The Endomorphism Ring Problem and Supersingular Isogeny Graphs

by

Doeon Cha

B.Math., University of Waterloo, 2019

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2021

Declaration of Committee

Name:	**Doeon Cha**
Degree:	**Master of Science**
Thesis title:	**The Endomorphism Ring Problem and Supersingular Isogeny Graphs**
Committee:	**Chair:** Weiran Sun Associate Professor, Mathematics
	Imin Chen Supervisor Professor, Mathematics
	Nils Bruin Committee Member Professor, Mathematics
	Stephen Choi Examiner Professor, Mathematics

Abstract

Supersingular isogeny graphs, which encode supersingular elliptic curves and their isogenies, have recently formed the basis for a number of post-quantum cryptographic protocols. The study of supersingular elliptic curves and their endomorphism rings has a long history and is intimately related to the study of quaternion algebras and their maximal orders.

In this thesis, we give a treatment of the theory of quaternion algebras and elliptic curves over finite fields as these relate to supersingular isogeny graphs and computational problems on such graphs, in particular, consolidating and surveying results in the research literature.

We also perform some numerical experiments on supersingular isogeny graphs and establish a number of refined upper bounds on supersingular elliptic curves with small non-integer endomorphisms.

Keywords: Quaternion algebras, supersingular elliptic curves, isogeny graphs

Acknowledgements

I would like to pay my special regards to my supervisor Professor Imin Chen for introducing me to the research topic of post-quantum cryptography and providing helpful guidance and contributions to the completion of my Master's thesis. He always has been a great advisor, mentor, and friend whom I could depend on. I also thank him for his efforts to enrich my time in Vancouver, especially in this harsh time of the pandemic. His kind invitations to small gatherings with nice meals provided me valuable time to make companions with other mathematicians from various institutions and fellow graduate students in SFU.

I am grateful to my committee members, Professor Nils Bruin and Professor Stephen Choi, who provided valuable comments to improve my thesis and offered their points of view to approach the endomorphism ring problem. Also, Professor Bruin's courses in Algebraic number theory and Algebraic geometry helped me a lot to build a solid preliminary background in theories of both elliptic curves and quaternion algebras.

I also had the great pleasure of working with fellow students in a series of seminars and classes in elliptic curves and various other topics. It was good to be with someone with whom I can share the passion to learn and provide inspiration to each other.

Lastly, I would like to thank my family for supporting my decision to study mathematics in Canada and giving their full material and emotional support. Without their help, I couldn't have initiated this long journey in Canada. Their continuing trust in me always has been a huge strength for me.

Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

The rise of quantum computers and their capability to break conventional cryptosystems draw attention to the need of alternative cryptosystems. In search of post-quantum cryptosystems that are not breakable by quantum computers, supersingular isogeny graphs (SIG) systems were first introduced by Charles, Goren, and Lauter in 2006 [8]. The SIG systems rely on the computational difficulty of finding isogenies between supersingular elliptic curves. They constructed cryptographic hash functions using paths in the ℓ-isogeny graph of supersingular elliptic cures over $\mathbb{F}_{p^2}$. Since then, a public key exchange based on SIG called SIKE was proposed by De Feo, Jao, and Plût in [14].

There are related problems to this path finding problem, namely computing the endomorphism ring of a supersingular elliptic curve and computing a maximal order in a quaterinon algebra isomorphic to the endomorphism ring of a supersingular elliptic curve. A fundamental result relating these problems is the one-to-one correspondence between the endomorphism rings of supersingular elliptic curves and maximal orders in quaternion algebras given by Deuring [16]. Under some heuristic assumptions, these three problems are believed to be equivalent. These problems are more precisely defined and algorithms for efficient reductions from one problem to another are discussed in [17]. There are no known algorithms for these problems with sub-exponential complexity. The first one who studied the endomorphism ring problem is Kohel [23]. He used cycles in the supersingular isogeny graph to compute endomorphisms linearly independent over $\mathbb{Z}$. The running time of the probabilistic alroghthm was $O(p^{1+\epsilon})$. In [15], Delfs and Galbraith gave an algorithm for finding isogenies between supersingular curves over $\mathbb{F}_p$ with complexity $\widetilde{O}(p^{1/4})$, and then used it to give a general algorithm for finding isogenies between supersingular elliptic curves with complexity $\widetilde{O}(p^{1/2})$.

In this thesis, we review preliminaries on quaternion algebras and elliptic curves to build up towards the proof of Deuring's correspondence, and provide a comprehensive review on the prob-

lem of finding paths in the supersingular isogeny graph, computing the endomorphism ring, and computing maximal orders in Deuring's correspondence, with reductions between them.

In Chapter 2, we introduce preliminary material on the arithmetic of quaternion algebras from Voight [33]. For every quaternion algebra B over $\mathbb{Q}$, there are only finitely many places in $\mathbb{Q}$ where B is ramified. This finite set of places uniquely determines a quaternion algebra over $\mathbb{Q}$ up to isomorphism. A few important algebraic structures such as lattices, orders, and ideals in quaternion orders, are essential to describe relations among the three problems of supersingular elliptic curves.

In Chapter 3, we present basic theory of elliptic curves and isogenies between them from [31], Vélu's formula for constructing isogenies between elliptic curves [18, 22], and elliptic curves with complex multiplication [12]. The endomorphism ring of elliptic curves is one of the following types of rings; either it is the ring of rational integers, an order in an imaginary quadratic field, or an order in a quaternion algebra, where the last case gives the definition of supersingular elliptic curve. There are equivalent conditions for an elliptic curve to be supersingular. Vélu's formula gives a way to explicitly evaluate an isogeny, given a specification of the kernel as a set of points in it or polynomial defining them. The j-invariant of an elliptic curve over $\mathbb{C}$ whose endomorphism ring is isomorphic to the maximal order in an imaginary quadratic field K generates the Hilbert class field of K. Then the Deuring Lifting Theorem shows that there is a way to obtain a supersingular elliptic curves as a reduction of an elliptic curve over a number field.

In Chapter 4, we follow a proof of Deuring's correspondence from [33], using the theory of elliptic curves and quaternion algebras presented in the previous chapters. For each prime p, there is a bijection from the set of supersingular elliptic curves up to Galois conjugacy to maximal orders in the quaterinon algebra ramified exactly at p and infinity up to isomorphism. Then we introduce a constructive algorithm computing a supersingular j-invariant such that the endomorphism ring is isomorphic to a given special order [7, 17].

In Chapter 5, we define the supersingular ℓ-isogeny graph using the classical modular polynomial and review its basic properties introduced in [3, 23, 9]. Supersingular isogeny graphs are connected regular directed multi-graphs, and it is a Ramanujan graph. We introduce the notion of M-small [27], (M, ℓ)-small, and (M, S)-small elliptic curves, and bound these, in order to describe the computational hardness of finding short cycles in supersingular isogeny graphs. We provide numerical data showing how hard it is to get a cycle in supersingular isogeny graphs from breadth first search.

In Chapter 6, we introduce a precise definition of three problems on SIG and algorithms in [17]. These algorithms provide reductions between the problems and show they are heuristically equivalent. This includes finding explicit versions of Deuring's correspondence and efficient algorithms to translate j-invariants into maximal orders in the quaternion algebra and conversely.

1.2 Notation and Terminology

1. We say that $f(x) = O(g(x))$ if there is a real constant M such that $|f(x)| \leq Mg(x)$ for sufficiently large x.

2. $\tilde{O}(g(x))$ means $O(g(x))$ up to factors in $\log g(x)$.

3. We say that $f(x) = \Omega(g(x))$ if there is a real constant M such that $f(x) \geq Mg(x)$ for sufficiently large x.

4. If K is a number field, then $\mathcal{O}_K$ denotes its ring of integers.

5. If L is a finite extension of a field K, then $[L : K] := \dim_K L$ denotes the degree of L over K, namely the dimension of L over K.

Chapter 2

Quaternion Algebras

2.1 Overview

Definition 2.1.1. Let F be a field with $\operatorname{char} F \neq 2$ and let $a, b \in F^\times$. A **quaternion algebra** B **over** F is an F-algebra with a basis $1, i, j, k$ such that $i^2 = a, j^2 = b$, and $k = ij = -ji$. We denote this algebra by $(a, b \mid F)$. The elements i, j are called **standard generators** for B (or we say $\{1, i, j, k\}$ is a **quaternionic basis** of B).

The following multiplication rules hold in B and can be F-linearly extended:

$$i^2 = a, j^2 = b, k^2 = -ab, ij = k, ji = -k, jk = -bi, kj = bi, ki = -aj, ik = aj.$$

Example 2.1.2. The quaternion algebra $\mathbb{H} := (-1, -1 \mid \mathbb{R})$ is called the ring of **Hamilton's quaternions**.

We have a notion of quaternion algebra when the base field F has characteristic 2, but often statements about quaternion algebra require an alternative proof to the case where $\operatorname{char} F \neq 2$. For the generality, we provide the definition of quaternion algebra over field of characteristic 2, but we will only give proofs for the case where $\operatorname{char} F \neq 2$.

Definition 2.1.3. An algebra B over a field F with $\operatorname{char} F = 2$ is called a **quaternion algebra** if there exists an F-basis $1, i, j, k$ for B such that

$$i^2 + i = a, j^2 = b, \text{ and } k = ij = j(i + 1)$$

with $a \in F$ and $b \in F^\times$.

Throughout the rest of this section, suppose that $\operatorname{char} F \neq 2$. See [33, Chapter 6] for the case $\operatorname{char} F = 2$.

Lemma 2.1.4. An F-algebra B is a quaternion algebra if and only if there exists nonzero elements $i, j \in B$ that generate B as an F-algebra and satisfy

$$i^2 = a, j^2 = b, \text{ and } ij = -ji \tag{2.1}$$

with $a, b \in F^\times$. In other words, once the relations (2.1) are satisfied for generators i, j, then automatically B has dimension 4 as an F-vector space, with F-basis $1, i, j, ij$.

Proof. See [33, Lemma 2.2.5]. □

Next, we discuss some standard isomorphisms between quaternion algebras.

Lemma 2.1.5. Let $B = (a, b \mid F)$ be a quaternion algebra. Then we have the following isomorphisms between quaternion algebras:

(i) $(a, b \mid F) \simeq (b, a \mid F)$.

(ii) $(a, b \mid F) \simeq (a, -ab \mid F)$.

(iii) $(a, b \mid F) \simeq (b, -ab \mid F)$.

(iv) $(a, b \mid F) \simeq (ac^2, bd^2 \mid F)$ for all $c, d \in F^\times$.

Proof. Different choices of standard generators give the isomorphisms. Let $i, j \in B$ be standard generators of B.

To prove (i), consider a canonical map obtained by F-linearly extending the map

$$B \to B'$$
$$i, j \mapsto i' := j, j' := i.$$

The map preserves the relations of standard generators in (2.1) since $i'^2 = j^2 = b$ and $j'^2 = i^2 = a$. Hence $B' = (b, a \mid F)$ is the quaternion algebra with standard generators i', j' and $B \simeq B'$.

For (ii), the map $i, j \mapsto i, ij$ gives the isomorphism $(a, b \mid F) \simeq (a, -ab \mid F)$ since $i^2 = a, (ij)^2 = -ab$, and $i(ij) = -(ij)i$. (iii) is Similar to (ii).

Lastly, we prove (iv). For $c, d \in F^\times$, the map $i, j \mapsto ci, dj$ gives the last isomorphism since $(ci)^2 = ac^2, (dj)^2 = bd^2$, and $(ci)(dj) = -(dj)(ci)$. □

Given a quaternion algebra over F, a field extension $K \supseteq F$ gives a new quaternion algebra by extending scalars. Hence, there is a canonical isomorphism

$$(a, b \mid F) \otimes_F K \simeq (a, b \mid K).$$

.

Proposition 2.1.6. Let $B = (a, b \mid F)$ and let $F(\sqrt{a})$ be a splitting field over F for the polynomial $x^2 - a$, with root $\sqrt{a} \in F(\sqrt{a})$. Then the map

$$\begin{aligned} m : B &\hookrightarrow \mathrm{M}_2(F(\sqrt{a})) \\ i, j &\mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \\ t + xi + yj + zij &\mapsto \begin{pmatrix} t + x\sqrt{a} & b(y + z\sqrt{a}) \\ y - z\sqrt{a} & t - x\sqrt{a} \end{pmatrix} \end{aligned}$$

is an injective F-algebra homomorphism.

Proof. See [33, Proposition 2.3.1]. □

Corollary 2.1.7. The multiplication in a quaternion algebra B is associative.

Proof. The map m in Proposition 2.1.6 gives an embedding such that $m(\alpha+\beta) = m(\alpha)+m(\beta)$ and $m(\alpha\beta) = m(\alpha)m(\beta)$. It follows that the multiplication in B is associative since the multiplication in a matrix ring is so. □

Definition 2.1.8. A quaternion algebra B over F is called **split** if $B \simeq \mathrm{M}_2(F)$. Otherwise, we say B is **non-split**.

Corollary 2.1.9. Let F be a field of $\operatorname{char} F \neq 2$. For all $a, c \in F^\times$,

$$(a, 1 \mid F) \simeq (a, c^2 \mid F) \simeq (a, -a \mid F) \simeq \mathrm{M}_2(F).$$

Proof. We follow the proof in [33, Corollary 2.3.6].

The isomorphisms between quaternion algebras are given in Lemma 2.1.5. The map

$$\begin{aligned} m : (a, 1 \mid F) &\to \mathrm{M}_2(F) \\ i, j &\mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

gives an isomorphsim $(a, 1 \mid F) \simeq \mathrm{M}_2(F)$ of F-algebras. □

Corollary 2.1.10. If $B = (a, b \mid \mathbb{R})$ is a quaternion algebra over $\mathbb{R}$, then

$$B \simeq \begin{cases} \mathbb{H} & \text{if } a < 0 \text{ and } b < 0, \\ \mathrm{M}_2(\mathbb{R}) & \text{otherwise.} \end{cases}$$

Also, the only quaternion algebra over $\mathbb{C}$ is $\mathrm{M}_2(\mathbb{C})$.

Proof. If $a, b < 0$, then $B = (-(\sqrt{-a})^2, -(\sqrt{-b})^2 \mid \mathbb{R}) \simeq \mathbb{H}$ by Lemma 2.1.5. Otheriwse, $B \simeq \mathrm{M}_2(\mathbb{R})$ by Corollary 2.1.9. Similarly, the only quaternion algebra over $\mathbb{C}$ is $(1, 1 \mid \mathbb{C}) \simeq \mathrm{M}_2(\mathbb{C})$. □

Definition 2.1.11. Let B be an algebra over a field F. An **involution** $\bar{}: B \to B$ is an F-linear map which satisfies

(i) $\overline{1} = 1$.

(ii) $\overline{\overline{\alpha}} = \alpha$ for all $\alpha \in B$.

(iii) $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$ for all $\alpha, \beta \in B$ (the map $\bar{}$ is an anti-automorphism).

An involution $\bar{}$ is called **standard** if $\alpha\overline{\alpha} \in F$ for all $\alpha \in B$.

Let $\bar{}$ be a standard involution on B. For any $\alpha \in B$,

$$\alpha + \overline{\alpha} = (\alpha + 1)(\overline{\alpha + 1}) - \alpha\overline{\alpha} - 1 \in F$$

since $\bar{}$ is standard. It follows that $\alpha\overline{\alpha} = \overline{\alpha}\alpha$, since

$$(\alpha + \overline{\alpha})\alpha = \alpha(\alpha + \overline{\alpha}).$$

Example 2.1.12. Let $B = (a, b \mid F)$ be a quaternion algebra over F with $\operatorname{char} F \neq 2$. The map

$$\begin{aligned} \bar{}: B &\to B \\ \alpha = t + xi + yj + zij &\mapsto \overline{\alpha} = t - (xi + yi + zij) \end{aligned}$$

defines a standard involution since

$$\alpha\overline{\alpha} = \overline{\alpha}\alpha = t^2 - ax^2 - by^2 + abz^2 \in F.$$

Also we have $\overline{\alpha} = 2t - \alpha$.

From now on, when we use a standard involution $\bar{}$, we mean the conjugation map in Example 2.1.12.

Definition 2.1.13. Let $\bar{}: B \to B$ be a standard involution on an F-algebra B. We define the **reduced trace** on B by

$$\begin{aligned} \mathrm{trd}: B &\to F \\ \alpha &\mapsto \alpha + \overline{\alpha}, \end{aligned}$$

and similarly the **reduced norm**

$$\begin{aligned} \mathrm{nrd} : B &\to F \\ \alpha &\mapsto \alpha\overline{\alpha}. \end{aligned}$$

We will write

$$\begin{aligned} B^0 &:= \{\alpha \in B : \mathrm{trd}(\alpha) = 0\} \\ B^1 &:= \{\alpha \in B^\times : \mathrm{nrd}(\alpha) = 1\}. \end{aligned}$$

for the F-subspace B^0 of elements of reduced trace 0 and for the subgroup B^1 of elements of reduced norm 1.

Definition 2.1.14. An element $\alpha = t + xi + yj + zij \in (a, b \mid F)$ is called **pure** if $t = 0$, i.e., $\mathrm{trd}(\alpha) = 0$.

Example 2.1.15. For $B = \mathrm{M}_2(F)$, the reduced trace is the usual matrix trace and the reduced norm is the determinant.

Theorem 2.1.16. An element $\alpha \in (a, b \mid F)$ is invertible if and only if $\mathrm{nrd}(\alpha) \neq 0$.

Proof. Suppose α is invertible so that $\alpha\alpha' = 1$ for some $\alpha' \in (a, b \mid F)$. Taking reduced norm on both sides gives

$$\mathrm{nrd}(\alpha)\,\mathrm{nrd}(\alpha') = 1,$$

so $\mathrm{nrd}(\alpha) \in F^\times$. Conversely, suppose $\mathrm{nrd}(\alpha) \neq 0$. Then

$$\alpha \cdot \frac{\overline{\alpha}}{\mathrm{nrd}(\alpha)} = \frac{\overline{\alpha}}{\mathrm{nrd}(\alpha)} \cdot \alpha = 1.$$

□

The reduced trace trd is an F-linear map, since this is true for the standard involution:

$$\mathrm{trd}(\alpha + \beta) = (\alpha + \beta) + \overline{(\alpha + \beta)} = (\alpha + \overline{\alpha}) + (\beta + \overline{\beta}) = \mathrm{trd}(\alpha) + \mathrm{trd}(\beta)$$

for all $\alpha, \beta \in B$. The reduced norm nrd is multiplicative, since

$$\mathrm{nrd}(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha\,\mathrm{nrd}(\beta)\overline{\alpha} = \mathrm{nrd}(\alpha)\,\mathrm{nrd}(\beta)$$

for all $\alpha, \beta \in B$.

Definition 2.1.17. Let B be an F-algebra. For any $\alpha \in B$, the polynomial

$$x^2 - \mathrm{trd}(\alpha)x + \mathrm{nrd}(\alpha) \in F[x]$$

is called the **reduced characteristic polynomial** of α.

