{\varphi} & 0 \end{pmatrix},$$

is compatible with the degree map. Thus there exists a unique ring homomorphism $C(I) \longrightarrow S$, commuting with the injection of $I$ in $S$. The even Clifford algebra $C_0(I)$ then embeds in $\mathcal{O}_1 \times \mathcal{O}_2$.

## 6.4 Representations of quadratic modules

We now restrict to the case that $\mathfrak{A}$ is a quaternion algebra over $\mathbb{Q}$, and let $\mathcal{O}$ be a maximal order in $\mathfrak{A}$. In this section we consider representations by quadratic modules $(\Lambda, \mathbf{q})$ associated to projective rank one left modules over $\mathcal{O}$. Special consideration is given to representations of binary quadratic modules by $\Lambda$. We have seen that the algebraic and quadratic module structures are intimately related. We pursue this further by presenting some algebraic results regarding the structure of modules over $\mathcal{O}$ viewed as modules over commutative subrings. Recall that a representation $(M, \mathbf{q}) \longrightarrow (\Lambda, \mathbf{q})$ is primitive if the quotient $\Lambda/M$ is a torsion free $\mathbb{Z}$-module. A subring $R$ of $\mathcal{O}$ is said to be optimally embedded if $\mathcal{O}/R$ is torsion free. The first result we prove is the following.

**Theorem 66** *If $R \to \mathcal{O}$ is an optimal embedding of a rank two commutative subring $R$ in $\mathcal{O}$, then the exact sequence of left $R$-modules*

$$0 \to R \to \mathcal{O} \to \mathcal{O}/R \to 0$$

*splits and the cokernel $\mathcal{O}/R$ is projective as a left $R$-module. In particular, $\mathcal{O}$ is projective as a left $R$-module over every optimally embedded subring $R$.*

**Proof.** We follow a line of reasoning suggested by Hendrik Lenstra. By the definition of an optimal embedding, the cokernel $\mathcal{O}/R$ is torsion free, hence we have a dual exact sequence

$$0 \to \mathrm{Hom}(\mathcal{O}/R, \mathbb{Z}) \to \mathrm{Hom}(\mathcal{O}, \mathbb{Z}) \to \mathrm{Hom}(R, \mathbb{Z}) \to 0.$$

Moreover this sequence is naturally equipped with a right $R$-module structure, for which $\mathrm{Hom}(R, \mathbb{Z})$ is projective as an $R$-module. The dual sequence then splits, and hence the original also. Let us write $\mathcal{O} = R + \mathrm{N}$, and let $S \subseteq R \otimes \mathbb{Q}$ be the left order of N. It suffices to show that $S$ equals $R$. Form the module $S + \mathrm{N} = S + \mathcal{O}$, which is clearly a left $S$-module. Moreover

$$\overline{(S + \mathcal{O}) \cdot S} = \overline{S} \cdot (\overline{S} + \overline{\mathcal{O}}) = S \cdot (S + \mathcal{O}) = S + \mathcal{O},$$

so that $(S + \mathcal{O}) \cdot S = S + \mathcal{O}$. Thus $S + \mathcal{O}$ is a ring containing $\mathcal{O}$, so $S$ equals $R$ by the maximality of $\mathcal{O}$.

We can now prove the following theorem regarding the algebraic structures attached to representations of binary quadratic modules.

**Theorem 67** *Let $(\Lambda, \mathbf{q})$ be the quadratic module associated to a projective rank one left module over $\mathcal{O}$, and let $(M, \mathbf{q})$ be a proper primitive binary quadratic submodule of $(\Lambda, \mathbf{q})$. Then the left order of $M$ is a ring $R$ of discriminant equal to $-\det(M)$*

*which optimally embeds in the left and right orders of* $\Lambda$. *The exact sequence of left* $R$*-modules*

$$0 \to M \to \Lambda \to \Lambda/M \to 0$$

*splits and the cokernel* $\Lambda/M$ *is projective as a left* $R$*-module. In particular* $\Lambda$ *is projective as a left* $R$*-module.*

**Proof.** We relate the algebraic structures on $\Lambda$ and $M$ by means of the Clifford algebra. The representation of $M$ by $\Lambda$ gives a unique homomorphism of Clifford algebras $C(M) \longrightarrow C(\Lambda)$, by which we view $C(M)$ as a subring of $C(\Lambda)$. We identify $M$ with $eM$ and $\Lambda$ with $e\Lambda$, with left orders $R = eC_0(M)$ and $\mathcal{O} = eC_0(\Lambda)$. Since $M$ is proper, 1 lies in $M \cdot M$, so $R = eM^2$ and the discriminant of $R$ is $-\det(M)$. We also identify $\widehat{M} = \mathrm{Hom}_R(M, R)$ with $Me$, thus

$$\begin{aligned} M \otimes_R \widehat{M} &\longrightarrow R \\ em_1 \otimes m_2 e &\longmapsto em_1 m_2 \end{aligned}$$

is an isomorphism. In $C(\Lambda)$ we can also identify $\Lambda \otimes_R \widehat{M}$ with $e\Lambda Me$ so that $\Lambda \otimes_R \widehat{M} \subseteq eC_0(\Lambda) = \mathcal{O}$. By hypothesis $\mathcal{O}\Lambda \subseteq \Lambda$ and $R = M \otimes_r \widehat{M} \subseteq \Lambda \otimes_R \widehat{M}$, so we have $\Lambda \otimes_R \widehat{M} = \mathcal{O}$. In addition, we have shown that $R \subseteq \mathcal{O}$, so there exists an exact sequence of $R$-modules

$$0 \longrightarrow M \longrightarrow \Lambda \longrightarrow N \longrightarrow 0.$$

Since $\widehat{M}$ is a projective, hence flat, $R$-module, we get an exact sequence

$$0 \longrightarrow R \longrightarrow \mathcal{O} \longrightarrow P = N \otimes_R \widehat{M} \longrightarrow 0,$$

in which $R$ optimally embeds in $\mathcal{O}$. By the previous theorem, we have a splitting $\mathcal{O} \cong R \oplus P$ of $R$-modules, where $P$ is projective over $R$. Hence $N = P \otimes_R M$ is projective and we have a splitting of $R$-modules $\Lambda \cong M \oplus N$.

**Corollary 68** *Let* $(\Lambda, \mathbf{q})$ *be the quadratic module associated to* $\mathrm{Hom}(E_1, E_2)$*, and let* $M \to \Lambda$ *be a primitive representation of a proper binary quadratic module* $(M, \mathbf{q})$. *If* $R$ *is the order of discriminant* $-\det(M)$ *in a quadratic extension of* $\mathbb{Q}$*, then* $R$ *optimally embeds in* $\mathrm{End}(E_1)$ *and* $\mathrm{End}(E_2)$.

Knowledge of the subrings optimally embedded in the rings of endomorphisms of supersingular elliptic curves provides strong information on the isomorphism class of this order, as indicated by the following proposition.

**Proposition 69** *An order* $R$ *in a complex imaginary quadratic extension of* $\mathbb{Q}$ *optimally embeds in* $\mathrm{End}(E)$ *if and only if* $j_E$ *is a root of the class equation* $H_D(X) \bmod p$ *for the discriminant* $D = \mathrm{disc}(R)$. *In particular, in its isogeny class,* $E$ *is one of at most* $h(R)$ *elliptic curves containing an optimal embedding of* $R$.

**Proof.** From Deuring's lifting theorem, $E$ can be lifted to an elliptic curve $\widetilde{E}$ over $\overline{\mathbb{Q}}$ with endomorphism ring $R$. Thus $j_{\widetilde{E}}$ satisfies the class equation of degree $h(R)$, and $j_E$ is one of $h(R)$ roots of the reduction of the class polynomial modulo $p$.

**Example.** In general it is not true that a projective module $\Lambda$ over a quaternion order inherits the complex multiplication of nonproper submodules primitively embedded in it. In particular, we may take $\Lambda$ equal to $\mathrm{Hom}(E_1, E_2)$, where $E_1$ and $E_2$ are elliptic curves with complex multiplication by orders of discriminant $D_1 = -16$ and $D_2 = -36$ over the algebraic closure of $\mathbb{F}_{103}$. Let $R = \mathbb{Z}[2i] \subseteq \mathrm{End}(E_2)$ be the commutative subring of discriminant $-16$ in $\mathrm{End}(E_2)$, and let $K = R \otimes \mathbb{Q}$. Neither endomorphism ring has the maximal order of discriminant $-4$ embedded in it, since the class polynomials for the orders of discriminant $-4$ and $-16$ and $-36$ are relatively prime modulo $p$. However, there exists a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\Lambda$ such that

$$(\Phi(\alpha_i, \alpha_j)) = \begin{pmatrix} 10 & 2 & 4 & 1 \\ 2 & 12 & 5 & 4 \\ 4 & 5 & 12 & 0 \\ 1 & 4 & 0 & 12 \end{pmatrix}.$$

The submodule $M$ generated by $\{\alpha_3, \alpha_4\}$ has left order equal to $\mathbb{Z}[i] \subseteq K$ and content equal to 6 as a quadratic module. The left order of $\Lambda/M \cong \Lambda + KM/KM$ is also $\mathbb{Z}[i]$. However, since $\Lambda$ is not a left $\mathbb{Z}[i]$-module, the exact sequence

$$0 \to M \to \Lambda \to \Lambda/M \to 0$$

has no splitting preserving the $R$-module structures on $M$ and $\Lambda/M$

## 6.5 Exterior algebras and determinant maps

Let $(\Lambda, \mathbf{q}) = (\mathrm{End}(E), \deg)$ be the quadratic module associated to any supersingular elliptic curve $E$, and let $\Phi$ be the associated bilinear form on $\Lambda$. Then the discriminant of an element $\tau$ in $\Lambda$, defined as the discriminant of the basis $\{1, \tau\}$ of $\mathbb{Z}[\tau]$ is equal to

$$\mathrm{disc}(\tau) = -\det \begin{pmatrix} \Phi(1,1) & \Phi(1,\tau) \\ \Phi(1,\tau) & \Phi(\tau,\tau) \end{pmatrix} = -(\Phi(1,1)\Phi(\tau,\tau) - \Phi(1,\tau)^2).$$

This defines a singular quadratic map on $\Lambda$, and suggests the definition of a positive definite quadratic map det, equal to $-\mathrm{disc}$, on $\Lambda/\mathbb{Z}$. We call the quadratic map det the *determinant* map on $\Lambda$. If we take $(\Lambda, \mathbf{q})$ to be the quadratic module associated to $\mathrm{Hom}(E_1, E_2)$ for supersingular elliptic curves $E_1$ and $E_2$, then no distinguished element plays the role of 1. For any two elements $\sigma$ and $\tau$ of $\Lambda$, the determinant of the submodule $M = \mathbb{Z}\sigma + \mathbb{Z}\tau$ is

$$\begin{vmatrix} \Phi(\sigma,\sigma) & \Phi(\sigma,\tau) \\ \Phi(\sigma,\tau) & \Phi(\tau,\tau) \end{vmatrix} = \Phi(\sigma,\sigma)\Phi(\tau,\tau) - \Phi(\sigma,\tau)^2.$$

This can be seen to be equivalent to the determinant map on $\mathrm{End}(E_2)$ restricted to the left ideal $\mathrm{Hom}(E_1, E_2)\widehat{\sigma}$. For a fixed element $\sigma$ of $\Lambda$ we define the determinant map relative to $\sigma$ via the bilinear form $\Phi$ on $\Lambda$ as

$$\tau \longmapsto \begin{vmatrix} \Phi(\sigma,\sigma) & \Phi(\sigma,\tau) \\ \Phi(\sigma,\tau) & \Phi(\tau,\tau) \end{vmatrix},$$

which is well-defined on $\Lambda/\sigma\mathbb{Z}$. Since all $\mathrm{End}(E_2)$-module embeddings of $\mathrm{Hom}(E_1, E_2)$ in $\mathrm{End}(E_2)$ as left modules over $\mathrm{End}(E_2)$ are given by

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) &\longrightarrow \mathrm{Hom}(E_1, E_2)\widehat{\sigma} \\ \tau &\longmapsto \tau\widehat{\sigma}, \end{aligned}$$

for some isogeny $\sigma$ in $\mathrm{Hom}(E_1, E_2)$, it appears reasonable to consider the quadratic maps derived in this manner. Of course the situation is symmetric, and we may as well consider this ternary quadratic module as that derived by the embedding of right $\mathrm{End}(E_1)$-modules $\widehat{\sigma}\Lambda \subseteq \mathrm{End}(E_1)$ with the determinant map on $\mathrm{End}(E_1)$. A more natural approach is to construct a bilinear module which represents all such maps under all possible embeddings of $\mathrm{Hom}(E_1, E_2)$ in its left or right order. For this purpose, we define the exterior algebra of $\Lambda$, and equip it with the determinant map derived from $\Phi$.