By the definition,

$$\alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha} = 0 \tag{2.2}$$

identically for any $\alpha \in B$. Hence $\alpha \in B$ is a root of its reduced polynomial. When $\alpha \notin F$, the reduced characteristic polynomial of α is its minimal polynomial, since if α satisfies a polynomial of degree 1 then $\alpha \in F$.

Definition 2.1.18. An F-algebra K of $\dim_F K = 2$ is called a **quadratic** algebra.

Lemma 2.1.19. Let K be a quadratic F-algebra. Then K is commutative and has a unique standard involution.

Proof. We follow the proof in [33, Lemma 3.4.2].

Since K has dimension 2, we can write $K = F \oplus F\alpha = F[\alpha]$ for any $\alpha \in K \setminus F$, which is commutative. Furthermore, $\alpha^2 = t\alpha - n$ for unique $t, n \in F$ since $1, \alpha$ is a basis for K. Then $K = F[\alpha]$ admits a standard involution $\bar{}: K \to K$ given by

$$\overline{x + y\alpha} := (x + ty) - y\alpha.$$

This is a standard involution since for any $x + y\alpha, x' + y'\alpha \in K$ with $x, x'y, y' \in F$,

$$\begin{aligned}
\overline{1} &= 1, \\
\overline{\overline{x + y\alpha}} &= \overline{(x + ty) - y\alpha} = (x + ty - ty) + y\alpha = x + y\alpha, \\
\overline{(x + y\alpha)(x' + y'\alpha)} &= xx' - nyy' + txy' + tx'y + t^2yy' - (xy' + x'y + tyy')\alpha = \overline{x + y\alpha}\,\overline{x' + y'\alpha} \\
(x + y\alpha)\overline{x + y\alpha} &= x^2 + txy + ny^2 \in F.
\end{aligned}$$

Note that this is the unique standard involution with the property that $\overline{\alpha} = t - \alpha$ since if i is another standard involution with the property, then

$$i(x + y\alpha) = x + yi(\alpha) = x + ty - y\alpha.$$

If $\bar{}: K \to K$ is any standard inovlution, then from

$$\alpha^2 = (\alpha + \overline{\alpha})\alpha - \alpha\overline{\alpha}$$

we must have $t = \alpha + \overline{\alpha}$ by the uniqueness of t. Hence any standard involution must have $\overline{\alpha} = t - \alpha$. It follows that standard involution on K is unique. □

Corollary 2.1.20. If an F-algebra B has a standard involution, then this involution is unique.

Proof. See [33, Corollary 3.4.4]. □

Definition 2.1.21. A ring is called a **division ring** if every nonzero element is a unit. A **division algebra** is an algebra that is a division ring.

Definition 2.1.22. Let B be an F-algebra. We say B is **central** if F is the center of B, and we say B is **simple** if B has no nontrivial two-sided ideals.

Let $Z(R)$ denote the center of a ring R. A quaternion algebra B over F is noncommutative and $Z(B) = F$. Indeed B can be characterized as a central simple algebra. Let F^{al} denote a choice of algebraic closure of F.

Corollary 2.1.23. Let B be an algebra over a field F. Then the following are equivalent:

(i) B is a quaternion algebra.

(ii) $B \otimes_F F^{\mathrm{al}} \simeq \mathrm{M}_2(F^{\mathrm{al}})$.

(iii) B is a central simple algebra of dimension $\dim_F B = 4$.

Moreover, a quaternion algebra B is either a division algebra or $B \simeq \mathrm{M}_2(F)$ is split.

Proof. See [33, Corollary 7.1.2]. □

Since division rings are simple (as any nonzero two-sided ideals contain 1), Corollary 2.1.23 implies that a division algebra B over F is a quaternion algebra over F if and only if it is central of dimension $\dim_F B = 4$.

Definition 2.1.24. Let B be a commutative finite-dimensional algebra over a field F. We say B is **separable** if

$$B \otimes_F F^{\mathrm{al}} \simeq F^{\mathrm{al}} \times \cdots \times F^{\mathrm{al}};$$

otherwise, we say B is **inseparable**.

Remark 2.1.25. If $B \simeq F[x]/(f(x))$ with $f(x) \in F[x]$, then B is separable if and only if f has distinct roots in F^{al}. If $\operatorname{char} F \neq 2$, and K is a quadratic F-algebra, then after completing the square, we see that the following are equivalent [33, 6.1.3]:

(i) K is separable.

(ii) $K \simeq F[x]/(x^2 - a)$ with $a \neq 0$.

(iii) K is reduced (K has no nonzero nilpotent elements).

(iv) K is a field or $K \simeq F \times F$.

Remark 2.1.26. [33, 6.1.4] If $\operatorname{char} F = 2$, then a quadratic F-algebra K is separable if and only if

$$K \simeq F[x]/(x^2 + x + a)$$

for some $a \in F$. A quadratic algebra of the form $K = F[x]/(x^2 + a)$ with $a \in F$ is inseparable.

Now we introduce a more general notation that gives a characteristic-independent way to define quaternion algebras. Let K be a separable quadratic F-algebra, and let $b \in F^\times$. We denote by

$$(K, b \mid F) := K \oplus Kj$$

the F-algebra with basis $1, j$ as a left K-vector space and with the multiplication rules $j^2 = b$ and $j\alpha = \overline{\alpha}j$ for $\alpha \in K$, where $^-$ is the standard involution on K (the nontrivial element of $\operatorname{Gal}(K/F)$ if K is a field). If $\operatorname{char} F \neq 2$ then writing $K = F[x]/(x^2 - a)$ we see that

$$(K, b \mid F) \simeq (a, b \mid F)$$

is a quaternion algebra over F.

2.2 Ramification

In this section, we give the classification of quaternion algebras; first over local fields and then over global fields. In particular, we will show that there exists a unique quaternion algebra over $\mathbb{Q}$, which is ramified exactly at a prime p and ∞.

Definition 2.2.1. A **local field** is a Hausdorff, locally compact topological field with a nondiscrete topology.

Definition 2.2.2. An absolute value on a field F is **nonarchimedean** if the **ultrametric inequality**

$$|x + y| \leq \sup\{|x|, |y|\}$$

is satisfied for all $x, y \in F$, and **archimedean** otherwise.

A field with absolute value is archimedean if and only if it satisfies the **archimedean property**: for all $x \in F^\times$, there exists $n \in \mathbb{Z}$ such that $|nx| > 1$. In particular, a field F equipped with an archimedean absolute value has $\operatorname{char} F = 0$.

Example 2.2.3. Let p be a prime. The set of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ defined by $|0|_p = 0$ and

$$|c|_p = p^{-\nu_p(c)} \text{ for } c \in \mathbb{Q}^\times,$$

where $\nu_p : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ is the p-adic valuation defined by $v_p(c) = k$ if $c = \frac{p^k m}{n}$, where $m, n \in \mathbb{Z}$ are relatively prime and $p \nmid mn$, and $v_p(0) = \infty$. $\mathbb{Q}_p$ is a local field with the valuation ring

$$\begin{aligned}\mathbb{Z}_p :&= \left\{ x = (x_n)_n \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : x_{n+1} \equiv x_n \pmod{p^n} \text{ for all } n \geq 1 \right\} \\ &= \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \\ &= \{x \in \mathbb{Q}_p : \nu_p(x) \geq 0\},\end{aligned}$$

the p-adic integers.

Theorem 2.2.4. A field F with absolute value is a local field if and only if F is one of the following:

(i) F is archimedean, and $F \simeq \mathbb{R}$ or $F \simeq \mathbb{C}$.

(ii) F is nonarchimedean with $\operatorname{char} F = 0$, and F is a finite extension of $\mathbb{Q}_p$ for some prime p.

(iii) F is nonarchimedean with $\operatorname{char} F = p$, and F is a finite extension of the Laurent series field $\mathbb{F}_p((t))$ for some prime p; in this case, there is a (non-canonical) isomorphism $F \simeq \mathbb{F}_q((t))$ where q is a power of p.

A field F with absolute value $|\cdot|$ is a nonarchimedean local field if and only if F is complete with respect to $|\cdot|$, and $|\cdot|$ is equivalent to the absolute value associated to a nontrivial discrete valuation $\nu : F \to \mathbb{R} \cup \{\infty\}$ with finite residue field.

Proof. See [33, Theorem 12.2.15]. □

Now we give the classification of quaternion algebras B over local fields F. First, suppose F is archimedean. The only quaternion algebra over $\mathbb{C}$ up to isomorphism is $B \simeq \mathrm{M}_2(\mathbb{C})$, and $\mathbb{H}$ is the unique division quaternion algebra over $\mathbb{R}$ by Corollary 2.1.10. We will give the classification of quaternion algebras over nonarchimedean local fields via extensions of valuations.

Let R be a complete discrete valuation ring (DVR) with valuation $\nu : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ and field of fractions F, maximal ideal $\mathfrak{p} = \pi R$ with a uniformizer π, and residue field $k := R/\mathfrak{p}$. Let $K \supseteq F$ be a finite separable extension of degree $n := [K : F]$. Then K is also a nonarchimedean local field as follows

Lemma 2.2.5. There exists a unique valuation w on K such that $w \mid_F = \nu$, defined by

$$w(x) := \frac{\nu(\mathrm{Nm}_{K/F}(x))}{[K : F]}.$$

The integral closure of R in K is the valuation ring

$$S := \{x \in K : w(x) \geq 0\}.$$

When $w \mid_F = \nu$, we say that w **extends** ν.

Proof. See [33, Lemma 13.2.1]. □

Definition 2.2.6. Let $K \supseteq F$ be fields defined as in Lemma 2.2.5. We say $K \supseteq F$ is **unramified** if a uniformizer π for F is also a uniformizer for K. We say $K \supseteq F$ is **totally ramified** if a uniformizer π_K of K has the property that π_K^n is a uniformizer for F.

In general, there is a (unique) maximal unramified subextension $K_{\text{un}} \subseteq K$, and the extension $K \supseteq K_{\text{un}}$ is totally ramified. We say that $e = [K : K_{\text{un}}]$ is the **ramification degree** and $f = [K_{\text{un}} : F]$ the **inertial degree**, and the fundamental equality

$$n = [K : F] = ef$$

holds.

We can generalize this to the noncommutative case. Let D be a central (simple) division algebra over F with $\dim_F D = [D : F] = n^2$. We extend the valutation ν to a map

$$\begin{aligned} w : D &\to \mathbb{R} \cup \{\infty\} \\ \alpha &\mapsto \frac{\nu(\text{Nm}_{D/F}(\alpha))}{[D : F]} = \frac{\nu(\text{nrd}(\alpha))}{n}, \end{aligned} \tag{2.3}$$

where the equality follows from the fact that $\text{Nm}_{D/F}(\alpha) = \text{nrd}(\alpha)^n$ (see [33, Section 7.8] for the reduced norm on D).

Lemma 2.2.7. The map w in (2.3) is the unique valuation on D extending ν i.e., the following hold:

(i) $w(\alpha) = \infty$ if and only if $\alpha = 0$.

(ii) $w(\alpha\beta) = w(\alpha) + w(\beta) = w(\beta\alpha)$ for all $\alpha, \beta \in D$.

(iii) $w(\alpha + \beta) \geq \min(w(\alpha), w(\beta))$ for all $\alpha, \beta \in D$.

(iv) $w(D^\times)$ is discrete in $\mathbb{R}$.

Proof. See [33, Lemma 13.3.2]. □

From Lemma 2.2.7, we say that w is a **discrete valuation** on D since it satisfies the same axioms as for a field. It follows from the Lemma 2.2.7 that the set

$$\mathcal{O} := \{\alpha \in D : w(\alpha) \geq 0\} \tag{2.4}$$

is a ring, called the **valuation ring** of D.

Proposition 2.2.8. The ring $\mathcal{O}$ in (2.4) is the unique maximal R-order in D, consisting of all elements of D that are integral over R.

Proof. See [33, Proposition 13.3.4]. □

Theorem 2.2.9. Let F be a nonarchimedean local field. Then the following statements hold.

(a) There is a unique division quaternion algebra B over F, up to F-algebra isomorphism given by

$$B \simeq (K, \pi \mid F) = K \oplus Kj,$$

where K is the unique quadratic unramified (separable) extension of F.

(b) Let B be as in (a). Then the valuation ring of B is $\mathcal{O} \simeq S \oplus Sj$, where S is the integral closure of R in K. Moreover, the ideal $P = \mathcal{O}j$ is the unique maximal ideal; we have $P^2 = \pi\mathcal{O}$, and $\mathcal{O}/P \supseteq R/\mathfrak{p}$ is a quadratic extension of finite fields.

Proof. See [33, Theorem 13.3.11]. □

Example 2.2.10. Let p be a prime number and let $q = p^2$. When $F = \mathbb{Q}_p$,

$$B \simeq (\mathbb{Q}_q, p \mid \mathbb{Q}_p)$$

is the unique quaternion algebra over F up to isomorphism, where $\mathbb{Q}_q$ is the unique quadratic unramified (separable) extension of $\mathbb{Q}_p$. The valuation ring of B is $\mathcal{O} \simeq \mathbb{Z}_q \oplus \mathbb{Z}_q j$, and the maximal ideal $P = \mathcal{O}j$ has $P^2 = p\mathcal{O}$ and $\mathcal{O}/P \simeq \mathbb{Z}_q/p\mathbb{Z}_q \simeq \mathbb{F}_q$. This is the special case of Theorem 2.2.9 (see [33, Theorem 13.1.6]).

Corollary 2.2.11. Let F be a nonarchimedean local field with valuation ν, let K be a separable, unramified quadratic F-algebra, and let $B = (K, b \mid F)$ with $b \in F^\times$. If $\nu(b) = 0$, then $B \simeq \mathrm{M}_2(F)$.

Proof. See [33, Corollary 13.4.1]. □

Let F be a nonarchimedean local field and let B be a division quaternion algebra over F. In analogy with the case of local field extensions, we define the **ramification index** of B over F as $e(B \mid F) = 2$ since $P^2 = \pi\mathcal{O}$, and the **inertial degree** of B over F as $f(B \mid F) = 2$ since B contains the unramified quadratic extension K of F, and we have the equality

$$e(B \mid F) f(B \mid F) = 4 = [B : F],$$

as in the commutative case.

We have the complete classification of quaternion algebras over local fields. In particular, there is a unique division quaternion algebra over a local field $F \neq \mathbb{C}$ up to F-algebra isomorphism. We

now give the classification of quaternion algebras over $\mathbb{Q}$. See [33, Chapter 14.6] for more general results over any global fields.

Definition 2.2.12. A **global field** is either a number field or a finite extension of $\mathbb{F}_p(t)$ (a function field) for a prime p.

Global fields are strongly governed by their completions with respect to nontrivial absolute values, which are local fields.

Definition 2.2.13. Let F be a global field. A **place** of F is an equivalence of embeddings $\iota : F \to F_\nu$ where F_ν is a local field and $\iota(F)$ is dense in F_ν; two embeddibgs $\iota' : F \to F_\nu$ and $\iota' : F \to F'_\nu$ are said to be **equivalent** if there is an isomorphism of topological fields $\phi : F_\nu \to F'_\nu$ such that $\iota' = \phi \circ \iota$. The set of places of F is denoted by $\operatorname{Pl} F$.

Every valuation $\nu : F \to \mathbb{R} \cup \{\infty\}$ on a global field F, up to scaling, defines a place $\iota_\nu : F \to F_\nu$ where F_ν is the completion of F with respect to the absolute value induced by ν. We call such a place **nonarchimedean**, and using this identification we will write ν for both the place of F and the corresponding valuation. If F is a function field, then all places of F are nonarchimedean. If F is a number field, a place $F \hookrightarrow \mathbb{R}$ is called a **real place** and a place $F \hookrightarrow \mathbb{C}$ (equivalent to its complex conjugate) is called a **complex place**. A real or complex place is called **archimedean**.

Example 2.2.14. The set of places $\operatorname{Pl} \mathbb{Q}$ of $\mathbb{Q}$ consists of the archimedean real place, induced by the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$ and the usual absolute value $|x|_\infty$, and the set of nonarchimedean places indexed by the primes p given by the embeddings $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, with the p-adic absolute value

$$|x|_p = p^{-\nu_p(x)}.$$

Definition 2.2.15. A set $S \subseteq \operatorname{Pl} F$ is **eligible** if S is finite, nonempty, and contains all archimedean places of F.

Definition 2.2.16. Let S be an eligible set of places. The **ring of S-integers** in F is the set

$$R_{(S)} := \{x \in F : \nu(x) \geq 0 \text{ for all } \nu \notin S\}.$$

A **global ring** is a ring of S-integers in a global field for an associated eligible set S.

Definition 2.2.17. Let $B = (a, b \mid F)$ be a quaternion algebra over a global field F and let $\nu \in \operatorname{Pl} F$. We say that B is **ramified** at ν if the completion $B_\nu := B \otimes_F F_\nu \simeq (a, b \mid F_\nu)$ is a division ring. Otherwise we say that B is **split** (or **unramified**) at ν. If $\nu \in \operatorname{Pl} F$ is a nonarchimedean place, corresponding to a prime $\mathfrak{p}$ of R, we will also say that B is **ramified** at $\mathfrak{p}$ when B is ramified at ν.

Let $\operatorname{Ram} B$ denote the set of ramified places of a quaternion algebra B over a global field F.

Let $R = R_{(S)}$ be a global ring, with $S \subset \operatorname{Pl} F$ eligible. Let B be a quaternion algebra over F. The set $\operatorname{Ram} B$ of ramified places of B is finite [33, Lemma 14.5.3], and we make the following definition.

Definition 2.2.18. The **R-discriminant** of B is the R-ideal

$$\operatorname{disc}_R(B) := \prod_{\substack{\mathfrak{p} \in \operatorname{Ram} B \\ \mathfrak{p} \notin S}} \mathfrak{p} \subseteq R$$

obtained as the product of all primes $\mathfrak{p}$ of $R = R_{(S)}$ ramified in B.

Remark 2.2.19. When F is a number field and S consists of archimeadean places only, so that R is the ring of integers of F, we abbreviate $\operatorname{disc}_R(B) = \operatorname{disc} B$.

From now on, we restrict our attention to the case when $F = \mathbb{Q}$.

Lemma 2.2.20. Let B be a quaternion algebra over $\mathbb{Q}$. The set $\operatorname{Ram} B$ of ramified places of B is finite.

Proof. See [33, Lemma 14.2.3]. □

Not every finite subset Σ of places can occur as $\operatorname{Ram} B$ for a quaternion algebra B. It turns out that the parity condition here is that we must have $\#\Sigma$ even.

Definition 2.2.21. Let B be a quaternion algebra over $\mathbb{Q}$. We define the **discriminant** of B to be the product $\operatorname{disc} B$ of primes that ramify in B, so $\operatorname{disc} B$ is a squarefree positive integer.

Proposition 2.2.22. Let Σ be a finite set of places of $\mathbb{Q}$ of even cardinality. Then there exists a quaternion algebra B over $\mathbb{Q}$ with $\operatorname{Ram} B = \Sigma$.

Proof. See [33, Proposition 14.2.7]. □

Example 2.2.23. Let $B = (a, b \mid \mathbb{Q})$ be a quaternion algebra of prime discriminant $D = p$ over $\mathbb{Q}$. Then:

(i) For $D = p = 2$, we take $a = b = -1$.

(ii) For $D = p = 3 \pmod 4$, we take $b = -p$ and $a = -1$.

(iii) For $D = p \equiv 1 \pmod 4$, we take $b = -p$ and $a = -q$ where $q \equiv 3 \pmod 4$ is prime and $\left(\frac{q}{p}\right) = -1$.

[33, Example 14.2.13]

Proposition 2.2.24. Let B, B' be quaternion algebras over $\mathbb{Q}$. The followings are equivalent.

(i) $B \simeq B'$.

(ii) $\operatorname{Ram} B = \operatorname{Ram} B'$.

(iii) $B_v \simeq B'_v$ for all places of $\mathbb{Q}$.

(iv) $B_v \simeq B'_v$ for all but one place of $\mathbb{Q}$.

Proof. See [33, Theorem 14.3.1]. □

Let B be a quaternion algebra over $\mathbb{Q}$. Proposition 2.2.22 shows that every allowable set of ramified places of B can be obtained, and Proposition 2.2.24 shows that the map $B \mapsto \operatorname{Ram} B$ is injective on isomorphism classes. Hence, we have the following classification of quaternion algebras over $\mathbb{Q}$.

Theorem 2.2.25. (Local-global principle) The maps

$$\begin{aligned} B &\mapsto \operatorname{Ram}(B) \\ \prod_{p\in\Sigma} p &\longmapsfrom \Sigma \end{aligned}$$

gives a bijection

$$\left\{\begin{matrix}\text{Quaternion algebras over } \mathbb{Q} \\ \text{up to isomorphism}\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Finite subsets of places of } \mathbb{Q} \text{ of} \\ \text{even cardinality}\end{matrix}\right\} \tag{2.5}$$

The composition of these maps is $B \mapsto \prod_{p\in\operatorname{Ram} B} p = \operatorname{disc} B$ [33, Theorem 14.1.3].

Corollary 2.2.26. Let B be a quaternion algebra over $\mathbb{Q}$. Then $B \simeq \mathrm{M}_2(\mathbb{Q})$ if and only if $B_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ for all primes p.

Proof. See [33, Corollary 14.3.2]. □

Definition 2.2.27. Let B be a quaternion algebra over $\mathbb{Q}$. We say that B is **definite** if $\infty \in \operatorname{Ram} B$ and B is **indefinite** otherwise

By definition, B is definite if and only if $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R} = (a, b \mid \mathbb{R}) \simeq \mathbb{H}$ if and only if $a, b < 0$ by Corollary 2.1.10.

Definition 2.2.28. Let B be a quaternion algebra over a number field F. We say that B is **totally definite** if all archimedean places of F are ramified in B. Otherwise, we say B is **indefinite**.

If ν is a complex place, then ν is necessarily split since the only quaternion algebra over $\mathbb{C}$ is $\mathrm{M}_2(\mathbb{C})$ by Corollary 2.1.10. Therefore, if B is totally definite quaternion algebra over a number field F, then F is totally real, i.e., for each embedding of F into $\mathbb{C}$ the image lies inside $\mathbb{R}$.

2.3 Lattices and orders

Let R be a domain with field of fractions $F := \operatorname{Frac} R$.

Definition 2.3.1. Let V be a n-dimensional vector space over F. An **R-lattice** in V is finitely generated R-submodule $M \subset V$ with $MF = V$, i.e., it contains a F-basis of V.

Definition 2.3.2. Let B be a finite dimensional F-algebra. An **R-order** $\mathcal{O} \subseteq B$ is a R-lattice that is also a ring. If $\mathcal{O}$ is not properly contained in any other order, we call it a **maximal order**.

Remark 2.3.3. For a quaternion algebra B over $\mathbb{Q}$, by a **lattice** in B, we mean a $\mathbb{Z}$-lattice of the form

$$\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_4$$

for some basis $\{x_1, \cdots, x_4\}$ of B and similarly for an **order** in B.

Example 2.3.4. One can easily check the lattice

$$\mathcal{O} := \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$$

is closed under multiplication, and so defines an order, but it is not maximal.

Lemma 2.3.5. The center of an R-order $\mathcal{O}$ in a quaternion algebra B over F is R.

Proof. Since $\mathcal{O}$ contains a F-basis of B, every element in $Z(\mathcal{O})$ commutes with B, so $Z(\mathcal{O}) \subseteq Z(B) = F$. Then

$$R = Z(R) = Z(\mathcal{O} \cap F) = Z(\mathcal{O}) \cap F = Z(\mathcal{O}).$$

□

Definition 2.3.6. Let I be an R-lattice in F-algebra B. The **left order** of I is the set

$$\mathcal{O}_L(I) := \{\alpha \in B : \alpha I \subseteq I\}.$$

We similarly define the **right order** $\mathcal{O}_R(I)$ of I.

The left or right orders are R-orders, so writing a lattice from a basis of F-algebra and then taking its right order is an immediate way to give an R-order.

Lemma 2.3.7. The left order (or the right order) of an R-lattice is an R-order.

Proof. See [33, Lemma 10.2.7]. □

The order has a few local properties as follows.

Lemma 2.3.8. Let B be a finite-dimensional F-algebra and let $I \subseteq B$ an R-lattice. Then the following are equivalent:

(i) I is an R-order.

(ii) $I_{(\mathfrak{p})}$ is an $R_{(\mathfrak{p})}$-order for all prime ideals $\mathfrak{p}$ of R.

(iii) $I_{(\mathfrak{m})}$ is an $R_{(\mathfrak{m})}$-order for all maximal ideals $\mathfrak{m}$ of R.

Proof. See [33, Lemma 10.2.10]. □

Lemma 2.3.9. Let R be a Dedekind domain. An R-order $\mathcal{O} \subseteq B$ is maximal if and only if $\mathcal{O}_{(\mathfrak{p})}$ is a maximal $R_{(\mathfrak{p})}$-order for all primes $\mathfrak{p}$ of R.

Proof. See [33, Lemma 10.4.3]. □

Lemma 2.3.10. Let R be a Dedekind domain and let $\mathcal{O} \subseteq B$ be an R-order. Then for all but finitely many primes $\mathfrak{p}$ of R, we have $\mathcal{O}_{(\mathfrak{p})} = \mathcal{O} \otimes_R R_{(\mathfrak{p})}$ is maximal.

Proof. See [33, Lemma 10.4.4]. □

An important quantity characterizing the order is the discriminant. Recall that the discriminant of a quaternion algebra B over $\mathbb{Q}$ is the square-free product of primes ramified in B. The discriminant of the order in B is defined as follows.

Definition 2.3.11. Let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subseteq B$ be an order. We define the **discriminant** of $\mathcal{O}$ to be

$$\operatorname{disc}(\mathcal{O}) := |\det(\operatorname{trd}(\alpha_i \alpha_j))_{i,j}| \in \mathbb{Z}_{>0}$$

where $\alpha_1, \cdots, \alpha_4$ is a $\mathbb{Z}$-basis for $\mathcal{O}$.

If $\mathcal{O}' \supseteq \mathcal{O}$, then we have

$$\operatorname{disc}(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 \operatorname{disc}(\mathcal{O}').$$

This implies $\mathcal{O}' = \mathcal{O}$ if and only if $\operatorname{disc}(\mathcal{O}') = \operatorname{disc}(\mathcal{O})$. Moreover, the discriminant of an order is always a square, so we define the **reduced discriminant** $\operatorname{discrd}(\mathcal{O})$ to be the square root of $\operatorname{disc}(\mathcal{O})$. One can also show that $\mathcal{O}$ is a maximal order if and only if $\operatorname{discrd}(\mathcal{O}) = \operatorname{disc}(B)$. We will generalize these notions to R-lattices and also prove their properties mentioned before.

Let R be a noetherian domain with $F = \operatorname{Frac} R$ and let B be a semisimple algebra over F with $\dim_F B = n$.

Definition 2.3.12. For elements $\alpha_1, \cdots, \alpha_n \in B$, we define

$$d(\alpha_1, \cdots, \alpha_n) := \det(\operatorname{trd}(\alpha_i \alpha_j))_{i,j=1,\cdots,n}.$$

Let $I \subseteq B$ be an R-lattice.

Definition 2.3.13. The **discriminant** of I is the R-submodule $\mathrm{disc}(I) \subseteq F$ generated by the set

$$\{d(\alpha_1, \cdots, \alpha_n) : \alpha, \cdots, \alpha_n \in I\}.$$

Lemma 2.3.14. Let $\alpha_1, \cdots, \alpha_n \in B$ and suppose $\beta_1, \cdots, \beta_n \in B$ are of the form $\beta_i = \sum_{j=1}^n m_{ij}\alpha_j$ with $m_{ij} \in F$. Let $M = (m_{ij})_{i,j=1\cdots,n}$. Then

$$d(\beta_1, \cdots, \beta_n) = \det(M)^2 d(\alpha_1, \cdots, \alpha_n).$$

Proof. [33, Lemma 15.2.5]. □

Corollary 2.3.15. If I is free as an R-module, and $\alpha_1, \cdots, \alpha_n$ is an R-basis for I, then

$$\mathrm{disc}(I) = d(\alpha_1, \cdots, \alpha_n)R.$$

Proof. See [33, Corollary 15.2.7] □

If $I = \mathcal{O}$ is an R-order (so closed under multiplication), then for $\alpha_1, \cdots, \alpha_n \in \mathcal{O}$ we have $\mathrm{trd}(\alpha_i\alpha_j) \in R$ for all i, j. Thus $d(\alpha_1, \cdots, \alpha_n) \in R$ and therefore $\mathrm{disc}(\mathcal{O}) \subseteq R$ is a principal R-ideal. When working over $\mathbb{Z}$, it is common to take the discriminant instead to be the positive generator of the discriminant as an ideal as we did in Definition 2.3.11.

The discriminant is well-behaved under automorphisms because the reduced trace is so.

Corollary 2.3.16. If $\phi : B \xrightarrow{\sim} B$ is an F-algebra automorphism, then $\mathrm{disc}(\phi(I)) = \mathrm{disc}(I)$.

Proof. [33, Corollary 15.2.9]. □

Example 2.3.17. Suppose $\mathrm{char}\, F \neq 2$. Let $B := (a, b \mid F)$ with $a, b \in R$. Let $\mathcal{O} := \langle 1, i, j, k\rangle \subseteq B$, called the **standard order**, which is clearly an order. Then $\mathrm{disc}(\mathcal{O})$ is the principal R-ideal generated by

$$d(1, i, j, ij) = \det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & -2ab \end{pmatrix} = -(4ab)^2.$$

Proposition 2.3.18. For any prime ideal $\mathfrak{p}$ of R,

$$\mathrm{disc}(I_{(p)}) = \mathrm{disc}(I)_{(\mathfrak{p})}$$

on localizations and

$$\mathrm{disc}(I_{\mathfrak{p}}) = \mathrm{disc}(I)_{\mathfrak{p}}$$

on completions. Then we can write

$$\operatorname{disc}(I) = \bigcap_{\mathfrak{p}} \operatorname{disc}(I_{(\mathfrak{p})}).$$

Proof. See [33, 15.2.13]. □

Lemma 2.3.19. If B is separable as an F-algebra and I is projective as an R-module then $\operatorname{disc}(I)$ is a nonzero projective fractional ideal of R.

Proof. See [33, Lemma 15.2.14]. □

Lemma 2.3.20. Let $I, J \subseteq B$ be projective R-lattices. Then

$$\operatorname{disc}(I) = [J : I]_R^2 \operatorname{disc}(J).$$

Moreover, if $I \subseteq J$, then $\operatorname{disc}(I) = \operatorname{disc}(J)$ if and only if $I = J$.

Proof. [33, Lemma 15.2.15]. □

Now, we show that the discriminant of every R-order is the square of an R-ideal and define this square root directly.

Definition 2.3.21. We define the form $m : B \times B \times B \to F$

$$\begin{aligned} m(\alpha_1, \alpha_2, \alpha_3) &:= \operatorname{trd}((\alpha_1\alpha_2 - \alpha_2\alpha_1)\overline{\alpha_3}) \\ &= \alpha\alpha_2\overline{\alpha_3} - \alpha_2\alpha_1\overline{\alpha_3} - \alpha_3\overline{\alpha_2}\,\overline{\alpha_1} + \alpha_3\overline{\alpha_1}\,\overline{\alpha_2} \end{aligned}$$

The form m is an alternating trilinear form which is well-defined as a form on B/F [33, Lemma 15.4.3].

Definition 2.3.22. Let $I \subseteq B$ be an R-lattice. The **reduced discriminant** of I is the R-submodule $\operatorname{discrd}(I)$ of F generated by

$$\{m(\alpha_1, \alpha_2, \alpha_3) : \alpha_1, \alpha_2, \alpha_3 \in I\}.$$

Similar to the discriminant, the reduced discriminant have the following properties; if $\alpha_i, \beta \in B$ with $\beta_i = M\alpha_i$ for some $M \in \mathrm{M}_3(F)$, then

$$m(\beta_1, \beta_2, \beta_3) = \det(M) m(\alpha_1, \alpha_2, \alpha_3)$$

and if $I \subseteq J$ are projective R-lattices in B, then

$$\operatorname{discrd}(I) = [J : I] \operatorname{discrd}(J).$$

Lemma 2.3.23. If I is a projective R-lattice in B, then $\operatorname{disc}(I) = \operatorname{discrd}(I)^2$.

Proof. See [33, Lemma 15.4.7]. □

From now, let R be a Dedekind domain.

Lemma 2.3.24. Let $\mathcal{O} \subseteq \mathcal{O}'$ be R-orders. Then $\mathcal{O} = \mathcal{O}'$ if and only if $\operatorname{disc} \mathcal{O} = \operatorname{disc} \mathcal{O}'$.

Proof. See [33, Lemma 15.5.1]. □

Proposition 2.3.25. There exists a maximal R-order in B, and every order $\mathcal{O}$ is contained in a maximal R-order $\mathcal{O}' \subseteq B$.

Proof. See [33, Proposition 15.5.2]. □

Lemma 2.3.26. Suppose that R is a DVR, and let $\mathcal{O} \subseteq B := \mathrm{M}_n(F)$ be an R-order. Then $\mathcal{O}$ is maximal if and only if $\operatorname{disc} \mathcal{O} = R$.

Proof. See [33, Lemma 15.5.3]. □

Lemma 2.3.27. Let F be a nonarchimedean local field with valuation ring R and let B be a division quaternion algebra over F. The valuation ring $\mathcal{O} \subset B$ is the unique maximal order with $\operatorname{disc} \mathcal{O} = \mathfrak{p}^2$ and $\operatorname{discrd} \mathcal{O} = \mathfrak{p}$. It follows that an R-order in B is maximal if and only if it has reduced discriminant $\mathfrak{p}$.

Proof. See [33, Example 15.5.4]. □

Theorem 2.3.28. Let R be a global ring with field of fractions F, let B be a quaternion algebra over F, and let $\mathcal{O} \subseteq B$ be an R-order. Then $\mathcal{O}$ is maximal if and only if $\operatorname{discrd}(\mathcal{O}) = \operatorname{disc}_R(B)$.

Let R be a Dedekind domain with field of fractions F, let B be a quaternion algebra over F.

Definition 2.3.29. An R-order $\mathcal{O} \subseteq B$ is called an **Eichler order** if it is the intersection of two maximal orders.

Definition 2.3.30. Suppose R is local. The **standard Eichler order of level $\mathfrak{p}^e$** in $\mathrm{M}_2(F)$ is the order

$$\mathcal{O}_0(\mathfrak{p}^e) := \begin{pmatrix} R & R \\ \mathfrak{p}^e & R \end{pmatrix}.$$

Remark 2.3.31. [33, 23.4.19] Suppose that R is a global ring. Let $\operatorname{disc}_R B = \mathfrak{D}$ and let $\mathcal{O}$ be an Eichler order with $\operatorname{discrd} \mathcal{O} = \mathfrak{R}$. If $\mathfrak{p} \mid \mathfrak{D}$, then $B_\mathfrak{p}$ has a unique maximal order, so $\mathfrak{O}_\mathfrak{p}$ is necessarily the maximal order. If $\mathfrak{p} \nmid \mathfrak{D}$, and $\operatorname{ord}_\mathfrak{p} \mathfrak{R} = e \geq 0$, then $\mathcal{O}_\mathfrak{p}$ is isomorphic to the standard Eichler order of level $\mathfrak{p}^e$. We have $\mathfrak{R} = \mathfrak{D}\mathfrak{M}$ with $\mathfrak{M} \subseteq R$ and $\mathfrak{M}$ is coprime to $\mathfrak{D}$. We call $\mathfrak{M}$ the **level** of the Eichler order $\mathcal{O}$.

2.4 Quaternion ideals and invertibility

Throughout this section, let R be a Dedekind domain with field of fractions F, let B be a finite-dimensional F-algebra, and let $I \subseteq B$ be an R-lattice.

Let $\mathcal{O} \subseteq B$ be an R-order. We study its ring structure via ideals.

Definition 2.4.1. I is principal if there exists $\alpha \in B$ such that

$$I = \mathcal{O}_L(I)\alpha = \alpha\mathcal{O}_R(I);$$

We say that I is **generated** by α

If $\alpha \in B$ generates an R-lattice, then $\alpha \in B^\times$ since

$$B = IF = \mathcal{O}_L(I)F\alpha = B\alpha = B.$$

Moreover, $I = \mathcal{O}_L(I)\alpha$ if and only if $I = \alpha\mathcal{O}_R(I)$ [33, 16.2.3], so it is sufficient to check for a one-sided generator.

The notion of principality extends locally as follows.

Definition 2.4.2. An R-lattice I is **locally principal** if $I_{(\mathfrak{p})} = I \otimes_R R_{(\mathfrak{p})}$ is a principal $R_{(\mathfrak{p})}$-lattice for all primes $\mathfrak{p}$ of R.

Definition 2.4.3. The product IJ of two R-lattices I and J in a F-algebra B is the R-lattice generated by

$$\{\alpha\beta : \alpha \in I, \beta \in J\},$$

as an R-submodule.

Definition 2.4.4. We say I is **compatible with** J if the right order of I is equal to the left order of J. If this is the case, we call IJ a **compatible product**.

The relation 'is compatible with' is in general neither symmetric nor transitive.

Definition 2.4.5. We say an R-lattice is **integral** if $I^2 \subseteq I$ (the product need not be compatible).

Lemma 2.4.6. Let I be an R-lattice. Then the following are equivalent:

(i) I is integral.

(ii) For all $\alpha, \beta \in I$, we have $\alpha\beta \in I$.

(iii) $I \subseteq \mathcal{O}_L(I)$, so I is a left ideal of $\mathcal{O}_L(I)$ in the usual sense.

(iii') $I \subseteq \mathcal{O}_R(I)$.

(iv) $I \subseteq \mathcal{O}_L(I) \cap \mathcal{O}_R(I)$.

If I is integral, then every element of I is integral over R.

Proof. See [33, Lemma 16.2.8]. □

By Lemma 2.4.6, R-lattice I is integral if and only if $I \subseteq \mathcal{O}_L(I)$. Hence, there exists nonzero $d \in R$ such that dI is integral, so every R-lattice $I = (dI)/d$ is fractional in the sense that it is obtained from an integral lattice with denominator.