Let $\Lambda$ be a module over a ring $R$. The exterior algebra of the $\Lambda$ is defined to be an $R$-algebra $\bigwedge(\Lambda)$ along with an $R$-module homomorphism $\psi : \Lambda \to \bigwedge(\Lambda)$ such that $\psi(v)^2 = 0$ for all $v$ in $\Lambda$ and which satisfies the following universal condition. Let $\varphi : \Lambda \to E$ be an $R$-module homomorphism into an $R$-algebra $E$ such that $\varphi(v)^2 = 0$ for all $v$ in $\Lambda$. Then there exists a unique homomorphism of $R$-algebras $\eta : \bigwedge(\Lambda) \to E$ such that $\eta \circ \psi = \varphi$.

As a consequence of this definition, $\bigwedge(\Lambda)$ is a graded $R$-algebra generated by the image of $\Lambda$ in $\bigwedge(\Lambda)$. One can construct $\bigwedge(\Lambda)$ explicitly as follows. Let $T(\Lambda)$ be the tensor algebra of $\Lambda$ and let $E$ be the quotient of $T(\Lambda)$ by the ideal generated by $v \otimes v$ for all $v$ in $\Lambda$. Then $E$ is isomorphic to $\bigwedge(\Lambda)$ via a unique isomorphism commuting with the inclusion of $\Lambda$ in each. We denote the product of $\sigma$ and $\tau$ in $\bigwedge(\Lambda)$ by $\sigma\wedge\tau$, and the $r$-th graded submodule by $\bigwedge^r(\Lambda)$. For a free module $\Lambda$ over an integral domain $R$, the exterior algebra $\bigwedge(\Lambda)$ is free of finite rank over $R$, and in fact has rank equal to $2^d$, where $d$ is the rank of $\Lambda$. Each $\bigwedge^r(\Lambda)$ has rank $\binom{d}{r}$. One notes that the determinant map is not an even bilinear form, so in general we have no associated quadratic form over $R$.

By definition $\bigwedge(\Lambda)$ is an alternating algebra, so on $\tau_1\wedge\cdots\wedge\tau_r$ in $\bigwedge^r(\Lambda)$ the determinant map

$$\tau_1\wedge\cdots\wedge\tau_r \longmapsto \det(\Phi(\tau_i, \tau_j))$$

is well-defined. For $\tau_1\wedge\cdots\wedge\tau_r$ and $\sigma_1\wedge\cdots\wedge\sigma_r$ in $\bigwedge^r(\Lambda)$ we define

$$\Phi_r(\sigma_1\wedge\cdots\wedge\sigma_r, \tau_1\wedge\cdots\wedge\tau_r) = \det(\Phi(\sigma_i, \tau_j)),$$

which defines the determinant map $\Phi_r$ as a bilinear map on all of $\bigwedge^r(\Lambda)$ by extending the definition of $\Phi_r$ linearly to sums. The inclusion of $\Lambda$ in $\bigwedge(\Lambda)$ gives an isometry of the bilinear module $(\Lambda, \Phi)$ with $(\bigwedge^1(\Lambda), \Phi_1)$. For simplicity, we denote $\Phi_r(\omega, \omega)$ by $\det(\omega)$ for "pure" forms $\omega = \tau_1 \wedge \cdots \wedge \tau_r$ in $\bigwedge^r(\Lambda)$. For supersingular elliptic curves $E_1$ and $E_2$, the bilinear module $(\Lambda, \Phi)$ associated to $\mathrm{Hom}(E_1, E_2)$ the determinant map on the ideal $\Lambda\widehat{\sigma}$ has a surjective representation on $\Lambda \wedge \sigma \subseteq \bigwedge^2(\Lambda)$ equipped with the determinant map $\Phi_2$.

**Theorem 70** *Let $(\Lambda, \Phi)$ be a regular bilinear module of rank $n$ over $R$ and let $\bigwedge(\Lambda)$ be the exterior algebra of $\Lambda$ with the quadratic module structure derived from the determinant form on the submodules $\bigwedge^r(\Lambda)$. Then for every quadratic submodule $M$ of of $\Lambda$ of rank $r$ over $R$, the determinant of the quadratic module $\bigwedge^r(M) \wedge \Lambda$ as a submodule of $\bigwedge^{r+1}(\Lambda)$ is $\det(M)^{n-r-1} \det(\Lambda)$.*

**Proof.** Let $V = \Lambda \otimes \mathbb{Q}$ and $U = M \otimes \mathbb{Q}$. Define $W$ to be the $n - r$ dimensional orthogonal complement of $U$ in $V$ relative to the bilinear form $\Phi$, and $N$ to be the projection of $\Lambda$ to $W$. Then $\bigwedge^r(M) \wedge \Lambda$ and $\bigwedge^r(M) \wedge N$ are equal as submodules of $\bigwedge(V)$, so it suffices to prove the result for $\bigwedge^r(M) \wedge N$. Let $\{\nu_i\}$ be any basis for $N$ and let $\omega_M$ be a generator for $\bigwedge^r(M)$. Since $N$ is orthogonal to $M$, by the definition of the bilinear form $\Phi_{r+1}$ on $\bigwedge^{r+1}(\Lambda)$, we have:

$$(\Phi_{r+1}(\omega_M \wedge \nu_i, \omega_M \wedge \nu_j)) = \det(M) \left(\Phi(\nu_i, \nu_j)\right).$$

We also have that $\det(\Lambda) = \det(M \oplus N) = \det(M) \det(N)$. Hence it follows that

$$\det(\bigwedge^r(M) \wedge N)) = \det\left(\det(M) N\right) = \det(M)^{n-r} \frac{\det(\Lambda)}{\det(M)},$$

and the result holds.

We can state several corollaries of this theorem. Hereafter, let $\Lambda$ be a quaternary quadratic module over $\mathbb{Z}$ associated to a left projective module over an order $\mathcal{O}$ in a quaternion algebra over $\mathbb{Q}$.

**Corollary 71** *For any $\alpha$ in $\Lambda$, the determinant of the ternary quadratic submodule $\alpha \wedge \Lambda$ of $\bigwedge^2(\Lambda)$ is $\Phi(\alpha, \alpha)^2 \det(\Lambda)$.*

**Proof.** Set $n = 4$ and $r = 1$ in Theorem 70.

**Corollary 72** *For any two linearly independent $\alpha$ and $\beta$ in $\Lambda$, the submodule $\alpha \wedge \beta \wedge \Lambda$ of $\bigwedge^3(\Lambda)$ is a binary quadratic module of determinant $\det(\alpha \wedge \beta) \det(\Lambda)$.*

**Proof.** Set $n = 4$ and $r = 2$ in Theorem 70.

**Theorem 73** *The bilinear module* $(\bigwedge^3(\Lambda), \Phi_3)$ *is isometric to the the bilinear submodule* $\mathfrak{D}\Lambda$ *of* $\Lambda$*, where* $\mathfrak{D}$ *is the different of* $\mathcal{O}$*. In particular the bilinear form* $\Phi_3$ *is even, and has content* $d(\mathcal{O})$*.*

**Proof.** We note that $\Lambda = \bigwedge^1(\Lambda)$ and $\bigwedge^3(\Lambda)$ are dual with respect to $\bigwedge^4(\Lambda) = \omega\mathbb{Z}$. Let $\mathbf{B} = \{v_1, v_2, v_3, v_4\}$ be a basis for $\Lambda$. Then

$$\{\omega_1, \omega_2, \omega_3, \omega_4\} = \{v_2 \wedge v_3 \wedge v_4, -v_1 \wedge v_3 \wedge v_4, v_1 \wedge v_2 \wedge v_4, -v_1 \wedge v_2 \wedge v_3\}$$

is the dual basis of $\mathbf{B}$ with respect to $\omega\mathbb{Z}$, and the matrix $C = (\Phi_3(\omega_i, \omega_j))$ is the classical adjoint of $A = (\Phi(v_i, v_j))$. Now let $\Lambda^*$ be the dual to $\Lambda$ with respect to $\Phi$ in $\Lambda \otimes \mathbb{Q}$, and let $\mathcal{O}^*$ be the dual to $\mathcal{O}$. For each $v$ in $\Lambda$, the dual to $\mathcal{O}\, v$ is $\mathcal{O}^* v\, \mathbf{q}(v)^{-1}$, so the dual to $\Lambda$ is $\Lambda^* = \bigcap_v \mathcal{O}^* v\, \mathbf{q}(v)^{-1} = \mathcal{O}^*\Lambda$. Let $\{v_1^*, v_2^*, v_3^*, v_4^*\}$ be the dual basis to the basis $\mathbf{B}$ for $\Lambda$. Then $(\Phi(v_i^*, v_j^*))$ is the inverse of the matrix $A$, and

$$(\Phi(d(\mathcal{O})\, v_i^*, d(\mathcal{O})\, v_j^*)) = \det(\Lambda)(\Phi(v_i^*, v_j^*))$$

is the classical adjoint. Thus $\omega_i \mapsto d(\mathcal{O})\, v_i^*$ determines an isometry of $\bigwedge^3(\Lambda)$ to $\Lambda$ with image $d(\mathcal{O})\, \mathcal{O}^*\Lambda = \mathfrak{D}\Lambda$.

**Corollary 74** *Let* $E_1$ *and* $E_2$ *be supersingular elliptic curves, and let* $(\Lambda, \mathbf{q})$ *be the quadratic module associated to* $\mathrm{Hom}(E_1, E_2)$*. Then the bilinear module* $(\bigwedge^3(\Lambda), \Phi_3)$ *is isometric to the quadratic submodule* $\mathrm{P}$ *of* $\Lambda$ *associated to the submodule of inseparable isogenies of* $\mathrm{Hom}(E_1, E_2)$ *with the degree map as quadratic map.*

**Proof.** The inseparable isogenies in $\mathrm{Hom}(E_1, E_2)$ are precisely the isogenies of degree divisible by $p$. Thus the inseparable isogenies are equal to $\mathfrak{D}_2 \mathrm{Hom}(E_1, E_2)$ and also to $\mathrm{Hom}(E_1, E_2)\mathfrak{D}_1$, where $\mathfrak{D}_1$ is the different of $\mathcal{O}_1 = \mathrm{End}(E_1)$ and $\mathfrak{D}_2$ is the different of $\mathcal{O}_2 = \mathrm{End}(E_2)$. The corollary now follows from Theorem 73.

## A result of Gauss

Gauss showed that if $D = -d \not\equiv 1 \bmod 8$ is the discriminant of a quadratic imaginary field extension $K$ of $\mathbb{Q}$, and $D$ is different from $-3$ and $-4$ then the number of times $d$ is represented by a quadratic form

$$f_0(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$$

equals either 12 or 24 times the class number of $K$, when $D \equiv 0 \bmod 4$ or $D \equiv 3 \bmod 4$ respectively. Brezinski and Eichler [2] interpret this and similar class number relations in terms of the number of embeddings of orders in imaginary quadratic extensions of $\mathbb{Q}$ in the maximal orders of quaternion algebras.