Definition 2.4.7. Let $\mathcal{O} \subset B$ be an R-order. A **left fractional $\mathcal{O}$-ideal** is a lattice $I \subseteq B$ such that $\mathcal{O} \subseteq \mathcal{O}_L(I)$ (so $OI \subseteq I$); similarly on the right.

If $\mathcal{O}, \mathcal{O}' \subseteq B$ are R-orders, then a **fractional $\mathcal{O}, \mathcal{O}'$-ideal** is a lattice I that is a left fractional $\mathcal{O}$-ideal and a right fractional $\mathcal{O}'$-ideal.

Proposition 2.4.8. A left ideal $I \subseteq \mathcal{O}$ in the usual sense is an integral left $\mathcal{O}$-ideal in the sense of Definition 2.4.7 if and only if $IF = B$, i.e., I is a (full) R-lattice. (Same for right and two-sided ideals.)

Proof. See [33, 16.2.10]. □

Definition 2.4.9. Let I be a left fractional $\mathcal{O}$-ideal. We say that I is **sated** as a left fractional $\mathcal{O}$-ideal if $\mathcal{O} = \mathcal{O}_L(I)$. We make a similar definition on the right and for two-sided ideals.

Suppose, for a moment, B is semisimple.

Definition 2.4.10. The **reduced norm** $\mathrm{nrd}(I)$ of I is the R-submodule of F generated by the set $\{\mathrm{nrd}(\alpha) : \alpha \in I\}$.

Example 2.4.11. When B is a quaternion algebra over $\mathbb{Q}$, we can define

$$\mathrm{nrd}(I) := \gcd(\{\mathrm{nrd}(\alpha) : \alpha \in I\}),$$

i.e., we can take $\mathrm{nrd}(I)$ to be a positive generator of the finitely generated subgroup of $\mathbb{Q}$ generated by $\mathrm{nrd}(\alpha)$ for $\alpha \in I$.

Definition 2.4.12. Let $I \subseteq B$ be a locally principal R-lattice. We define the **absolute norm** of I to be

$$N(I) := [\mathcal{O}_L(I) : I]_{\mathbb{Z}} = [\mathcal{O}_R(I) : I]_{\mathbb{Z}}.$$

If I is integral then

$$N(I) = \#(\mathcal{O}_L(I)/I) = \#(\mathcal{O}_R(I))/I.$$

If B is simple with $\dim_F B = n^2$ then

$$N(I) = N(\mathrm{nrd}(I))^n.$$

See [33, Chapter 16.4] for full details of the absolute norm.

Now, we drop the condition that B is semisimple and proceed.

Definition 2.4.13. An R-lattice I is **right invertible** if there exists an R-lattice I' in B such that $II' = \mathcal{O}_L(I)$ is a compatible product and similarly I is **left invertible** if $I'I = \mathcal{O}_R(I)$ is a compatible product. An R-lattice I is (two-sided) **invertible** if I is left and right invertible by the same I'.

Definition 2.4.14. We define the **quasi-inverse** of I as

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

If I has a two-sided inverse, then this inverse is uniquely given by I^{-1}.

Lemma 2.4.15. The following statements hold.

(a) The quasi-inverse I^{-1} is an R-lattice and $II^{-1}I \subseteq I$.

(b) If $\mathcal{O}$ is an R-order, then $\mathcal{O}^{-1} = \mathcal{O}$.

Proof. See [33, Lemma 16.5.7]. □

Proposition 2.4.16. The following are equivalent:

(i) I^{-1} is a (two-sided) inverse for I.

(ii) $I^{-1}I = \mathcal{O}_R(I)$ and $II^{-1} = \mathcal{O}_L(I)$.

(iii) I is invertible.

(iv) There is a compatible product $II^{-1}I = I$ and both $1 \in II^{-1}$ and $1 \in I^{-1}I$.

Proof. See [33, Proposition 16.5.8]. □

Proposition 2.4.17. An R-lattice I is an R-order if and only if $1 \in I$, every element of I is integral, and I is invertible.

Proof. See [33, 16.6.12]. □

Proposition 2.4.18. Let I, J are R-lattices. If I is compatible with J and J is invertible, then $\mathcal{O}_L(IJ) = \mathcal{O}_L(I)$.

Proof. See [33, Lemma 16.5.11]. □

Proposition 2.4.19. If I, J are R-lattices and I is compatible with J, then IJ is invertible with $(IJ)^{-1} = J^{-1}I^{-1}$ if and only if both I, J are invertible.

Proof. See [33, Exercise 16.10]. □

Proposition 2.4.20. Let $\mathcal{O}$ be a maximal order in a quaternion algebra B over $\mathbb{Q}$. Then a left or right fractional $\mathcal{O}$-ideal is invertible.

Proof. See [33, 16.1.2]. □

We can generalize this to any quaternion algebras, let B be a quaternion algebra over F and let $I \subset B$ be an R-lattice. If either $\mathcal{O}_L(I)$ or $\mathcal{O}_R(I)$ is maximal, then I is invertible, and both $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$ are maximal [33, Proposition 16.6.15(b)].

Definition 2.4.21. Let $\mathcal{O}, \mathcal{O}' \subseteq B$ be R-orders and let I be a fractional $\mathcal{O}, \mathcal{O}'$-ideal. We say I is **invertible** if I is invertible as a lattice and I is sated (i.e., $\mathcal{O} = \mathcal{O}_L(I)$ and $\mathcal{O}' = \mathcal{O}_R(I)$).

Remark 2.4.22. The condition that I is sated in Definition 2.4.21 is important: we must be careful to work over left and right orders and not some smaller order. Indeed, if I is invertible as an R-lattice then it is invertible as a fractional $\mathcal{O}_L(I), \mathcal{O}_R(I)$-ideal, but not for any strictly smaller order. If I' is an R-lattice and $II' = \mathcal{O}$ for some $\mathcal{O} \subseteq \mathcal{O}_L(I)$, then multiplying on both sides on the left by $\mathcal{O}_L(I)$ gives

$$\mathcal{O} = II' = \mathcal{O}_L(I)II' = \mathcal{O}_L(I)\mathcal{O} = \mathcal{O}_L(I)$$

and the same on the right. In other words, if we are going to call out an invertible fractional ideal by labelling actions on left and right, then we require these labels to be the actual orders that make the inverse work [33, 16.5.18].

We similarly define one-sided invertibility. Recall that R is a Dedekind domain with field of fractions F and B is a finite-dimensional algebra over F with $I \subseteq B$ an R-lattice.

Definition 2.4.23. A right fractional $\mathcal{O}$-ideal I is **right invertible** if I is right invertible as a lattice and I is sated (i.e., $\mathcal{O} = \mathcal{O}_L(I)$). We similarly define **left invertible**.

Proposition 2.4.24. The following are equivalent:

(i) I^{-1} is a right inverse for I.

(ii) I is right invertible.

(iii) There is a compatible product $II^{-1}I = I$ and $1 \in II^{-1}$.

Similar equivalences hold on the left.

Proof. See [33, Proposition 16.7.4]. □

Lemma 2.4.25. Suppose B has a standard involution. Then an R-lattice I is left invertible if and only if I is right invertible if and only if I is invertible.

Proof. See [33, Lemma 16.7.5]. □

Corollary 2.4.26. Suppose R is a Dedekind domain and that B has a standard inovlution. Then an R-lattice I is right invertible with $II' = \mathcal{O}_L(I)$ if and only if $I' = I^{-1}$. A similar statement holds for the left inverse; in particular, this shows that a right inverse is necessarily unique.

Proof. See [33, Corollary 16.7.6]. □

Theorem 2.4.27. Let B be a quaternion algebra over F and let $I \subseteq B$ be an R-lattice. Then the following are equivalent.

(i) I is locally principal.

(ii) I is invertible.

(iii) I is right invertible.

(iii') I is left invertible.

(iv) $\mathrm{nrd}(I)^2 = [\mathcal{O}_R(I) : I]$.

(iv') $\mathrm{nrd}(I)^2 = [\mathcal{O}_L(I) : I]$.

Proof. See [33, Theorem 16.7.7]. □

2.5 Classes of quaterion ideals

Throughout this section, let R be a Dedekind domain with field of fractions $F = \operatorname{Frac} R$, and let B be a simple F-algebra.

Definition 2.5.1. Let $I, J \subseteq B$ be R-lattices, we define the equivalent classes as follows: we say I, J are **in the same right class**, and we write $I \sim_R J$, if there exists $\alpha \in B^\times$ such that $\alpha I = J$. The class of a R-lattice I is denoted $[I]$. Analogous definitions can be made on the left.

When B has a standard involution, the map $I \mapsto \overline{I}$ interchanges left and right.

Lemma 2.5.2. Let $I, J \subseteq$ be R-lattices. Then I, J are in the same right class if and only if I is isomorphic to J as a right module over $\mathcal{O}_R(I) = \mathcal{O}_R(J)$.

Proof. See [33, Lemma 17.3.3]. □

Definition 2.5.3. Let $\mathcal{O} \subset B$ be an order. The **right class set** of $\mathcal{O}$ is

$$\mathrm{Cl}_R \mathcal{O} := \{[I]_R : I \text{ an invertible right fractional } \mathcal{O}\text{-ideal}\}.$$

Recall that, by definition of fractional $\mathcal{O}$-ideal, a representative I in the right class set of $\mathcal{O}$ satisfies $\mathcal{O}_R(I) = \mathcal{O}$.

Note that the (right) class set of $\mathcal{O}$ does not have the structure of a group under multiplication since we have $[\alpha J]_R = [J]_R$ for $\alpha \in B^\times$, but we do not have $[I\alpha J]_R = [IJ]$ in general.

Definition 2.5.4. We say R-orders $\mathcal{O}, \mathcal{O}'$ are **of the same type** if there exists $\alpha \in B^\times$ such that $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$.

Lemma 2.5.5. The R-orders $\mathcal{O}, \mathcal{O}'$ are of the same type if and only if they are isomorphic as R-algebras.

Proof. See [33, Lemma 17.4.2]. □

Remark 2.5.6. [33, 17.4.3] If $\mathcal{O}, \mathcal{O}'$ are of the same type, then an isomorphism $\mathcal{O} \xrightarrow{\sim} \mathcal{O}'$ induces a bijection $\operatorname{Cl}\mathcal{O} \xrightarrow{\sim} \operatorname{Cl}\mathcal{O}'$ of pointed sets. Such an isomorphism is provided by conjugation $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$ for some $\alpha \in B^\times$. The principal lattice $I = \mathcal{O}\alpha = \alpha\mathcal{O}'$ has $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I) = \mathcal{O}'$.

Generalizing this, the class sets of two orders are in bijection if they are connected, in the following sense.

Definition 2.5.7. $\mathcal{O}$ is **connected to** $\mathcal{O}'$ if there exists a locally principal fractional $\mathcal{O}, \mathcal{O}'$-ideal $J \subseteq B$, called a **connecting ideal**.

If B is a quaternion algebra, connecting ideals are invertible fractional $\mathcal{O}, \mathcal{O}$-ideals by definition.

The relation of being connected is an equivalence relation on the set of R-orders. If two R-orders $\mathcal{O}, \mathcal{O}'$ are of the same type, then they are connected by a principal connecting ideal by Remark 2.5.6.

Definition 2.5.8. We say $\mathcal{O}, \mathcal{O}'$ are **locally of the same type** or **locally isomorphic** if $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}'_\mathfrak{p}$ are of the same type (i.e., $\mathcal{O}_\mathfrak{p} \simeq \mathcal{O}'_\mathfrak{p}$) for all primes $\mathfrak{p}$ of R.

Lemma 2.5.9. The R-orders $\mathcal{O}, \mathcal{O}'$ are connected if and only if $\mathcal{O}, \mathcal{O}'$ are locally isomorphic.

Proof. See [33, Lemma 17.4.6]. □

Lemma 2.5.10. If $\mathcal{O}, \mathcal{O}' \subseteq B$ are maximal R-orders, then $\mathcal{O}\mathcal{O}'$ is a $\mathcal{O}, \mathcal{O}'$-connecting ideal.

Proof. See [33, Lemma 17.4.7]. □

Definition 2.5.11. Let $\mathcal{O} \subset B$ be an R-order. The **genus** of $\mathcal{O}$ is the set of R-orders in B locally isomorphic to $\mathcal{O}$. The **type set** $\operatorname{Typ}\mathcal{O}$ of $\mathcal{O}$ is the set of isomorphism classes of orders in the genus of $\mathcal{O}$.

Lemma 2.5.12. Let $\mathcal{O}, \mathcal{O}'$ be connected R-orders, and let J be a connecting $\mathcal{O}, \mathcal{O}'$-ideal. Then maps

$$\begin{aligned} \mathrm{Cl}_R \mathcal{O} &\xrightarrow{\sim} \mathrm{Cl}_R \mathcal{O}' \\ [I]_R &\mapsto [IJ]_R \\ [I'J^{-1}]_R &\hookleftarrow [I']_R \end{aligned} \tag{2.6}$$

are mutually inverse bijections. In particular, if $\mathcal{O}'$ is in the genus set of $\mathcal{O}$ then $\#\,\mathrm{Cl}_R \mathcal{O} = \#\,\mathrm{Cl}_R \mathcal{O}'$.

Proof. See [33, 17.4.11]. □

Lemma 2.5.13. The map

$$\begin{aligned} \mathrm{Cl}_R \mathcal{O} &\to \mathrm{Typ}\, \mathcal{O} \\ [I]_R &\mapsto \text{ class of } \mathcal{O}_L(I) \end{aligned}$$

is a surjective map of sets.

Proof. We follow the proof in [33, Lemma 17.4.13].

If $\mathcal{O}'$ is connected to $\mathcal{O}$, then there is a connecting $\mathcal{O}', \mathcal{O}$-ideal I, and $[I]_R \in \mathrm{Cl}_R \mathcal{O}$ has $\mathcal{O}_L(I) \simeq \mathcal{O}'$. □

Lemma 2.5.14. Let B be a definite quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subseteq B$ be an order. Then the group of units of reduced norm 1

$$\mathcal{O}^1 = \{\alpha \in \mathcal{O} : \mathrm{nrd}(\alpha) = 1\}$$

is a finite group and $\mathcal{O}^\times = \mathcal{O}^1$.

Proof. See [33, Lemma 17.7.13]. □

Proposition 2.5.15. Let B be a definite quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subset B$ be an order.

Then $\mathcal{O}^\times = \mathcal{O}^1$ is a finite group, and every right ideal class in $\mathrm{Cl}_R \mathcal{O}$ is represented by an integral right $\mathcal{O}$-ideal with the absolute norm

$$\mathrm{N}(I) \leq \frac{8}{\pi^2} \mathrm{discrd}(\mathcal{O}),$$

and the right class set of $\mathcal{O}$ is finite.

Proof. See [33, Lemma 17.7.13] and [33, Proposition 17.5.6]. □

Theorem 2.5.16. Let R be a Dedekind domain with field of fractions $F = \operatorname{Frac} R$, let B be a simple F-algebra and let $\mathcal{O} \subseteq B$ be a maximal R-order. If $I \subseteq B$ is an R-lattice such that $\mathcal{O}_L(I) = \mathcal{O}$ or $\mathcal{O}_R(I) = O$, then I is invertible and both $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$ are maximal R-orders.

Proof. See [33, Theorem 18.1.2]. □

For the rest of this section, let B be a simple finite-dimensional F-algebra. Let $\mathcal{O} \subseteq B$ be an R-order.

Definition 2.5.17. A two-sided ideal $P \subseteq \mathcal{O}$ is **prime** if $P \neq \mathcal{O}$ and for all two-sided ideals $I, J \subseteq \mathcal{O}$ we have

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ or } J \subset P.$$

Let $\operatorname{Idl}(\mathcal{O})$ be the set of invertible two-sided fractional $\mathcal{O}$-ideals.

Lemma 2.5.18. The set $\operatorname{Idl}(\mathcal{O})$ is a group under multiplication with identity element $\mathcal{O}$.

Proof. Suppose $I, J \in \operatorname{Idl}(\mathcal{O})$. IJ is invertible as a lattice if and only if I, J are invertible by Proposition 2.4.19. IJ is sated since we have $\mathcal{O}_L(IJ) = \mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(IJ) = \mathcal{O}_R(I) = \mathcal{O}$ by Proposition 2.4.18. □

Let $\operatorname{PIdl}(\mathcal{O}) \leq \operatorname{Idl}(\mathcal{O})$ be the subgroup of principal two-sided fractional $\mathcal{O}$-ideals. Recall that the map

$$\begin{aligned} \operatorname{Cl}_R \mathcal{O} &\to \operatorname{Typ} \mathcal{O} \\ [I]_R &\mapsto \text{ class of } \mathcal{O}_L(I) \end{aligned}$$

is surjective by Lemma 2.5.13. The fiber of this map over the isomorphism class of $\mathcal{O}$ is given by the quotient group $\operatorname{Idl}(\mathcal{O})/\operatorname{PIdl}(\mathcal{O})$ as follows.

Proposition 2.5.19. Let B be a central simple F-algebra and let $\mathcal{O} \subset B$ an R-order. There is a bijection

$$\operatorname{Idl}(\mathcal{O})/\operatorname{PIdl}(\mathcal{O}) \leftrightarrow \{[I]_R \in \operatorname{Cl}_R \mathcal{O} : \mathcal{O}_L(I) \simeq \mathcal{O}\}$$

given by $I \to [I]_R$.

Proof. See [33, Proposition 18.5.10]. □

Definition 2.5.20. Let $\mathcal{O}, \mathcal{O}' \subset B$ be R-orders. A $\mathcal{O}, \mathcal{O}'$-**bimodule** over R is an abelian group M with a left $\mathcal{O}$-module and a right $\mathcal{O}'$-module structure with the same action by R on the left and right (i.e, acting centrally, so $rm = mr$ for all $r \in R$ and $m \in M$).

The R-lattice $I \subseteq B$ is an $\mathcal{O}_L(I), \mathcal{O}_R(I)$-bimodule over R.

Definition 2.5.21. The **Picard group** of $\mathcal{O}$ over R is the group $\mathrm{Pic}_R(\mathcal{O})$ of isomorphism classes of invertible $\mathcal{O}$-bimodules over R under tensor product.

When $R = \mathbb{Z}$, we denote $\mathrm{Pic}(\mathcal{O}) := \mathrm{Pic}_R(\mathcal{O})$.

Remark 2.5.22. If $I \subseteq B$ is an R-lattice that is a fractional two-sided $\mathcal{O}$-ideal, then I is a $\mathcal{O}$-bimodule over R. Conversely, if I is a $\mathcal{O}$-bimodule over R then $I \otimes_R F \simeq B$ as B-bimodules, and choosing such an isomorphism gives an embedding $I \hookrightarrow B$ as an R-lattice [33, 18.4.3].

Lemma 2.5.23. Let $I, J \subseteq B$ be R-lattices that are fractional two-sided $\mathcal{O}$-ideals. Then I is isomorphic to J as $\mathcal{O}$-bimodules over R if and only if there exists $a \in F^\times$ such that $J = aI$.

Proof. See [33, Lemma 18.4.4]. □

Let $N_{B^\times}(\mathcal{O}) := \{\alpha \in B^\times \alpha\mathcal{O} = \mathcal{O}\alpha\}$ be the normalizer of $\mathcal{O}$ in B.