In the case of the quadratic form $f_0(\mathbf{x})$ of Gauss, the number of representations of a number $d$ can be interpreted as the number of embeddings of an order in $K$ in a maximal order $\mathcal{O}$ of the definite quaternion algebra $\mathfrak{A}$ over $\mathbb{Q}$ ramified at 2 and at infinity. Since the type number of this algebra is 1, every order which embeds optimally in a maximal order of $\mathfrak{A}$ does so in $\mathcal{O}$.

The determinant forms introduced in this section serve as a useful tool for presenting this phenomenon. One can show that the "correct" quadratic form representing discriminants of imaginary quadratic subrings of $\mathcal{O}$ is

$$f_1(x_1, x_2, x_3) = 3x_1^2 + 2x_1x_2 - 2x_1x_3 + 3x_2^2 + 2x_3x_2 + 3x_3^2.$$

This is the quadratic form associated to the quadratic module $(\mathcal{O}\wedge 1, \Phi_2)$ by means of a choice of basis.

Let $\{v_1, v_2, v_3\}$ be a basis for the quadratic module $(\Lambda_0, \mathbf{q}_0)$ associated to $f_0$ such that

$$\mathbf{q}_0(x_1v_1 + x_2v_2 + x_3v_3) = f_0(x_1, x_2, x_3),$$

and let $\{u_1, u_2, u_3\}$ be a basis for a quadratic module $(\Lambda_1, \mathbf{q}_1)$ associated to $f_1$ such that

$$\mathbf{q}_1(x_1u_1 + x_2u_2 + x_3u_3) = f_1(x_1, x_2, x_3).$$

Then the map $\iota : \Lambda_1 \to \Lambda_2$ given by

$$\begin{aligned} \iota(u_1) &= v_1 + v_2 + v_3 \\ \iota(u_2) &= v_1 - v_2 + v_3 \\ \iota(u_3) &= v_1 - v_2 - v_3 \end{aligned}$$

is a representation of $\Lambda_1$ by $\Lambda_0$. In terms of the image of $\{u_1, u_2, u_3\}$ in $\Lambda_1$, the basis $\{v_1, v_2, v_3\}$ for $\Lambda_0$ is given by

$$v_1 = \frac{\iota(u_1) + \iota(u_3)}{2}, \quad v_2 = \frac{\iota(u_1) - \iota(u_2)}{2}, \quad v_3 = \frac{\iota(u_2) + \iota(u_3)}{2},$$

so that $f_0(x_1, x_2, x_3)$ represents an "authentic" discriminant of a rank two subring of $\mathcal{O}$ if and only if $x_1 \equiv x_2 \equiv x_3 \bmod 2$. It follows that an integer $D$ represented by $f_0$ is authentic if $D \equiv 0, 3 \bmod 4$ and extraneous if $D \equiv 1, 2 \bmod 4$.

# Chapter 7

# Supersingular elliptic curves

The main objective of this chapter is to prove the following theorem.

**Theorem 75** *There exists an algorithm that given any supersingular elliptic curve $E$ over a finite field $k$ computes four endomorphisms in* $\mathrm{End}(E)$ *linearly independent over* $\mathbb{Z}$*. For any* $\varepsilon > 0$ *the algorithm terminates deterministically in* $\mathrm{O}(p^{3/2+\varepsilon})$ *operations in the field $k$ and probabilistically with expected* $\mathcal{O}(p^{1+\varepsilon})$ *operations in $k$, where $p$ is the characteristic of $k$.*

The algorithm is based on the connectedness of the graph of $l$-isogenies for any prime $l$ and the bound on the number of supersingular elliptic curves. We note that the square of the Frobenius endomorphism $\pi$ is equal to a root of unity times a power of $p$. Thus determining the isomorphism type of the commutative ring $\mathrm{End}_k(E)$ when $\pi \notin \mathbb{Z}$ amounts to determining if the index of $\mathbb{Z}[\pi]$ in $\mathrm{End}_k(E)$ locally at 2. We note that $\mathrm{End}_k(E)$ is always maximal at $p$, and $\mathbb{Z}[\pi]$ is maximal everywhere outside of 2 and $p$. This case is solved by a trivial application of the algorithm for ordinary elliptic curves. Thus we interpret the problem as one of finding the full endomorphism ring $\mathrm{End}(E)$ and hereafter work over the algebraic closure of the finite field $k$.

The discrepancy between the deterministic running time and the expected probabalistic running time is due to the lack of an adequate deterministic polynomial factoring algorithm over finite fields.

We define a directed pseudo multigraph $G$ as a finite set $V$ of *vertices* together with a finite set $A$ of *arrows* and a function from $A$ to $V \times V$. Functions on arrows which have image in the diagonal of $V \times V$ are not excluded. A graph is called $m$-regular if for each $v$ in $V$, the inverse image of $\{v\} \times V$ in $A$ has $m$ elements. We define the directed pseudo multigraph $G$ of $l$-isogenies of supersingular elliptic curves as follows. Let $\{E_i\}$ be a complete set of representatives of the isomorphism classes supersingular elliptic curves over the algebraic closure of $k$. We define each $E_i$ to be a vertex of the graph and define an arrow connecting $E_i$ to $E_j$ for each isogeny of

degree $l$, taking only one isogeny up to isomorphism of the curve $E_j$. Thus there are $l+1$ edges with initial vertex $E_i$ corresponding to the $l+1$ cyclic subgroups of $E_i[l]$, so $G$ is $(l+1)$-regular.

We define the additional structure of a dual map on the graph $G$. The dual map takes the arrow of an isogeny to that of its dual isogeny. This map is, however, in general neither surjective nor injective on arrows. An arrow is defined to be an isogeny $\varphi : E_1 \longrightarrow E_2$ chosen from the set $\mathrm{Aut}(E_2)\varphi$. Thus if $E_2$ has more automorphisms than $E_1$ there may be multiple arrows from $E_2$ to $E_1$ and one arrow $E_1 \longrightarrow E_2$ image of the dual map for all of them.

We will use the following theorem on positive definite quadratic modules to deduce results on the graph $G$.

**Theorem 76** *Let $(\Lambda, \mathbf{q})$ be a positive definite quadratic module over $\mathbb{Z}$ of rank at least four. Then there exists an integer $N$ such that if $n \geq N$ is an integer which is primitively represented by $\Lambda \otimes \mathbb{Z}_l$ for all primes $l$, then $n$ is primitively represented by $\Lambda$ over $\mathbb{Z}$.*

**Proof.** This is Theorem 1.6 of Chapter 11 in Cassels [3].

The following theorem gives one proof of the connectedness of $G$. We define an isogeny $\varphi : E_1 \longrightarrow E_2$ of degree $n$, to be *primitive* if there exists no integer $m > 1$ and isogeny $\psi : E_1 \longrightarrow E_2$ such that $\varphi = [m] \circ \psi$.

**Corollary 77** *Let $E_1$ and $E_2$ be supersingular elliptic curves over $k$ in the same isogeny class and suppose that $\pi$ lies in $\mathbb{Z}$. Then for every $n$ sufficiently large and relatively prime to $p$, there exists a primitive isogeny $\varphi : E_1 \longrightarrow E_2$ over $k$ of degree $n$.*

**Proof.** Since $E_1$ and $E_2$ lie in the same isogeny class the condition that $\pi$ lies in $\mathbb{Z}$ is unambiguously defined and both $\mathrm{End}_k(E_1)$ and $\mathrm{End}_k(E_2)$ are of rank four over $\mathbb{Z}$. Thus also $\mathrm{Hom}_k(E_1, E_2) = \mathrm{Hom}(E_1, E_2)$ and we equip the module $\Lambda$ of $k$-isogenies with the structure of a quaternary quadratic module with the degree map. Theorem 76 implies that it is sufficient to look locally. For all primes $l$, the projective $\mathcal{O}_l$ module $\Lambda_l$ is free of rank one and generated by an isogeny of degree relatively prime to $l$. For all primes at which $\mathcal{O}_l$ splits, the local condition is trivially satisfied, because the matrix algebra $\mathbb{M}_2(\mathbb{Z})$ representes all integers primitively, as is demonstrated by the example

$$\begin{pmatrix} n+1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Thus we need only consider the splitting prime $p$. Here also, every integer $n$ relatively prime to $p$ is represented, since $\mathcal{O}_p$ contains an unramified quadratic extension $R_p$ of $\mathbb{Z}_p$, and the reduced norm map on $\mathcal{O}_p$ induces the surjective norm map on units

$N : R_p^* \longrightarrow \mathbb{Z}_p^*$. Since $n$ lies in $\mathbb{Z}_p^*$, any representation of $n$ is trivially primitive in $\Lambda_p$. Thus the conditions of Theorem 76 are satisfied, and the corollary follows.

**Corollary 78** *The graph of $l$-isogenies of supersingular elliptic curves is connected.*

**Proof.** Corollary 77 proves the existence of an isogeny $\varphi : E_1 \longrightarrow E_2$ of degree $l^r$ for every pair of elliptic curves $E_1$ and $E_2$ for $r$ sufficiently large.

**Note.** The standard proof of this fact uses the observation that the number of connected components of a $m$-regular graph $G$ is the dimension of the eigenspace for $k$ in the adjacency matrix for $G$. The adjacency matrix of the $l$-isogenies of supersingular elliptic curves defines the action of the Hecke operator $T_l$, and the one dimensional space of Eisenstein series is the eigenspace for $l+1$. To make Corollary 77 effective, we exploit the interpretation of the adjacency matrix for $G$ as the matrix of the Hecke operator.

We follow the construction of Mestre and Oesterlé in [20].

Next let $M(p)$ be the free abelian group generated by the $H$ supersingular elliptic curves over $\overline{k}$. For each elliptic curve $E_i$ set

$$w_i = \frac{|\operatorname{Aut}(E_i)|}{2},$$

and define a bilinear map $\langle \cdot, \cdot \rangle : M(p) \times M(p) \to \mathbb{Z}$ by setting $\langle E_i, E_j \rangle = 0$ for all $i \neq j$ and $\langle E_i, E_i \rangle = w_i$. Set $\mathcal{E} = \sum_i w_i^{-1} E_i$. Then the orthogonal complement to $\mathcal{E}$ is the subgroup:

$$S(p) = \{\sum_i n_i E_i : \sum_i n_i = 0\}.$$

For each $E_i$ define $\mathcal{S}_i \in S(p)$ by the decomposition

$$E_i = \frac{\mathcal{E}}{\langle \mathcal{E}, \mathcal{E} \rangle} + \mathcal{S}_i.$$

For any prime $l$ different from $p$, we define a *Hecke operator* $T(l)$ on $M(p)$ by letting $T(l)E_i$ be the sum of the final vertices of the arrows in the graph $G$ of having initial vertex $E_i$. By definition, the adjacency matrix of $G$ is the matrix of the operator $T(l)$ in terms of the basis of supersingular elliptic curves, and satisfies the property that $T(l)E_i = \sum_j n_{ij} E_j$ where $\sum_j n_{ij} = l + 1$. From this property, the $\mathcal{E}$ is an eigenvector of the Hecke operator with eigenvalue $l + 1$, and stabilizes the orthogonal subspace $S(p)$.

For the graph of supersingular elliptic curves in characteristic 47, we find adjacency matrices

$$T_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \quad \text{and} \quad T_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 \\ 3 & 2 & 2 & 0 & 0 \end{pmatrix}.$$

Here we see that the automorphisms of certain curves result in a nonsymmetric adjacency matrix.