Theorem 2.5.24. Let B be a quaternion algebra over $\mathbb{Q}$ of discriminant $D := \mathrm{disc}\, B$, and let $\mathcal{O} \subset$ be a maximal order. Then

$$\mathrm{Pic}\, \mathcal{O} \simeq \prod_{p \mid D} \mathbb{Z}/2\mathbb{Z}$$

generated by (unique) prime two-sided $\mathcal{O}$-ideals with reduced norm $p \mid D$, and there is an exact sequece

$$\begin{aligned} 0 \to N_{B^\times}(\mathcal{O})/(\mathbb{Q}^\times \mathcal{O}^\times) &\to \mathrm{Pic}\, \mathcal{O} \to \mathrm{Idl}(\mathcal{O})/\,\mathrm{PIdl}(\mathcal{O}) \to 0 \\ \alpha(\mathbb{Q}^\times \mathcal{O}^\times) &\mapsto [\mathcal{O}\alpha\mathcal{O}]. \end{aligned}$$

Proof. See [33, Proposition 18.5.3]. □

2.6 Special maximal orders

The following gives explicit descriptions of the quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞ and some explicit maximal orders.

Proposition 2.6.1. Let p be a prime. Then the (unique) quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified precisely at p and ∞ is given by:

$$B_{p,\infty} = \begin{cases} (-1,-1) & \text{if } p = 2, \\ (-1,-p) & \text{if } p \equiv 3 \mod 4, \\ (-2,-p) & \text{if } p \equiv 5 \mod 8, \\ (-p,-q) & \text{if } p \equiv 1 \mod 8 \end{cases}$$

where q is a prime with $q \equiv 3 \bmod 4$ and $(p/q) = -1$.

Proof. See [29, Proposition 5.1]. □

Proposition 2.6.2. Let p be a prime and let $B_{p,\infty} = (a, b \mid \mathbb{Q})$ be the quaternion algebra given by Proposition 2.6.1 above. Then a maximal order $\mathcal{O}_0$ of $B_{p,\infty}$ is given by the $\mathbb{Z}$-basis:

p	(a, b)	$\mathcal{O}_0$ [17]
$p = 2$	$(-1, -1)$	$\langle \frac{1+i+j+k}{2}, i, j, k \rangle$
$3 \bmod 4$	$(-p, -1)$	$\langle 1, j, \frac{1+k}{2}, \frac{i+j}{2} \rangle$
$5 \bmod 8$	$(-p, -2)$	$\langle 1, j, \frac{2-j+k}{4}, \frac{-1+i+j}{2} \rangle$
$1 \bmod 8$	$(-p, -q)$	$\langle \frac{1+j}{2}, \frac{i+k}{2}, \frac{j+ck}{q}, k \rangle$

Here $1, i, j, k$ is the standard basis of $B_{p,\infty}$, $q \equiv 3 \bmod 4$ is an integer such that $(p/q) = -1$, and c is an integer such that $q \mid c^2 p + 1$. Assuming the generalized Riemann hypothesis (GRH) is true, there exists $q = O((\log p)^2)$ satisfying these conditions [2] (as $(q/p) = (p/q) = -1$)), and all $\mathbb{Z}$-bases have polynomial representation size in terms of $1, i, j, ij$.

We can compute the discriminant of $\mathcal{O}_0$ to check it is maximal. For example, when $p \equiv 3 \pmod 4$, the discriminant of $\mathcal{O}_0 = \langle 1, j, \frac{1+k}{2}, \frac{i+j}{2} \rangle$ is

$$\operatorname{disc} \mathcal{O}_0 = \begin{vmatrix} 2 & 0 & 1 & 0 \\ 0 & -2 & 0 & -1 \\ 1 & 0 & \frac{1-p}{2} & 0 \\ 0 & -1 & 0 & \frac{p+1}{2} \end{vmatrix} = -p^2.$$

Hence $\operatorname{discrd} \mathcal{O}_0 = p = \operatorname{disc} B$ and $\mathcal{O}_0$ is maximal.

In all cases the maximal order $\mathcal{O}_0$ given by Proposition 2.6.2 contains $\langle 1, i, j, k \rangle$ as a small index subring.

We will now prove that every conjugacy class of maximal orders has a representative whose basis has representation size $O(\log p)$ when written in terms of the standard basis $1, i, j, ij$ for $B_{p,\infty}$. The following arguments are taken from [22].

Note that $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to $\mathbb{H}$, the Hamiltonian quaternions. Let $1, i', j, i'j'$ be the basis of $\mathbb{H}$ with $i'^2 = j'^2 = -1$. Let $f : B_{p,\infty} \otimes \mathbb{R} \to \mathbb{H}$ be the isomorphism given by $i, j \mapsto \sqrt{q}i', \, j'$. Then the norm on $\mathbb{H}$, which is the square of the standard Euclidean norm on $\mathbb{R}^4$, is just the reduced norm on the image of $\mathbb{B}_{p,\infty}$ in $\mathbb{H}$ under the isomorphism. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Define its **covolume**, denoted $\operatorname{Covol}(\Lambda)$, to be $\sqrt{\det(L^T L)}$ for any matrix L consisting of a basis for Λ. If $\mathcal{O} \subseteq B_{p,\infty}$ is a lattice, define its covolume to be $\operatorname{Covol}(f(\mathcal{O}))$.

Proposition 2.6.3. Let $\mathcal{O}$ be a lattice in $B_{p,\infty}$. Then $\operatorname{Covol}(\mathcal{O})^2 = \frac{1}{16} \operatorname{disc}(\mathcal{O})$.

Proof. See [17, Proposition 2]. □

Let $\|\cdot\|_2$ denote the Euclidean norm.

Definition 2.6.4. A basis $\{v_1, \cdots, v_n\}$ of a lattice $\Lambda \subseteq \mathbb{R}^n$ is **Minkowski-reduced** if for $1 \leq k \leq n$, the element v_k satisfies

$$\|v_k\|_2 \leq \|v_k'\|_2,$$

for any v_k' such that the sequence $v_1, \ldots, v_{k-1}, v_k'$ can be completed to a basis for Λ.

Definition 2.6.5. Let Λ be a lattice in $\mathbb{R}^n$. We define the i**th successive minimum of** Λ, denoted $\lambda_i(\Lambda)$, to be the smallest nonnegative, real number r such that there are i linearly independent lattice vectors of Λ contained in the closed ball of radius r centered at the origin. So $\lambda_1(\Lambda)$ is the length of a shortest nonzero vector of Λ.

For $n \leq 4$, there is a basis $v_1, \cdots, v_n$ of Λ such that $\|v_i\|_2 = \lambda_i(\Lambda)$ [28], which implies such a basis is Minkowski-reduced. When we refer to a Minkowski-reduced basis, we will always assume we choose such a basis.

Theorem 2.6.6. Every conjugacy class of maximal orders in $B_{p,\infty}$ has a $\mathbb{Z}$-basis $x_1, \cdots, x_4$ with $\mathrm{nrd}(x_i) \in O(p^2)$. If we express x_r (for $1 \leq r \leq 4$) as a coefficient vector in terms of $1, i, j, ij$, then the rational numbers appearing have numerators and denominators whose representation size are polynomial in $\log p$.

Proof. See [17, Theorem 2].

□

Chapter 3

Elliptic Curves

3.1 Overview

Let K be a field of $\operatorname{char} K \neq 2, 3$ with an algebraic closure K^{al}.

Definition 3.1.1. An **elliptic curve** $E \subset \mathbb{P}^2 := \mathbb{P}^2(K^{\mathrm{al}})$ defined over K, denoted E/K, is a nonsingular projective curve of genus one whose points satisfy a **Weierstrass equation**

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

where $A, B \in K$ with the **discriminant** $\Delta := 4A^3 + 27B^2 \neq 0$.

We often write E using the dehomogenization of its Weierstrass equation

$$E : y^2 = x^3 + Ax + B,$$

where $x = X/Z$ and $y = Y/Z$. Note that E has a special point $O = [0, 1, 0]$, the point at infinity.

The points of E form an abelian group with identity O. Any projective lines in $\mathbb{P}^2$ intersect E at exactly three points, where the three points may not be distinct if the line is tangent to E. This gives the geometric composition law on E as follows; let $P, Q \in E$, let L be the line through P and Q, and let R is the third point of intersection of L with E. If L' is the line through R and O, then L' intersects E at R, O, and a third point. We denote the third point by $P + Q$.

Definition 3.1.2. The set of **K-rational points** of E is the subgroup

$$E(K) = \left\{(x, y) \in K^2 : y^2 = x^3 + Ax + B\right\} \cup \{O\}.$$

Definition 3.1.3. For an elliptic curve E, the constant

$$j(E) := \frac{256 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$$

is called the j**-invariant** of E.

An elliptic curve E can be identified with its j-invariant. The only change of variables fixing $[0,1,0]$ and preserving the Weierstrass form of the equation is

$$x = u^2x' \text{ and } y = u^3y'$$

for some nonzero $u \in K^{\text{al}}$. After change of varaibles, new constants for the Weierstrass equation are given by

$$u^4A' = A \text{ and } u^6B' = B.$$

These change of variables fix j-invariant as well. Indeed, two elliptic curves E', E are isomorphic over K^{al} if and only if $j(E) = j(E')$ [31, Proposition 1.4]. Moreover, if $j \in K^{\text{al}}$ then there exists an elliptic curve defined over $K(j)$ whose j-invariant is equal to j; let $E(j)$ be an elliptic curve given by

$$E(j) := \begin{cases} E : y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728} & \text{if } j \neq 0, 1728, \\ E : y^2 = x^3 + 1 & \text{if } j = 0, \\ E : y^2 = x^3 + x & \text{if } j = 1728. \end{cases}$$

Then the j-invariant of E is j.

Recall that a curve is a variety of dimension one. Now we review some aspects of it as a variety. Then some of definition will naturally follow.

The Galois group $\text{Gal}(K^{\text{al}}/K)$ acts on $\mathbb{P}^n$ by acting on homogeneous coordinates; for $\sigma \in \text{Gal}\,(K^{\text{al}}/K)$ and $P = [x_0, \cdots, x_n] \in \mathbb{P}^n$,

$$P^\sigma := [\sigma(x_0), \cdots, \sigma(x_n)].$$

This action is well-defined, independent of choice of homogeneous coordinates.

Let $V \subseteq \mathbb{P}^n$ be a projective variety and let $K^{\text{al}}[X] = K^{\text{al}}[X_0, \cdots, X_n]$ be a polynomial ring. If $f \in K^{\text{al}}[X]$ is a homogeneous polynomial, then $\text{Gal}\,(K^{\text{al}}/K)$ acts on f by acting on its coefficients so that

$$f(P)^\sigma = f(P^\sigma),$$

for any $P \in \mathbb{P}^n$ and $\sigma \in \text{Gal}\,(K^{\text{al}}/K)$.

Suppose V is defined over K. The action of $\text{Gal}\,(K^{\text{al}}/K)$ on $\mathbb{P}^n$ induces an action on V. Moreover, $\text{Gal}\,(K^{\text{al}}/K)$ fixes the ideal $I(V)$ of V, so we obtain an action of $\text{Gal}\,(K^{\text{al}}/K)$ on the coordinate ring $K^{\text{al}}[V]$ and the function field $K^{\text{al}}(V)$. If we denote the action of $\sigma \in \text{Gal}\,(K^{\text{al}}/K)$ on f by f^σ, then for all points $P \in V$,

$$(f(P))^\sigma = f^\sigma(P^\sigma).$$

Let $\phi : V_1 \to V_2$ be a rational map between varieties. If V_1 and V_2 are defined over K, then $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ acts on ϕ; if $\phi(P) = [f_0(P), \cdots, f_n(P)] \in E_2$ where $f_0, \cdots, f_n \in K^{\mathrm{al}}(E_1)$, then

$$\phi^\sigma(P) = [f_0^\sigma(P), \cdots, f_n^\sigma(P)].$$

Notice that we have the formula

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma)$$

for all $\sigma \in \mathrm{Gal}\,(K^{\mathrm{al}}/K)$ and $P \in E_1$. Hence, ϕ is defined over K if and only if $\phi = \phi^\sigma$ for all $\sigma \in \mathrm{Gal}\,(K^{\mathrm{al}}/K)$.

Definition 3.1.4. A rational map ϕ is **defined over** K if it commutes with the action of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$, i.e., $\phi(P)^\sigma = \phi(P^\sigma)$.

Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a nonconstant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K,

$$\phi^* : K(C_2) \to K(C_1), \phi^* f = f \circ \phi$$

called the **pullback** of ϕ. Note that if ϕ is a nonconstant map defined over K, then $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$.

Theorem 3.1.5. Let $\phi : C_1, \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.

Proof. See [31, Theorem II.2.3]. □

Definition 3.1.6. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the **degree** of ϕ to be 0. Otherwise we say that ϕ is a **finite map** and we define its **degree** to be

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

We say that ϕ is **separable**, **inseparable**, or **purely inseparable** if the field extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$ respectively.

Definition 3.1.7. Let E_1 and E_2 be elliptic curves. An **isogeny** from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2$$

which sends O to O. Two elliptic curves are **isogenous** if there is a nonzero isogeny between them.

Since a morphism between curves is either constant or surjective by Theorem 3.1.5, we have either $\phi(E_1) = \{\mathcal{O}\}$ or $\phi(E_1) = E_2$. Then for a nonzero isogeny $\phi : E_1/K^{\mathrm{al}} \to E_2/K^{\mathrm{al}}$, we can

define the pullback ϕ^* and the degrees $\deg \phi, \deg_i \phi$, and $\deg_s \phi$ as a rational map as in Definition 3.1.6. We set $\deg[0] = 0$ so that for chain of isogenies $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$, we have

$$\deg(\psi\phi) = \deg(\psi)\deg(\phi),$$

where $\psi\phi := \psi \circ \phi$.

Next, we look at the algebraic structures on the set of isogenies $\mathrm{Hom}(E_1, E_2)$ from E_1 to E_2. Elliptic curves are abelian groups, so $\mathrm{Hom}(E_1, E_2)$ form a group, where the sum of two isogenies is defined by

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

(see [31, Theorem III.4.8]). If $E_1 = E_2$, then we can also compose isogenies. Thus if E is an elliptic curve, the set of endomorphisms $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring whose multiplication is composition.

Definition 3.1.8. Let $m \in \mathbb{Z}$. Denote

$$mP := P + \cdots + P \ (m \text{ times})$$

if $m > 0$, and let $mP := (-m)(-P)$ if $m < 0$ and let $0P = O$. **The multiplication-by-m map**, denoted $[m]$, on an elliptic curve E is an endomorphism on E that sends P to mP. In particular, $[0]$ is the zero isogeny.

Proposition 3.1.9. The following statements hold.

(a) Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$. Then the multiplication-by-m map $[m] : E \to E$ is nonconstant.

(b) Let E_1 and E_2 be elliptic curves. Then the group of isogenies

$$\mathrm{Hom}(E_1, E_2)$$

is a torsion-free $\mathbb{Z}$-module.

(c) Let E be an elliptic curve. Then the endomorphism ring $\mathrm{End}(E)$ is a ring of characteristic 0 with no zero divisors.

Proof. See [31, Proposition III.4.2]. □

Definition 3.1.10. Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The **m-torsion subgroup** of E, denoted by $E[m]$, is the set of points of E of order dividing m.

An important fact about the multiplication-by-m map is that it has degree m^2, from which one can deduce the structure of the finite group $E[m]$.

Definition 3.1.11. Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m. As shown in Theorem [31, Corollary III.6.1(a)], there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [m]$. Such an isogeny is called the **dual isogeny** to ϕ.

The following theorem summarizes the properties of the dual isogeny.

Theorem 3.1.12. Let $\phi : E_1, \to E_2$ be an isogeny with $\deg \phi = m$. Then

(a) $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.

(b) Let $\lambda : E_2 \to E_3$ be another isogeny. Then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

(e) $\deg \hat{\phi} = \deg \phi$.

(f) $\hat{\hat{\phi}} = \phi$.

Proof. See [31, Theorem III.6.2]. □

Definition 3.1.13. Let A be an abelian group. A map

$$d : A \to \mathbb{R}$$

is a **quadratic form** if it satisfies the following conditions:

(i) $\mathrm{d}(\alpha) = d(-\alpha)$ for all $\alpha \in A$.

(ii) The pairing

$$\begin{aligned} A \times A &\to \mathbb{R} \\ (\alpha, \beta) &\mapsto d(\alpha + \beta) - d(\alpha) - d(\beta), \end{aligned}$$

is bilinear.

A quadratic form d is **positive definite** if it further satisfies:

(iii) $d(\alpha) \geq 0$ for all $\alpha \in A$.

(iv) $d(\alpha) = 0$ if and only if $\alpha = 0$.

Remark 3.1.14. Note that the dual $\widehat{\ }$ is a standard involution (2.1.11) on $\mathrm{End}(E)$ with the induced norm $\mathrm{nrd}(\phi) := \phi\hat{\phi}$, which is positive by the following corollary.

Corollary 3.1.15. Let E_1 and E_2 be elliptic curves. The degree map

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

is a positive definite quadratic form.

Proof. See [31, Corollary III.6.3]. □

Definition 3.1.16. Let K be a field of characteristic $p > 0$, let $q = p^r$, and let E/K be an elliptic curve. The curve $E^{(q)}/K$ is defined by raising the coefficients of the equation for E to the qth power, and the **qth power Frobenius morphism** π is defined by

$$\begin{aligned} \pi : E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q). \end{aligned}$$

By working on Weierstrass coefficients, one can show that $j(E^{(q)}) = j(E)^q$.

Remark 3.1.17. Suppose $E/\mathbb{F}_q$ is an elliptic curve. Since the qth power map on $\mathbb{F}_q$ is the identity, $E^{(q)} = E$ and π is an endomorphism of E, called the **Frobenius endomorphism**. Also, since the Galois group $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{al}})/\mathbb{F}_q$ is (topologically) generated by the qth power map on $\mathbb{F}_q^{\mathrm{al}}$, we see that for any point $P \in E(\mathbb{F}_q^{\mathrm{al}})$,

$$P \in E(\mathbb{F}_q) \quad \text{if and only if} \quad \pi(P) = P$$

[31, Example III.4.6].

Proposition 3.1.18. Let π be the qth power Frobenius endomorphism. Then π is purely inseparable and $\deg \pi = q$.

Proof. See [31, Proposition II.2.11]. □

Proposition 3.1.19. Let $\phi : E_1 \to E_2$ be an isogeny between elliptic curves over a field of characteristic $p > 0$ and let $q = \deg_i(\phi)$. Then ϕ factors through π, the qth power Frobenius map,

$$E_1 \xrightarrow{\pi} E_1^{(q)} \xrightarrow{\psi} E_2,$$

where the map ψ is separable.

Proof. See [31, Corollary II.2.12]. □

Remark 3.1.20. Proposition 3.1.19 implies that $\deg_i \phi$ is a power of p.

Corollary 3.1.21. Let E_1, E_2 be elliptic curves over a field of characteristic p and let ϕ be a degree ℓ-isogeny where ℓ is coprime to p. Then ϕ is separable.