From the definition of $\mathcal{E}$ and of $\langle \cdot, \cdot \rangle$ on $M(p)$, the value of $\langle \mathcal{E}, \mathcal{E} \rangle$ is $\sum_i w_i^{-1}$ and

$$\langle \mathcal{S}_i, \mathcal{S}_j \rangle = \delta_{ij} w_i - \frac{1}{\langle \mathcal{E}, \mathcal{E} \rangle}$$

where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise. By Theorem 4.1 of Husemöller [11, §13.5], the value of $\langle \mathcal{E}, \mathcal{E} \rangle$ is $(p-1)/12$. From the orthogonal decomposition of $E_i$, the number of isogenies of degree $l^r$ from $E_i$ to $E_j$ is

$$\langle T(l)^r E_i, E_j \rangle = \frac{(l+1)^r}{\langle \mathcal{E}, \mathcal{E} \rangle} + \langle T(l)^r \mathcal{S}_i, \mathcal{S}_j \rangle$$

As noted by Mestre [20], the Hecke operator $T(l)$ is Hermitian with respect to the inner product $\langle \cdot, \cdot \rangle$. Thus if $b$ is a bound on the eigenvalues of the Hecke operator, we find a bound

$$|\langle T(l)^r \mathcal{S}_i, \mathcal{S}_j \rangle| \leq b^r \langle \mathcal{S}_i, \mathcal{S}_i \rangle^{1/2} \langle \mathcal{S}_j, \mathcal{S}_j \rangle^{1/2},$$

by the Cauchy-Schwartz inequality. Thus for $r$ satisfying the lower bound:

$$\left( \frac{l+1}{b} \right)^r \geq (w_j + \frac{1}{\langle \mathcal{E}, \mathcal{E} \rangle})^{1/2} (w_j + \frac{1}{\langle \mathcal{E}, \mathcal{E} \rangle})^{1/2} \langle \mathcal{E}, \mathcal{E} \rangle$$

the number of isogenies of degree $l^r$ from $E_i$ to $E_j$ is at least one. The Riemann hypothesis for function fields, proved by Deligne (see Katz [12]), implies that the eigenvalues for the Hecke operators are bounded by $b = 2\sqrt{l}$. Both $H - 1$ and $\langle \mathcal{E}, \mathcal{E} \rangle$ are bounded by $(p+1)/12$, so we obtain a bound of $\mathrm{O}(\log p)$ on $r$.

We define the *distance* between any two vertices in a graph to be the least number of edges of all paths between them, and the *diameter* of a graph to be the maximum of all the distances between pairs of vertices of the graph. We have proved the following theorem.

**Theorem 79** *For all primes $l$, the diameter of the graph of $l$-isogenies of supersingular elliptic curves is $\mathrm{O}(\log p)$, where the constant in the bound is independent of $l$.*

Mestre and Oesterlé [20] use the above results to obtain a complexity bound for the construction of the graph of $l$-isogenies.

**Theorem 80** *Let $l$ be a prime. There exists an algorithm which, given a prime $p$ and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, determines the graph of $l$-isogenies of supersingular elliptic curves in characteristic $p$ and for any $\varepsilon > 0$ runs deterministically in time $\mathrm{O}(p^{3/2+\varepsilon})$ and probabilistically in expected time $\mathrm{O}(p^{1+\varepsilon})$.*

**Proof.** The prime $l$ is subsumed in the constant for the complexity bound, thus we may assume for simplicity that we have an explicit model for the modular equation for $X_0(l)$. For each supersingular elliptic curve $E_i$, the curves $l$-isogenous to $E_i$ can be obtained by solving for the roots of a modular equation over the field $\mathbb{F}_{p^2}$. The methods of Elkies can be used to produce equations for the kernel of the isogeny. Factoring polynomials of bounded degree over the field $\mathbb{F}_{p^2}$ can be achieved in time $\mathrm{O}(p^{1/2+\varepsilon})$ or using probabilistic methods, in expected polynomial time in $\log p$. The number of supersingular elliptic curves is bounded by $(p+1)/12+1$, so this proves the result.

**Theorem 81** *There exists an algorithm which given endomorphisms $\alpha$ and $\beta$ of $E$ with degrees $n_1$ and $n_2$ and which are expressed as the composite of isogenies of degree bounded by $S$, computes $\Phi(\alpha,\beta)$ in time bounded by a polynomial function in $\log n_1$ $\log n_2$ and $S$.*

**Proof.** The algorithm is essentially the algorithm of Schoof [27] for computing the trace of Frobenius. The argument is simplified by the existence of a compact form for the dual of the isogenies. On each of $\mathrm{O}(\log n)$ torsion subgroups $E[r]$ for small primes $r$ we calculate $\alpha\widehat{\beta}$ and $\beta\widehat{\alpha}$ and find $t$ such that $\Phi(\alpha,\beta) = \alpha\widehat{\beta} + \beta\widehat{\alpha}$ equals multiplication by $t$ on $E[r]$. Then $t$ can be reconstructed by the Chinese remainder theorem and the bound $t \leq 4n$.

We define a *simple cycle* of $G$ to be a path in $G$ from a vertex to itself for which no arrow immediately follows an isogeny with its dual, and which has no repeated vertices.

**Proposition 82** *Every simple cycle through $E$ corresponds to a primitive endomorphisms of $E$ of degree equal to a power of $l$.*

**Proof.** The image of the $l$-torsion of any $l$-isogeny is a cyclic subgroup $C$ of the $l$-torsion group. The dual isogeny kills $C$. Any other isogeny of degree $l$ necessarily maps $C$ injectively into the $l$-torsion of the image curve. Thus the composite of such of degree $l$ does not kill $E[l]$, and is bijective on all other torsion groups $E[r]$, where $r$ is relatively prime to $l$.

We can now prove Theorem 75. A breadth first search of a graph is defined to be a graph search algorithm which sequentially tests all vertices at distance $t$ from an initial vertex before moving to vertices at distance $t+1$. Let $l < 12$ prime and denote by $G$ be the graph of $l$ isogenies of supersingular elliptic curves. By means of a breadth first search of the $G$, beginning at the vertex $E$ we build a spanning tree of the graph of $l$-isogenies, constructing an arrow and its dual simultaneously. Theorem 79 implies that the spanning tree so constructed has depth $\mathrm{O}(\log p)$. Thus arrows absent from the tree at terminal vertices complete simple cycles through $E$ of

length $O(\log p)$. The entire spanning tree for $G$ can be constructed in the time bound of Theorem 80.

In this way we find an endomorphism $\alpha$ and can compute its trace to find the discriminant of the ring $\mathbb{Z}[\alpha]$ in $\mathrm{End}(E)$. By a geometry of numbers argument we expect to find $\alpha$ with discriminant $O(p)$, though the graph diameter only gives a bound in terms of a power of $p$. If a bound of $O(p)$ holds then the class number $h$ of $\mathbb{Z}[\alpha]$ is $O(p^{1/2} \log p)$ and we have narrowed the field of candidate orders from $O(p)$ to $h$.