Proof. Suppose ϕ is not separable. ϕ factors through qth power Frobenius map π for some $q = p^r, r > 0$. Since $\ell = \deg \phi = \deg_s \phi \deg \pi = (\deg_s \phi)q$ and ℓ is coprime to p, we have a contradiction and ϕ must be separable. □

Theorem 3.1.22. Let $\phi : E_1 \to E_2$ be a nonzero isogeny.

(a) For every $Q \in E_2$,

$$\#\phi^{-1}(Q) = \deg_s \phi.$$

Further, for every $P \in E_1$,

$$e_\phi(P) = \deg_i \phi.$$

(b) Suppose that ϕ is separable. Then ϕ is unramified,

$$\#\ker \phi = \deg \phi,$$

and $K^{\mathrm{al}}(E_1)$ is a Galois extension of $\phi^* K^{\mathrm{al}}(E_2)$.

(see [31, II.2] for the ramification index $e_\phi(P)$ of ϕ at P and unramified map of smooth curves)

Proof. See [31, Theorem III.4.10]. □

Corollary 3.1.23. Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be nonconstant isogenies, and assume that ϕ is separable. If $\ker \phi \subset \ker \psi$, then there is a unique isogeny $\lambda : E_2 \to E_3$ such that $\psi = \lambda \circ \phi$.

Proof. See [31, Corollary III.4.11]. □

Proposition 3.1.24. Let E be an elliptic curve and let $G \subseteq E$ be a finite subgroup. There are a unique elliptic curve E' and a separable isogeny $\phi : E \to E'$ such that $\ker \phi = G$.

Proof. See [31, Proposition III.4.12]. □

We will discuss how to explicitly write down equations for the curve $E' = E/G$ and isogeny $\phi : E \to E'$ in the next section.

Corollary 3.1.25. Let E/K be an elliptic curve, let $m \in \mathbb{Z}$ with $m \neq 0$, and let π be the pth power Frobenius map.

(a) $\deg[m] = m^2$.

(b) If either $\mathrm{char}\, K = 0$ or $p = \mathrm{char}\, K$ and $p \nmid m$, then $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(c) Suppose $\mathrm{char}(K) = p > 0$ and $m = p^e$ for some integer $e \geq 1$. Then

$$E[m] = \begin{cases} \{O\} & \text{if } \hat{\pi} \text{ is inseparable,} \\ \mathbb{Z}/m\mathbb{Z} & \text{if } \hat{\pi} \text{ is separable.} \end{cases}$$

Proof. See [31, Corollary III.6.4]. □

Corollary 3.1.26. Let E/K be an elliptic curve with $\operatorname{char} K = p$ and let $m \in \mathbb{Z}$ with $m \neq 0$. The multiplication-by-m map $[m]$ is separable if and only if $p \nmid m$.

Proof. If $[m]$ is separable, then

$$\#E[m] = \#\ker[m] = \deg[m] = m^2$$

by Theorem 3.1.22. It follows that we must have $p \nmid m$ by Corollary 3.1.25.

Conversely, suppose $p \nmid m$. Then $\deg[m] = m^2$ is coprime to p, so $[m]$ is separable by Corollary 3.1.21. □

Now, we give a characterization of the endomorphism ring $\operatorname{End}(E)$.

Corollary 3.1.27. Let E_1 and E_2 be elliptic curves. Then

$$\operatorname{Hom}(E_1, E_2)$$

is a free $\mathbb{Z}$-module of rank at most 4.

Proof. See [31, Corollary III.7.5]. □

Theorem 3.1.28. Let R be a ring of characteristic 0 having no zero divisors, and assume that R has the following properties:

(i) R has rank at most 4 as $\mathbb{Z}$-module.

(ii) R has an anti-involution $\alpha \mapsto \hat{\alpha}$ satisfying

$$\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}, \quad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \quad \hat{\hat{\alpha}} = \alpha, \quad \hat{a} = a \text{ for } a \in \mathbb{Z} \subset R.$$

(iii) For $\alpha \in R$, the product $\alpha\hat{\alpha}$ is a nonnegative integer, and $\alpha\hat{\alpha} = 0$ if and only if $\alpha = 0$.

Then R is one of the following types of rings:

(a) $R \simeq \mathbb{Z}$.

(b) R is an order in an imaginary quadratic extension of $\mathbb{Q}$.

(c) R is an order in a definite quaternion algebra over $\mathbb{Q}$.

Proof. See [31, Theorem III.9.3]. □

Corollary 3.1.29. Let E/K be an elliptic curve. Then one of the following hold:

(i) $\mathrm{End}(E) = \mathbb{Z}$.

(ii) $\mathrm{End}(E)$ is an order in an imaginary quadratic field.

(iii) $\mathrm{End}(E)$ is an order in a definite quaternion algebra over $\mathbb{Q}$.

In particular, if $\mathrm{char}(K) = 0$, then $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field. [31, Corollary III.9.4].

Proof. We show that the ring $\mathrm{End}(E)$ satisfies all three conditions in Theorem 3.1.28. $\mathrm{End}(E)$ is of characteristic 0 and it has no zero divisors by Proposition 3.1.9, and it is a $\mathbb{Z}$-module with rank at most 4 by Corollary 3.1.27. $\mathrm{End}(E)$ has an anti-involution given by $\phi \mapsto \hat{\phi}$ by Theorem 3.1.12bcf. Lastly, the product $\phi\hat{\phi}$ is a non-negative integer by Theorem 3.1.12a, and for an isogeny $\phi \in \mathrm{End}(E)$ with $\deg \phi = m$,

$$\begin{aligned} \phi\hat{\phi} = 0 &\iff \deg(\phi\hat{\phi}) = \deg([m]) = 0 \ \because \text{ Corollary 3.1.15} \\ &\iff \phi = 0. \end{aligned}$$

When $\mathrm{char}(K) = 0$, then $\mathrm{End}(E)$ is a commutative ring [31, Corollary III.5.6c], so it can't be an order in a quaternion algebra. □

Remark 3.1.30. From Corollary 3.1.29, if we are given the rank of $\mathrm{End}(E)$ as a $\mathbb{Z}$-module, then we can determine which of the three cases holds for $\mathrm{End}(E)$; $\mathrm{End}(E) = \mathbb{Z}$ if it is of rank 1, $\mathrm{End}(E) = \mathcal{O}$ is an order in an imaginary quadratic field K if it is of rank $2 = [K : \mathbb{Q}]$, and $\mathrm{End}(E) = \mathcal{O}'$ is an order in a definite quaternion algebra B over $\mathbb{Q}$ if it is of rank $4 = [B : \mathbb{Q}]$.

Let E/K be an elliptic curve with $\mathrm{char}\, K = p$. Recall that $E[p]$ is either cyclic of order p or trivial by Corollary 3.1.25. The terms ordinary and supersingular distinguish these two cases.

Theorem 3.1.31. Let K be a field of characteristic p, and let E/K be an elliptic curve. For each integer $r \geq 1$, let ϕ_r be the p^r-power Frobenius map. The following are equivalent.

(i) $E[p^r] = 0$ for one (all) $r \geq 1$.

(ii) $\hat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$.

(iii) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

(iv) $\mathrm{End}(E)$ is an order in a quaternion algebra.

(v) The formal group $\hat{E}/K$ associated to E has height 2.

Furthermore, if the equivalent conditions do not hold, then

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$$

for all $r \geq 1$, and the formal group $\hat{E}/K$ has height 1. If further $j(E) \in \overline{\mathbb{F}}_p$, then $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

Proof. See [31, Theorem V.3.1]. □

Definition 3.1.32. If E satisfies the equivalent conditions in Theorem 3.1.31, then we say E is **supersingular**. Otherwise we say that E is **ordinary**.

Let E be a supersingular elliptic curve over K^{al} with $\mathrm{char}\, K = p$. By Theorem 3.1.31, the curve has a representative defined over $\mathbb{F}_{p^2}$, so we will assume that $K = \mathbb{F}_{p^2}$.

Example 3.1.33. Since a supersingular curve has j-invariant in $\mathbb{F}_{p^2}$, one can easily check that the only supersingular curve over $\mathbb{F}_2^{\mathrm{al}}$ is

$$E : y^2 + y = x^3.$$

Definition 3.1.34. Let E be an elliptic curve and let $\ell \in \mathbb{Z}$ be a prime. The **ℓ-adic Tate module** of E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

the inverse limit being taken with respect to the natural maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

The Tate module is a $\mathbb{Z}_\ell$-module since $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module for each ℓ.

Let E/K be an elliptic curve and let $m \geq 2$ be an integer, prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$. Note that $\sigma \in \mathrm{Gal}\,(K^{\mathrm{al}}/K)$ acts on $E[m]$; if $P \in E[m]$, then

$$[m](P^\sigma) = ([m]P)^\sigma = O^\sigma = O.$$

We thus obtain a representation

$$\mathrm{Gal}\,(K^{\mathrm{al}}/K) \to \mathrm{Aut}(E[m]).$$

The action of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ on each $E[\ell^n]$ commutes with the multiplication-by-ℓ map, so $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ also acts on $T_\ell[E]$.

Definition 3.1.35. The **ℓ-adic representation** (of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ associtated to E) is the homomorphism

$$\rho_\ell : \mathrm{Gal}\,(K^{\mathrm{al}}/K) \to \mathrm{Aut}(T_\ell(E))$$

induced by the action of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ on the ℓ^n-torsion points of E.

Proposition 3.1.36. The Tate module has the following structure:

(a) $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module if $\ell \neq \mathrm{char}(K)$.

(b) $T_p(E) \simeq \{0\}$ or $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module if $p = \mathrm{char}(K) > 0$. [31, Proposition III.7.1]

Proof. This is an immediate consequence of Corollary 3.1.25. □

Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves over K^{al}. Let $\ell \neq \mathrm{char}\, K$ be a prime. Then ϕ induces maps

$$\phi : E_1[\ell^n] \to E_2[\ell^n],$$

and hence it induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2).$$

We thus obtain a natural homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

This map is injective, but much stronger result about the structure of $\mathrm{Hom}(E_1, E_2)$ can be shown.

Theorem 3.1.37. Let E_1 and E_2 be elliptic curves and let $\ell \neq \mathrm{char}(K)$ be a prime. Then the natural map

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)), \quad \phi \mapsto \phi_\ell$$

is injective.

Proof. See [31, Theorem III.7.4]. □

Definition 3.1.38. Recall that an isogeny is defined over K if it commutes with the action of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$. We similarly define $\mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ to be the group of $\mathbb{Z}_\ell$-linear maps from $T_\ell(E_1)$ to $T_\ell(E_2)$ that commute with the action of $\mathrm{Gal}\,(K^{\mathrm{al}}/K)$ as given by the ℓ-adic representation.

Theorem 3.1.39. (Tate's Isogeny Theorem)
Let $\ell \neq \mathrm{char}(K)$ be a prime. The natural map

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$$

is an isomorphism in the following two situations:

(a) K is a finite field.

(b) K is a number field.

Proof. See [31, Theorem III.7.7]. □

Corollary 3.1.40. Let $E/K, E'/K$ be elliptic curves over a finite field K. Then E, E' are isogenous over K if and only if $\#E(K) = \#E'(K)$. It follows that any two supersingular elliptic curves over a finite field are isogenous. [31, Exercise V.5.4]

Proof. See [32] and note the Tate modules of two elliptic curves over a finite field are isomorphic if and only if they have the same number of points. □

Proposition 3.1.41. Let E, E' be elliptic curves over K that are isogenous. Then E is supersingular if and only if E' is supersingular.

Proof. This was shown in the proof of Theorem 3.1.31. Let $[p], [p]'$ are multiplication-by-p on E, E' respectively. Suppose $\phi : E \to E'$ be a nonconstant isogeny. Since $\phi \circ [p] = [p]' \circ \phi$, we have $\deg[p] = \deg[p]'$ by comparing degrees and cancelling $\deg \phi$. Also, by comparing inseparable degree, $\deg[p] = \deg_i[p] = \deg_i[p]'$ since $[p] : E \to E$ is purely inseparable. It follows that $[p]'$ is purely inseparable. Hence $\#E'[p] = \deg_s[p]' = 1$ by Theorem 3.1.22, i.e., $E[p] = 0$, so by Theorem 3.1.31, $[p]'$ is supersingular. □

The following result from [3] provides information about the fields of definition of endomorphisms of supersingular elliptic curves.

Proposition 3.1.42. Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then $\mathrm{End}_{\mathbb{F}_{p^{2d}}}(E) = \mathrm{End}(E)$ where $d = 1$ if $j(E) \neq 0, 1728$, $d = 1, 3$ if $j(E) = 0$, and $d = 1, 2$ if $j(E) = 1728$.

Proof. See [3, Proposition 2.4]. □

See [3, Corollary 2.5] for a similar result for homomorphisms.

3.2 Vélu's formula

Recall that for a given finite subgroup G of an elliptic curve E, there exists a unique elliptic curve E' and a separable isogeny $\phi : E \to E'$ whose kernel is G by Proposition 3.1.24. We now give an explicit formulation of E' and ϕ due to Vélu.

Theorem 3.2.1. Let E be an elliptic curve over a field K defined by

$$F(x, y) = x^3 + Ax + B - y^2 = 0$$

in Weierstrass form. Let $G \subset E(K^{\mathrm{al}})$ be a finite subgroup. Let G_2 be the set of points in G of order 2 and let $G_1 \subseteq G$ be a subset such that

$$\#G = 1 + \#G_2 + 2\#G_1 \text{ and } G = \{O_E\} \cup G_2 \cup G_1 \cup \{-Q : Q \in G_1\}.$$

Write

$$F_x = \frac{\partial F}{\partial x} = 3x^2 + A \text{ and } F_y = \frac{\partial F}{\partial y} = -2y.$$

For a point $Q = (x_Q, y_Q) \in G_1 \cup G_2$ define the quantities

$$u(Q) = (F_y(Q))^2 = (-2y_Q)^2$$

and

$$t(Q) = \begin{cases} F_x(Q) & \text{if } Q \in G_2, \\ 2F_x(Q) - a_1 F_y(Q) & \text{if } Q \in G_1. \end{cases}$$

Note that if $Q \in G_2$ then $F_y(Q) = 0$ and so $u(Q) = 0$.

Define

$$t(G) = \sum_{Q \in G_1 \cup G_2} t(Q) \text{ and } w(G) = \sum_{Q \in G_1 \cup G_2} (u(Q) + x_Q t(Q))$$

and set

$$C = A - 5t(G) \text{ and } D = B - 7w(G).$$

Then the map $\phi : (x, y) \mapsto (X, Y)$ where

$$X = x + \sum_{Q \in G_1 \cup G_2} \frac{t(Q)}{x - x_Q} + \frac{u(Q)}{(x - x_Q)^2}$$

and

$$Y = y - \sum_{Q \in G_1 \cup G_2} u(Q)\frac{2y}{(x - x_Q)^3} + t(Q)\frac{y - y_Q}{(x - x_Q)^2} - \frac{F_x(Q)F_y(Q)}{(x - x_Q)^2}$$

is a separable isogeny from E to

$$E' : Y^2 = X^3 + CX + D$$

with kernel G.

Proof. See [18, Theorem 25.1.6]. □

Definition 3.2.2. We say that two separable isogenies $\phi_1, \phi_2 : E \to E'$ are **equivalent isogenies** if $\ker(\phi_1) = \ker(\phi_2)$.

Theorem 3.2.3. Let E, G, and ϕ be defined as in Theorem 3.2.1. Let $\psi : E \to E'$ be another isogeny over K such that $\ker(\psi) = G$. Then

$$\psi = \lambda \circ \phi$$

for an automorphism λ of E'. Similarly, if $\psi : E \to E''$ is an isogeny over K with $\ker(\psi) = G$ then

$$\psi = \lambda \circ \phi$$

where $\lambda : E' \to E''$ is an isomorphism over K of elliptic curves. [18, Exercise 9.6.20].

Remark 3.2.4. Equivalent isogenies define an equivalence class of isogenies. The isogeny in Proposition 3.1.24 given by the finite subgroup G may not be unique, but Theorem 3.2.3 says that it is unqiue in a sense that all such isogenies would be in the same class. Furthermore, Velu's formula gives a fixed choice of representative of the class.

Theorem 3.2.5. Let $\phi : E \to E'$ be a separable isogeny. If $\lambda \in \mathrm{Aut}(E')$ then $\lambda \circ \phi$ is equivalent to ϕ. Note that $\phi \circ \lambda$ is not necessarily equivalent to ϕ for $\lambda \in \mathrm{Aut}(E)$. [18, Exercise 25.1.1].

Kohel [23, Chapter 2.4] gave formulae for the Vélu isogeny in terms of the coefficients of the polynomial defining the kernel, rather than in terms of the points in the kernel.

Let E be an elliptic curve over a field K given by

$$E : y^2 = x^3 + Ax + B.$$

Assume that the degree of the isogeny determined by the equation $\psi(x)$ for the kenel is odd. A general isogeny over K can be docomposed 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.

$$(x, y) \mapsto (X, Y) = \left(\frac{\phi(x)}{\psi(x)^2}, \frac{\omega(x, y)}{\psi(x)^3} \right),$$

where $\phi(x)$ is given by

$$\begin{aligned} \phi(x) = {} & 4(x^3 + Ax + B)(\psi'(x)^2 - \psi''(x)\psi(x)) \\ & - 2(3x^2 + A)\psi'(x)\psi(x) + (dx - 2s_1)\psi(x)^2, \end{aligned}$$

where the degree of the isogeny is $d = 2n + 1$, and s_i is the ith 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 $\mathrm{char}(K) \neq 2$, then $\omega(x, y)$ can be defined as follows.

$$\omega(x, y) = y(\phi'(x)\psi(x) - 2\phi(x)\psi'(x)).$$

The functions x_G and y_G then satisfy the following equation of Velu.

$$Y^2 = X^3 + (A - 5t)X + (B - 7w) \tag{3.1}$$

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

$$t = 6(s_1^2 - 2s_2) + 2nA,$$
$$w = 10(s_1^3 - 3s_1s_2 + 3s_3) + 6As_1 + 4nB.$$

Now suppose that the subgroup G defined by $\psi(x)$ has elements of order 2. We will first determine the isogeny corresponding to the subgroup H of degree 2 or degree 4 defined by $\psi_H(x) = \gcd(\psi(x), 4(x^3 + Ax + B))$. 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

$$x_H = x + \frac{3x_0^2 + A}{x - x_0}$$
$$y_H = y - \frac{(3x_0^2 + A)y}{(x - x_0)^2}$$

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

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

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

$$\omega(x, y) = y(\phi'(x)\psi(x) - \phi(x)\psi'(x)).$$

Since $\psi_H(x)$ determines a separable isogeny, the characteristic is necessarily different form 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 (3.1), with the following values of t and w. If $\psi_H(x) = x - x_0$, then $t = 3x_0^2 + A$, and $w = x_0t$. Otherwise set

$$t = 3(s_1^2 - 2s_2) + 3A,$$
$$w = 3(s_1^3 - 3s_1s_2 + 3s_3) + As_1.$$

3.3 Complex multiplication

Recall that the endomorphism ring of an elliptic curve defined over a field of characteristic 0 is either $\mathbb{Z}$ or imaginary quadratic order by Corollary 3.1.29. Accordingly, we have the following definition.