We continue, choosing a second endomorphism $\beta$ and computing $\Phi(1, \beta)$ and $\Phi(\alpha, \beta)$. In the cycle corresponding to $\alpha$, the arrows correspond to prime ideals lying over $l$ in the endomorphism rings of the vertex curves, and $\alpha$ is a generator of the principal ideal $\mathfrak{l}^r$ in $\mathbb{Z}[\alpha]$, where $\mathfrak{l}$ lies over $l$ and $r$ is the length of the cycle. Provided the cycle for $\beta$ is not contained in that for $\alpha$ or its dual, the ring $\mathbb{Z}\langle\alpha, \beta\rangle$ generated by $\alpha$ and $\beta$ is not contained in a rank two order. We can now conclude with the following proposition.

**Proposition 83** *The endomorphisms $\alpha$ and $\beta$ generate a suborder of $\mathrm{End}(E)$ of discriminant*

$$\left(\frac{D_1 D_2 - t^2}{4}\right)^2,$$

*where $D_1$ is the discriminant of $\mathbb{Z}[\alpha]$, where $D_2$ is the discriminant of $\mathbb{Z}[\beta]$ and where $t = \Phi(1, \alpha)\Phi(1, \beta) - \Phi(\alpha, \beta)$.*

**Proof.** The discriminant is explicitly computed for the basis $\{1, \alpha, \beta, \alpha\beta\}$.

This completes the proof of Theorem 75.

**Note.** The number of maximal orders containing a ring $\mathbb{Z}\langle\alpha, \beta\rangle$ is greatly constrained by explicit bounds in terms of the discriminants $D_1$, $D_2$, and $t$, as noted in [2].

In the following case we can prove that $\alpha$ and $\beta$ suffice to generate the endomorphism ring of $E$.

**Theorem 84** *Suppose that the norm of $\alpha$ is $l^{h_1}$, where $h_1$ is the class number of the ring $\mathbb{Z}[\alpha]$, and the norm of $\beta$ is $l^{h_2}$ where $h_2$ is the class number of the ring $\mathbb{Z}[\beta]$. Then if the cycles for $\alpha$ and $\beta$ intersect only at $E$, the endomorphism ring of $E$ is uniquely determined by the embedding of $\mathbb{Z}\langle\alpha, \beta\rangle$.*

**Proof.** Let $\mathfrak{l}$ be a prime of $\mathbb{Z}[\alpha]$ lying over the the rational prime $l$. Then the ideal $\mathfrak{l}^i$ is the intersection with $\mathbb{Z}[\alpha]$ of the kernel ideal for the isogeny to the $i$-th elliptic curve in the cycle defining $\alpha$. Since $\alpha$ is a simple cycle, $\mathfrak{l}$ generates the class group and the elliptic curves in the cycle of isogenies determining $\alpha$ represent all isomorphism classes of elliptic curves whose endomorphism ring contains $\alpha$. By symmetry all isomorphism classes of elliptic curves are represented by the elliptic curves in the cycle for $\beta$. Thus $E$ and hence the endomorphism ring of $E$ is determined uniquely by $\alpha$ and $\beta$.

The problem of determining necessary and sufficient conditions to determine the isomorphism type of the endmorphism ring of $E$ is a subject for future research by the author.

# Bibliography


[1] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[2] J. Brezinski and M. Eichler. On the imbeddings of imaginary quadratic orders in definite quaternion algebras. *J. Reine Angew. Math.*, 426:91–105, 1992.

[3] J. W. S. Cassels. *Rational Quadratic Forms*. Academic Press, 1978.

[4] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1991.

[5] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. PhD thesis, École Normale Supérieure, 1994.

[6] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.

[7] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195:127–151, 1955.

[8] M. Eichler. Quadratische Formen und Modulfunktionen. *Acta Arith.*, IV:1217–239, 1958.

[9] N. Elkies. Explicit isogenies. Manuscript, 1991.

[10] T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[11] D. Husemöller. *Elliptic curves*. Springer-Verlag, 1987.

[12] N. Katz. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. *Annals of Math.*, 28:275–305, 1976.

[13] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag, second edition, 1993.

[14] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields*. Academic Press, 1977.

[15] T. Y. Lam. *The algebraic theory of quadratic forms*. Mathematics Lecture Notes. W. A. Benjamin, 1973.

[16] S. Lang. *Elliptic Functions*. Springer-Verlag, 1987.

[17] S. Lang. *Introduction to modular forms*. Springer-Verlag, 1995.

[18] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

[19] S. MacLane. *Categories for the Working Mathematician*. Springer-Verlag, 1972.

[20] J.-F. Mestre. Sur la méthode des graphes, exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, pages 217–242. Nagoya University, 1986.

[21] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. *J. Théorie des Nombres de Bordeaux*, 7:255–282, 1995.

[22] I. Pays. Formes normes d'ordres. *Journal of Algebra*, 155:325–334, 1993.

[23] A. Pizer. The action of the canonical involution on modular forms of weight 2 on $\Gamma_0(N)$. *Math. Ann.*, 226:99–116, 1977.

[24] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *Journal of Algebra*, 64:340–390, 1980.

[25] I. Reiner. *Maximal orders*. Academic Press, 1975.

[26] B. Schoeneberg. *Elliptic Modular Functions*. Springer-Verlag, 1974.

[27] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Mathematics of Computation*, 44:483–494, 1985.

[28] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[29] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[30] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[31] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones math.*, 2:134–144, 1966.

[32] J. Tate. Global class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 305–347. Academic Press, 1967.

[33] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris, Sér. A.*, 273:238–241, 1971.

[34] M.-F. Vignéras. *Arithmétique des Algèbres de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[35] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. Éc. Norm. Sup.*, 2:521–560, 1969.

[36] A. Weil. *Basic Number Theory*. Springer-Verlag, 1973.

[37] N. Yui and D. Zagier. On the singular values of Weber modular functions. *Mathematics of Computation*, 1996. To appear.