Definition 3.3.1. Let E be an elliptic curve over a field of characteristic 0. If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, in which case $\mathrm{End}(E) \simeq \mathcal{O}$ for some imaginary quadratic order $\mathcal{O}$, then we say that E has **complex multiplication (CM) by** $\mathcal{O}$.

Definition 3.3.2. An **abelian extension** of a field is an Galois extension with the abelian Galois group.

Definition 3.3.3. Given a number field K, there exists a unique maximal unramified Abelian extension of K, which contains all other unramified Abelian extensions of K [12, Theorem 5.18]. This finite extension, denoted H_K, is called the **Hilbert class field** of K.

Let K be an imaginary quadratic field with the ring of integers $\mathcal{O}_K$. For an order $\mathcal{O}$ in K, let

$$\mathrm{Ell}(\mathcal{O}) := \{j(E) : E/\mathbb{C} \text{ with } \mathrm{End}(E) \simeq \mathcal{O}\}$$

be the set of j-invariants of elliptic curves $E/\mathbb{C}$ with CM by $\mathcal{O}$. If $E/\mathbb{C}$ has CM by $\mathcal{O}$, then its j-invariant generates abelian extensions of K as follows.

Corollary 3.3.4. Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then there is a one-to-one correspondence between the ideal class group $\mathrm{Cl}(\mathcal{O})$ and the $\mathrm{Ell}(\mathcal{O})$.

Proof. See [12, Corollary 10.20]. □

Theorem 3.3.5. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$, and let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) \simeq \mathcal{O}_K$. Then $j(E)$ is an algebraic integer and $K(j(E))$ is the Hilbert class field H_K of K.

Proof. See [12, Theorem 11.1]. □

Definition 3.3.6. Suppose $j \in \mathrm{Ell}(\mathcal{O})$. The **class polynomial**, denoted $H_{\mathcal{O}}$, is the minimal polynomial of j over $\mathbb{Q}$. If $\mathcal{O} = \mathcal{O}_K$ is a maximal order, then it's called the **Hilbert class polynomial**.

Proposition 3.3.7. Suppose $\mathcal{O}$ is an imaginary quadratic order with discriminant $D = \mathrm{disc}(\mathcal{O})$. Then

$$H_D(x) := H_{\mathcal{O}}(x) = \prod_{j \in \mathrm{Ell}(\mathcal{O})} (x - j) \in \mathbb{Z}[x].$$

Proof. See [12, Proposition 13.2]. □

The fact that $H_D \in \mathbb{Z}[x]$ implies that the j-invariant of any elliptic curve $E/\mathbb{C}$ with complex multiplication must be an algebraic integer, meaning that E can actually be defined over a number field. It implies that of the uncountably many isomorphism classes of elliptic curves over $\mathbb{C}$, only countably many have complex multiplication.

We now recall the notion of reduction of an elliptic curve [30, VII.2].

Definition 3.3.8. Let E be an elliptic curve defined over K. A Weierstrass equation $y^2 = x^3 + Ax + B$ for E is called **minimal with respect to** a discrete valuation of K if $\nu(A), \nu(B) \geq 0$ and $\nu(\Delta)$ is minimal subject to that condition.

For each discrete valuation of K, there exists a minimal equation for E. This equation is unique up to isomorphism of curves over K.

For a discrete valuation ν of K, let R be the valuation ring, $\mathfrak{p}$ be the unique maximal ideal of R, $k = R/\mathfrak{p}$ be the residue class field, $\pi \in \mathfrak{p}$ be a prime so that $\nu(\pi) = 1$. Let Γ be a minimal equation for E/K with respect to ν. Reducing the coefficients A and B of Γ modulo $\mathfrak{p} = \pi R$, one obtains an equation $\tilde{\Gamma}$ for a plane cubic curve $\tilde{E}$ defined over k, which is unique up to isomorphism of curves over k. If $\tilde{\Gamma}$ is non-singular (over k^{al}) then $\tilde{E}$ is an elliptic curve over k and $\tilde{\Gamma}$ is a Weierstrass equation for Γ over k. In that case, the discriminant $\tilde{\Delta} := \Delta \mod \mathfrak{p}$, or equivalently $\nu(\Delta) = 0$, and we say that E **has good (or non-degenerate) reduction at** ν. In case $\tilde{\Delta} = 0$, i.e. $\nu(\Delta) > 0$, then $\tilde{E}$ is a rational curve and we say that E **has bad (or degenerate) reduction at** ν.

The following theorems due to Deuring will be useful to construct supersingular j-invariants.

Theorem 3.3.9. Let p be a prime number. Let E be an elliptic curve over a number field L, with $\mathrm{End}(E) \simeq \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let $\mathfrak{p} \mid p$ be a prime of L where E has good reduction (non-degenerate). Then $E \mod \mathfrak{p}$ is supersingular if and only if p does not split in K (either p ramifies or p remains prime in K).

Proof. See [25, Theorem 13.12]. □

Remark 3.3.10. For an imaginary quadratic order $\mathcal{O}$, a general procedure to find an elliptic curve E with $\mathrm{End}(E) \simeq \mathcal{O}$ and the base number field L in Theorem 3.3.9 would be to compute the class polynomial $H_{\mathcal{O}}(x)$. The root j of $H_{\mathcal{O}}(x)$ is the j-invariant in $\mathrm{Ell}(\mathcal{O})$ by Proposition 3.3.7, and $\mathbb{Q}(j)$ is the minimal field of definition for $E(j)$ [30, Proposition 4.5]. Hence, we can take $E = E(j)$ and $L = \mathbb{Q}(j)$.

Theorem 3.3.11. (Deuring Lifting Theorem) Let E_0 be an elliptic curve over a finite field of characteristic p, with a nontrivial endomorphism ϕ_0. Then there exists an elliptic curve E defined over a number field, an endomorphism ϕ of E, and a non-degenerate reduction of E at a place $\mathfrak{p}$ lying above p, such that E_0 is isomorphic to $E \mod \mathfrak{p}$, and ϕ_0 corresponds to $\phi \mod \mathfrak{p}$ under isomorphism.

Proof. See [25, Theorem 13.14]. □

Chapter 4

Deuring's Correspondence

4.1 Overview

Theorem 4.1.1. Let E/K be an elliptic curve with $\operatorname{rank}_{\mathbb{Z}} \operatorname{End}(E) = 4$. Then $B = \operatorname{End} E \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ ramified at $p = \operatorname{char} K$ and ∞, and $\operatorname{End}(E)$ is a maximal order in B.

Proof. We follow the proof in [33, Theorem 42.1.9]. Let $\mathcal{O} = \operatorname{End} E \subseteq B$. For any $n > 0$ coprime to p,

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

is a (simple) $\mathbb{Z}$-module by Corollary 3.1.25. Then the endomorphism ring of $E[n]$ is

$$\operatorname{End}_{\mathbb{Z}} E[n] \simeq \mathrm{M}_2(\operatorname{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})) \simeq \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z}) \tag{4.1}$$

since $\mathrm{M}_n(\operatorname{End}(A)) = \operatorname{End}(A^n)$ for any abelian group A and the endomorphism ring of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to itself as an abelian group.

Next, we show that the structure map $\mathcal{O}/n\mathcal{O} \to \operatorname{End} E[n]$ is an isomorphism. The structure map is injective since if $\phi \in \mathcal{O}$ annihilates $E[n] = \ker[n]$, then the isogeny will factor as the composition $[n] \circ \psi$ of the separable isogeny $[n]$ and some isogeny $\psi \in \mathcal{O}$ by Corollary 3.1.23 so $\phi = 0 \in \mathcal{O}/n\mathcal{O}$. But further, since $\#\mathcal{O}/n\mathcal{O} = \#\operatorname{End} E[n] = n^4$, the structure map is an isomorphism.

Since $\mathcal{O}$ is a free $\mathbb{Z}$-module by Corollary 3.1.27, we have

$$\mathcal{O}_\ell := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} \simeq \varprojlim_n \mathcal{O}/\ell^n\mathcal{O}.$$

The structure isomorphisms in the previous paragraph are compatible with respect to powers of ℓ, so with the isomorphism in (4.1) they provide an isomorphism

$$\mathcal{O}_\ell \xrightarrow{\sim} \varprojlim_n \operatorname{End}_{\mathbb{Z}/n\mathbb{Z}} E[\ell^n] = \operatorname{End}_{\mathbb{Z}_\ell} E[\ell^\infty] \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$$

of $\mathbb{Z}_\ell$-algebras, which is maximal in $\mathrm{M}_2(\mathbb{Q}_\ell)$ and $B_\ell \simeq \mathrm{M}_2(\mathbb{Q}_\ell)$. Hence B is split at all prime $\ell \neq p$.

Since $\mathrm{End}(E)$ is of rank 4 as a $\mathbb{Z}$-module, B is definite by (3.1.30). It follows that $\mathrm{Ram}(B) = \{p, \infty\}$ by Theorem 2.2.25, so B_p is a division algebra over $\mathbb{Q}_p$.

For an isogeny $\phi \in \mathcal{O}$, $\deg_i \phi$ is a power of p and it is divisible by $q = p^r$ if and only if ϕ factors via the qth power Frobenius map $\pi : E \to E^{(q)}$ by Corollary 3.1.19. The map

$$\begin{aligned} \nu : \mathrm{End}\, E \otimes \mathbb{Q} &\to \mathbb{Q} \cup \{\infty\} \\ \nu(a\phi) &= \mathrm{ord}_p(a) + \frac{1}{2}\,\mathrm{ord}_p(\deg_i \phi) \end{aligned}$$

for $a \in \mathbb{Q}$ and $\phi \in \mathrm{End}(E)$ is well-defined since $\deg_i[p] = \deg[p] = p^2$ (by Theorem 3.1.31, $[p]$ is purely inseparable since E is supersingular). Recall that the dual defines a standard involution on $\mathrm{End}(E)$ (3.1.14). Factoring an isogeny into its separable and inseparable parts shows that

$$\mathrm{ord}_p(\deg_i \phi) = \mathrm{ord}_p(\deg \phi) = \mathrm{ord}_p(\mathrm{nrd}\, \phi)$$

so ν is precisely the valuation (2.3) on $B = \mathrm{End}\, E \otimes \mathbb{Q}$ extending the p-adic valuation on $\mathbb{Q}$.

To conclude, we show that $\mathcal{O}_{(p)}$ is the valuation ring (2.4) of B and is therefore maximal by Proposition 2.2.8. If $\alpha \in \mathcal{O}_{(p)} = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, then $\deg \alpha \in \mathbb{Z}_{(p)}$ so α is in the valuation ring. Conversely, let $\alpha \in B$ be a rational isogeny with $\nu(\alpha) \geq 0$, and $\alpha = a\phi$ where ϕ is an (actual) isogeny not divisible by any integer. Then $\nu(\alpha) = \mathrm{ord}_p(a) + \nu(\phi) \geq 0$ and $0 \leq \nu(\phi) \leq 1/2$, since the multiplication-by-p map is purely inseparable; so $\mathrm{ord}_p(a) \geq -\frac{1}{2}$ and therefore $a \in \mathbb{Z}_{(p)}$, and hence $\alpha \in \mathcal{O}_{(p)}$.

Finally, since an order is maximal if and only if it is locally maximal by Lemma 2.3.9, $\mathcal{O}$ itself is a maximal order in the quaternion algebra B.

□

So far we saw the $\mathbb{Z}$-module structure of $\mathrm{End}(E)$. More generally, we have shown that $\mathrm{Hom}(E_1, E_2)$ is a $\mathbb{Z}$-module of rank at most 4. Now we will discuss what we can say more about $\mathrm{Hom}(E_1, E_2)$ when E_1, E_2 are supersingular.

Lemma 4.1.2. Let E, E' be supersingular elliptic curves over $\mathbb{F}_p^{\mathrm{al}}$. Then $\mathrm{Hom}(E, E')$ is a $\mathbb{Z}$-module of rank 4 that is invertible as a right $\mathrm{End}(E)$-module under precomposition and a left $\mathrm{End}(E')$-module under postcomposition. In particular, there exists a separable isogeny from E to E'.

Proof. We follow the proof in [33, Lemma 42.1.11].

We may suppose E is defined over $\mathbb{F}_q$ for some $q = p^r$ such that all of its endomorphisms defined over $\mathbb{F}_q$. Let $\mathcal{O} := \mathrm{End}(E)$ so that $B := \mathcal{O} \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ and let $\pi \in \mathcal{O}$ be the qth power Frobenius map. Since each $\alpha \in \mathcal{O}$ is defined over $\mathbb{F}_q$, for any $P \in E$

$$\pi \circ \alpha(P) = \alpha \circ \pi(P).$$

Hence π commutes with every isogeny in $\mathcal{O}$, and so π lies in the center of $\mathcal{O}$. Since $Z(B) = \mathbb{Q}$, we have $\pi \in Z(\mathcal{O}) = \mathbb{Z}$ by Lemma 2.3.5. For each prime $\ell \neq p$, we have an isomorphism

$$\mathrm{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}_q}(T_\ell(E), T_\ell(E'))$$

by Theorem 3.1.39, where $\mathrm{Hom}_{\mathbb{F}_q}(T_\ell(E), T_\ell(E'))$ is the group of $\mathbb{Z}_\ell$-linear maps that commute with the action of qth-power Frobenius Galois automorphism. We showed that this Frobenius action is in $\mathbb{Z}$ so commuting is automatic, and

$$\mathrm{Hom}_{\mathbb{F}_q}(T_\ell(E), T_\ell(E')) = \mathrm{Hom}(\mathbb{Z}_\ell^2, \mathbb{Z}_\ell^2) \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$$

by Proposition 3.1.36, and $\mathrm{Hom}_{\mathbb{F}_q}(E, E') = \mathrm{Hom}(E, E')$ has rank 4 as a $\mathbb{Z}$-module. Finally, we can precompose by endomorphisms of E so $\mathrm{Hom}(E, E')$ is a torsion free $\mathbb{Z}$-module (by Proposition 3.1.9) with a right action by $\mathcal{O}$. Let $\psi \in \mathrm{Hom}(E, E')$ be nonzero and let $\hat{\psi}$ be the dual isogeny. Then $I := \hat{\psi}\,\mathrm{Hom}(E, E') \subseteq \mathcal{O}$ is an integral right $\mathcal{O}$-ideal; since $\mathcal{O}$ is maximal order by Theorem 4.1.1, the right $\mathcal{O}$-ideal I is invertible by Theorem 2.5.16, and the same then holds for $\mathrm{Hom}(E, E')$ as a right $\mathcal{O}$-module. The same is true as a left $\mathrm{End}(E')$-module, and these two actions commute. □

We now investigate the quaternionic endomorphism rings of supersingular elliptic curves in more detail. Let E be a supersingular elliptic curve over $F := \mathbb{F}_p^{\mathrm{al}}$, let $\mathcal{O} = \mathrm{End}(E)$, and let $B = \mathcal{O} \otimes \mathbb{Q}$. By Theorem 4.1.1, we have $B = B_{p,\infty}$, and $\mathcal{O} \subset B$ is a maximal order. Thus, $\mathrm{disc}\, B = p = \mathrm{discrd}\, \mathcal{O}$.

Let $I \subseteq \mathcal{O}$ be a nonzero integral left $\mathcal{O}$-ideal. Since $\mathcal{O}$ is maximal, I is locally principal (in particular, invertible) by Proposition 2.4.20.

We define $E[I] \subseteq E$ to be the scheme-theoretic intersection

$$E[I] := \bigcap_{\alpha \in I} E[\alpha]$$

where $E[\alpha] = \ker \alpha$ as a group scheme over F. [1] Accordingly, there exists an isogeny $\phi_I : E \to E_I$ where $E_I = E/E[I]$. The scheme language is useful to carry out the required proofs without considering the separable and purely inseparable cases separately as $E[n]$ always has rank n^2 as a group scheme regardless of the characteristic of the base field.

The image of $\mathrm{Hom}(E_I, E)$ under composition by ϕ_I lands in $\mathrm{End}(E) = \mathcal{O}$ and factors through ϕ_I, so in fact lands in I, as $\phi \in \mathrm{End}(E)$ lies in I if and only if $E[I] \subseteq \ker \phi$ by [33, Proposition 42.2.16(b)].

[1] The scheme-theoretic intersection of two closed immersions is given by the fiber product of the two closed immersions.

Lemma 4.1.3. The pullback map

$$\begin{aligned}\phi_I^* : \mathrm{Hom}(E_I, E) &\to I \\ \psi &\mapsto \psi\phi_I\end{aligned}$$

is an isomorphism of left $\mathcal{O}$-modules.

Proof. See [33, Lemma 42.2.7] □

Corollary 4.1.4. For every isogeny $\phi : E \to E'$, there exists a left $\mathcal{O}$-ideal I and an isomorphism $\rho : E_I \to E'$ such that $\phi = \rho\phi_I$. Moreover, for every maximal order $\mathcal{O}' \subset B$, there exists E'' such that $\mathcal{O}' \simeq \mathrm{End}(E'')$.

Proof. See [33, Corollary 42.2.21]. □

Lemma 4.1.5. Let $I, I' \subseteq \mathcal{O}$ be nonzero integral left $\mathcal{O}$-ideals. Then the natural map

$$\mathrm{Hom}(E_I, E)\,\mathrm{Hom}(E_{I'}, E_I) \to \mathrm{Hom}(E_{I'}, E)$$

is bijective, giving a further bijection

$$\begin{aligned}\mathrm{Hom}(E_{I'}, E_I) &\to I^{-1}I' \\ \psi &\mapsto \phi_I^{-1}\psi\phi_{I'}.\end{aligned}$$

Proof. See [33, Lemma 42.2.22]. □

Theorem 4.1.6. Let E_0 be a supersingular elliptic curve over $F := \mathbb{F}_p^{\mathrm{al}}$. Let $\mathcal{O}_0 := \mathrm{End}(E_0)$ and $B_0 := \mathcal{O}_0 \otimes \mathbb{Q}$. The association $E \mapsto \mathrm{Hom}(E, E_0)$ is functorial and defines an equivalence between the category of

$$\{\text{supersingular elliptic curves over } F, \text{ under isogenies}\}$$

and

$$\{\text{invertible left } \mathcal{O}_0\text{-modules, under nonzero left } \mathcal{O}_0\text{-module homomorphisms}\}.$$

Proof. We follow the proof in [33, Theorem 42.3.2].

First we show that $\mathrm{Hom}(-, E_0)$ is a (contravariant) functor. $\mathcal{F} := \mathrm{Hom}(E, E_0)$ is an invertible left $\mathrm{End}(E_0)$-module under postcomposition by Lemma 4.1.2, so the functor $\mathcal{F}$ maps objects from the first category to the second category. Furthermore, if we have an isogeny $\phi : E \to E'$ between two supersingular elliptic curves, $\mathcal{F}$ associates ϕ to its pullback map

$$\begin{aligned}\phi^* : \mathrm{Hom}(E', E_0) &\to \mathrm{Hom}(E, E_0) \\ \psi &\mapsto \psi\phi.\end{aligned}$$

with the properties

$$\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$$

and

$$\mathcal{F}([1]) = \mathrm{id}_{\mathcal{F}(E)},$$

where $f : E \to E'$, $g : E' \to E''$ are isogenies between supersingular elliptic curves, $[1]$ is the identity in $\mathrm{End}(E)$, and $\mathrm{id}_{\mathcal{F}(E)} : \mathrm{Hom}(E, E_0) \to \mathrm{Hom}(E, E_0), \psi \mapsto \psi[1]$ is the identity. The map ϕ^* is a homomorphism of left $\mathcal{O}_0$-modules since it is compatible with postcomposition with $\mathcal{O}_0 = \mathrm{End}(E_0)$. Hence $\mathcal{F} = \mathrm{Hom}(-, E_0)$ is functorial and it is contravariant.

Next, we claim that $\mathrm{Hom}(-, E_0)$ is surjective. Let I be an invertible left $\mathcal{O}_0$-module. Tensoring with $\mathbb{Q}$ we get an embedding $I \hookrightarrow I \otimes \mathbb{Q} \simeq B_0$, so up to isomorphism of left $\mathcal{O}_0$-modues, we may suppose $I \subseteq B_0$. Scaling by an integer, we may suppose $I \subseteq \mathcal{O}_0$ is a left $\mathcal{O}_0$-ideal. By Lemma 4.1.3, we have $\mathrm{Hom}(E_I, E_0) \simeq I$ as left $\mathcal{O}_0$-modules, where $E_I = E/E[I]$.

Finally, we show that $\mathrm{Hom}(-, E_0)$ is fully faithful, i.e., the map

$$\begin{aligned} \mathrm{Hom}(E, E') &\to \mathrm{Hom}(\mathrm{Hom}(E', E_0), \mathrm{Hom}(E, E_0)) \\ \phi &\mapsto \phi^* \end{aligned}$$

is bijective. By Corollary 4.1.4, there exists a left $\mathcal{O}_0$-ideal I such that $E \simeq E_{0,I}$. Applying this isomorphism, we map suppose without loss of generality that $E = E_{0,I}$. Then by Lemma 4.1.3, we have $I = \mathrm{Hom}(E_{0,I}, E_0)\phi_{0,I}$. Repeat with E' and I'. After these identifications, we are reduced to the setting of Lemma 4.1.5 with the location of the prime swapped. The map

$$\begin{aligned} \mathrm{Hom}(E_{0,I}, E_{0,I'}) &\to I'^{-1} I \\ \psi &\mapsto \phi_{0,I}^{-1} \psi \phi_{0,I} \end{aligned}$$

is bijective. □

Note that we can similarly show that $\mathrm{Hom}(E_0, -)$ is a covariant functor to right $\mathcal{O}_0$-modules.

Corollary 4.1.7. There is a bijection between isomorphism classes of supersingular elliptic curves over $F = \mathbb{F}_p^{\mathrm{al}}$ and left class set $\mathrm{Cl}_L \mathcal{O}_0$. Under this bijection, if $E \leftrightarrow [I]$, then $\mathrm{End}(E) \simeq \mathcal{O}_R(I)$ and $\mathrm{Aut}(E) \simeq \mathcal{O}_R(I)^\times$. [33, Corollary 42.3.7]

Proof. Note that in the equivalence of categories in Theorem 4.1.6, every isomorphism class of (invertible) left $\mathcal{O}_0$-modules was represented by a left $\mathcal{O}_0$-ideal. Hence we can take isomorphism classes on both sides of the equivalence in Theorem 4.1.6 and compare endomorphism rings and automorphism groups. □

Lemma 4.1.8. Let $\mathcal{O} \subseteq B_{p,\infty}$ be a maximal order. Then there exist one or two supersingular elliptic curves E up to isomorphism over $F = \mathbb{F}_p^{\mathrm{al}}$ such that $\mathrm{End}(E) \simeq \mathcal{O}$. There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Proof. We follow the proof in [33, Lemma 42.4.1]. By Corollary 4.1.4, there is always at least one supersingular elliptic curve E with $\mathrm{End}(E) \simeq \mathcal{O}$ using a connecting ideal.

By Corollary 4.1.7, the isomorphism classes of supersingular elliptic curves are in bijection with the left class set $\mathrm{Cl}_L \mathcal{O}_0$, where $\mathcal{O}_0$ was the endomorphism ring of a supersingular elliptic curve E_0 over $F = \mathbb{F}_p^{\mathrm{al}}$. Their endomorphism rings are then given by $\mathrm{End}(E) \simeq \mathcal{O}_R(I)$ for $[I] \in \mathrm{Cl}_L \mathcal{O}_0$. By Lemma 2.5.13 (interchanging left for right), the map

$$\begin{aligned} \mathrm{Cl}_L \mathcal{O}_0 &\to \mathrm{Typ}\, \mathcal{O}_0 \\ [I]_L &\mapsto \text{ class of } \mathcal{O}_R(I) \end{aligned}$$

is a surjective map of sets. The connecting ideals are precisely the fibers of this map, and by the bijection of Corollary 4.1.7, there is a bijection between the set of supersingular elliptic curves E with $\mathrm{End}(E) \simeq \mathcal{O}$ and the fiber of this map over the isomorphism class of $\mathcal{O}$.

We now count these fibers. We recall Proposition 2.5.24 with $D = p$ and Proposition 2.5.19: the fibers are given by the quotient group $\mathrm{PIdl}\, \mathcal{O} \setminus \mathrm{Idl}\, \mathcal{O}$ of the invertible fractional two-sided $\mathcal{O}$-ideals by the subgroup of principal such ideals. There is a surjection $\mathrm{Pic}(\mathcal{O}) \to \mathrm{PIdl}\, \mathcal{O} \setminus \mathrm{Idl}\, \mathcal{O}$ and $\mathrm{Pic}(\mathcal{O}) \simeq \mathbb{Z}/2\mathbb{Z}$ is generated by the unique maximal two-sided ideal P of reduced norm P. The class of P in the quotient is trivial if and only if $P = \mathcal{O}\pi$ is principal.

To conclude recall [33, 42.2.4]: the Frobenius map is the map $E \to E_P \simeq E^{(p)}$. So P is principal if and only if $E^{(p)} \simeq E$ if and only if $j(E) = j(E^{(p)}) = j(E)^p$ if and only if $j(E) \in \mathbb{F}_p$. □

Theorem 4.1.1 and Lemma 4.1.8 prove the following classic result due to Deuring.

Theorem 4.1.9. (Deuring's Correspondence)
For each prime p, there is a bijection from the set of supersingular elliptic curves up to Galois conjugacy to maximal orders in $B_{p,\infty}$ up to isomorphism.

$$\{\text{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\} / \simeq \longleftrightarrow \left\{\text{supersingular } j \in \mathbb{F}_{p^2}\right\} / \mathrm{Gal}\,(\mathbb{F}_{p^2}/\mathbb{F}_p)$$

that sends $\mathrm{End}(E) \simeq \mathcal{O}$ to $j(E)$.

Remark 4.1.10. Here we neglect to write the base field of supersingular elliptic curves since every supersingular elliptic curve has j-invariant in $\mathbb{F}_{p^2}$, so it has a Weierstrass model defined over $\mathbb{F}_{p^2}$. The supersingular j-invariant in $\mathbb{F}_{p^2}$ is unique up to Galois conjugation. The maximal order is unique up to conjugation by Remark 2.5.6. By choosing a Hermite basis of the maximal order, which are four vectors forming $\mathbb{Z}$-basis, we get a unique representation in the quaterinon side of this correspondence.

Let E be an elliptic curve with $\mathrm{End}(E) \simeq \mathcal{O}$. There is a one-to-one correspondence between isogenies $\phi : E \to E'$ and left $\mathcal{O}$-ideals I, where I is a connecting ideal of $\mathcal{O}$ and $\mathcal{O}' \simeq \mathrm{End}(E')$ (I is a left $\mathcal{O}$-ideal and a right $\mathcal{O}'$-ideal), and $\deg \phi = \mathrm{nrd}(I)$. This follows from Theorem 4.1.6 since under the association $E' \mapsto \mathrm{Hom}(E', E)$, each isogeny $\phi : E \to E'$ corresponds to the pullback $\phi^* : \mathrm{Hom}(E', E) \xrightarrow{\sim} I := \mathrm{Hom}(E', E)\phi \subseteq \mathcal{O}$ given in Lemma 4.1.3.

4.2 Constructive algorithms

In this section, we discuss Bröker's algorithm in [7] to construct a supersingular elliptic curve over a given prime field.

Lemma 4.2.1. Let K be an imaginary quadratic field with class number h_k. Then h_k is odd if and only if

(i) $K = \mathbb{Q}(\sqrt{-1})$, or

(ii) $K = \mathbb{Q}(\sqrt{2})$, or

(iii) $K = \mathbb{Q}(\sqrt{-q})$ with q prime and congruent to 3 mod 4.

Proof. We follow the proof in [7, Lemma 2.3].

Let D be the discriminant of K, and let $p_1, \cdots, p_n$ be the odd prime factors of D. The genus field

$$G = K(\sqrt{p_1^*}, \cdots, \sqrt{p_n^*})$$

with $p_i^* = (-1)^{(p_i-1)/2} p_i$ is the maximal unramified abelian extension of K that is abelian over $\mathbb{Q}$ [12, Theorem 6.1], and Galois group $\mathrm{Gal}(G/K)$ is isomorphic to the 2-Sylow group of $\mathrm{Cl}(\mathcal{O}_K)$. We see that h_k is odd if and only if we have an equality $G = K$. This yields the lemma. □

Proposition 4.2.2. Given a prime p, Algorithm 1 computes a supersingular j-invariant in $\mathbb{F}_p$.

Proof. We follow the proof in [7].

Let K be an imaginary quadratic field. Recall that the Hilbert class field of K is $H_K = K[x]/(P_K)$ by Theorem 3.3.5, where P_K is the Hilbert class polynomial of K. Since K is a number field of degree $[K : \mathbb{Q}] = 2$, there are only three possible factorization of prime p in $\mathcal{O}_K$;

(a) $(p) = \mathfrak{p}^2 : (p)$ ramifies, or

(b) $(p) = \mathfrak{p} : (p)$ is inert, or

(c) $(p) = \mathfrak{p}_1\mathfrak{p}_2 : (p)$ splits.

Hence, if we take K such that p is inert in $\mathcal{O}_K$, then the roots of $P_K \in \overline{\mathbb{F}}_p[x]$ are supersingular j-invariants by Theorem 3.3.9 and the discussion in Remark 3.3.10. Since the j-invariant of a supersingular curve is contained in $\mathbb{F}_{p^2}$, the polynomial P_K splits over $\mathbb{F}_{p^2}$.

Next, we show that $P_K \in \mathbb{F}_p[x]$ has a root in $\mathbb{F}_p$ if h_K is odd. Write

$$P_K(x) = \prod_{j \in \mathrm{Ell}(\mathcal{O}_K)} f_j(x)^{e_j} \in \mathbb{F}_p[x],$$

and let S be the splitting field of P_K. Every finite extension of $\mathbb{F}_p$ is Galois, so we have

$$[S : \mathbb{F}_p] = \mathrm{lcm}(\deg(f_j)).$$

Note that $S \subseteq \mathbb{F}_{p^2}$ since P_K splits over $\mathbb{F}_{p^2}$. This implies that $\deg(f_j) \leq 2$ for all j. If $\deg(P_K)$ is odd, then not all $\deg(f_j)$ is even, i.e. some $\deg(f_i) = 1$ and P_K has a root in $\mathbb{P}_K$.

Hence, Lemma 4.2.1 gives a sufficient condition for $P_K \in \mathbb{F}_p[x]$ to have a root in $\mathbb{F}_p$.

If the quadratic field K has class number $h_k = 1$, then there exists a curve $E/\mathbb{Q}$ with $\mathrm{End}(E) \simeq \mathcal{O}_K$ (Primes inert in quadratic field of class number one). In particular, for $K = \mathbb{Q}(i)$, the reduction of $E : y^2 = x^3 - x$ modulo prime $p \equiv 3 \pmod 4$ yields a supersingular curve modulo p and similarly, $E' : y^2 = x^3 + 1$ is supersingular for all primes $p \equiv 2 \pmod 3$. □

Algorithm 1: Bröker's algorithm to compute a supersingular j-invariant

input : A prime p.
output: A supersingular curve over $\mathbb{F}_p$.
1. If $p = 2$, return $y^2 + y = x^3$.
2. If $p \equiv 3 \bmod 4$, return $y^2 = x^3 - x$.
3. Let q be the smallest prime congruent to 3 mod 4 with $\left(\frac{-q}{p}\right) = -1$.
4. Compute $P_K \in \mathbb{Z}[x]$ for $K = \mathbb{Q}(\sqrt{-q})$.
5. Compute a root $j \in \mathbb{F}_p$ of $P_K \in \mathbb{F}_p[x]$.
6. If $q = 3$, return $y^2 = x^3 + 1$. Else, put $a \leftarrow 27j/(4(1728 - j)) \in \mathbb{F}_p$ and return $y^2 = x^3 + ax - a$.

Remark 4.2.3. Under GRH, the expected running time of Algorithm 1 is $\tilde{O}((\log p)^3)$ [7, Lemma 2.5].

Let $\pi : (x, y) \to (x^p, y^p)$ be the pth power Frobenius map.

Proposition 4.2.4. Given a prime p, Algorithm 2 computes a supersingular j-invariant $j_0 \in \mathbb{F}_p$ such that $\mathrm{End}(E(j_0)) \simeq \mathcal{O}_0$, where $\mathcal{O}_0$ is as given by Proposition 2.6.2, together with a map $\phi \in \mathrm{End}(E(j_0)))$ such that $\theta : B_{p,\infty} \to \mathrm{End}(E(j_0)) \otimes \mathbb{Q} : (1, i, j, k) \to (1, \phi, \pi, \pi\phi)$ is an isomorphism of quaternion algebras.

Proof. We follow the proof in [17, Proposition 3].

The case $p = 2$ is trivial. There is only one supersingular j-invariant in $\mathbb{F}_{p^2}$, so $B_{p,\infty}$ has a unique maximal order (up to isomorphism) by Theorem 4.1.9.

The case $p \equiv 3 \pmod 4$ is treated in [17]. We will detail the case $p \equiv 1 \pmod 8$. The case $p \equiv 5 \pmod 8$ is similar.

Let $q \equiv 3 \bmod 4$ and $(p/q) = -1$ be chosen as in Proposition 2.6.2. Let $\mathcal{O}_K$ be the ring of integers of the number field $K = \mathbb{Q}(\sqrt{-q})$. Consider Algorithm 2 below.

Step 1 is a modification of Algorithm 1. We first show that the cardinality of

$$\mathcal{J} = \left\{\text{supersingular } j \in \mathbb{F}_{p^2} : \mathcal{O}_K \subseteq \mathrm{End}(E(j))\right\}$$

is equal to the class number h_K of K, which is bounded by q. Note that $\mathcal{O}_K = \langle 1, \frac{1+j}{2}\rangle \subseteq \mathcal{O}_0$ since $j^2 = -q \equiv 1 \pmod 4$. We will show that for each $j \in \mathcal{J}$, there exists a unique $j' \in \mathrm{Ell}(\mathcal{O}_K)$ such that $E(j) = E(j') \mod \mathfrak{p}$ for a fixed prime $\mathfrak{p}$ of $\mathcal{O}_K$.

Suppose $j \in \mathcal{J}$ is a supersingular j-invariant such that $\mathcal{O}_K \subseteq \mathrm{End}(E(j))$. Then if $\mathcal{O}_K = \mathbb{Z}[\alpha]$, by Theorem 3.3.11 applied to $E(j)$ and α, there is an elliptic curve $\widetilde{E}/\mathbb{C}$ such that $\mathrm{End}(\widetilde{E}) \simeq \mathcal{O}_K$ (since we assumed $O_K \subseteq \mathrm{End}(E(j))$) and a prime $\mathfrak{p}$ of $\mathcal{O}_K$ dividing p such that $\widetilde{E} \mod \mathfrak{p} = E(j)$. Since $\widetilde{E}$ has complex multiplication by $\mathcal{O}_K$, $j(\widetilde{E})$ is a root of the Hilbert class polynomial of K. Since $p \equiv 1 \mod 4$, we have $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right) = -1$ by quadratic reciprocity. This implies p is inert in $\mathcal{O}_K$, i.e., $\mathfrak{p} = p\mathcal{O}_K$ is the unique prime ideal of $\mathcal{O}_K$ lying over p. Hence $\#\mathcal{J} \leq \#\,\mathrm{Ell}(\mathcal{O}_K) = h_k$.

Conversely, an elliptic curve $E/\mathbb{C}$ representing an isomorphism class in $\mathrm{Ell}(\mathcal{O}_K)$ has a reduction modulo $\mathfrak{p}$ whose j-invariant is in $\mathcal{J}$ by Theorem 3.3.9. Principal prime ideals of $\mathcal{O}_K$ split completely in the Hilbert class field of K by [12, Corollary 5.25], so the Hilbert class polynomial will have h_K distinct roots modulo p. Hence, $\#\mathcal{J} \geq h_k$.

To compute ϕ in Step 2 one can compute all isogenies of degree q using Vélu's formulae and identify the one corresponding to an endomorphism. Using map ϕ allows us to construct an isomorphism of quaternion algebras over $\mathbb{Q}$,

$$\begin{aligned}\theta : B_{p,\infty} &\to \mathrm{End}(E(j_0)) \otimes \mathbb{Q}\\ (1, i, j, k) &\mapsto (1, \pi, \phi, \phi\pi).\end{aligned}$$

Let $\alpha = \theta(j) = \pi$. Then $\alpha + \bar{\alpha} = 0$ and $\alpha\bar{\alpha} = p$. Since $\alpha^2 + (\alpha + \bar{\alpha})\alpha + \alpha\bar{\alpha} = \alpha^2 + p = 0$, we deduce that $\alpha^2 = -p$. Similarly, $\beta = \theta(i)$ satisfies $\beta^2 = \phi^2 = -q$. Hence, the linear map θ defines a well defined ring homomorphism.

To perform the check in Step 3, one applies θ to the numerators of the basis elements for $\mathcal{O}_0$, and then check whether the resulting maps annihilate the D-torsion, where D is the denominator of the basis elements for $\mathcal{O}_0$.

As $p \equiv 1 \pmod 8$ then $\frac{1+j}{2}, \frac{i+k}{2}, \frac{j+ck}{q}, k$ is a basis for $\mathcal{O}_0$. Assuming $E[2] \subseteq \ker(\theta(1+j))$ there exists a (unique) map $f : E/E[2] \simeq E \to E$ such that $\theta(1+j) = f \circ [2]$ by Corollary 3.1.23. Write $\frac{1+\phi}{2} := f$ so we have $f \in \mathrm{End}(E(j_0))$.

Similarly, we can define $\frac{\pi+\phi}{2}$ and $\frac{\phi+c\phi\pi}{q}$ so that the images of $1, i, j, k$ under θ are contained in $\mathrm{End}(E(j_0))$. The order generated by these images corresponds to $\mathcal{O}_0$ so it is maximal. Hence, we deduce that $\mathrm{End}(E(j_0)) \simeq \mathcal{O}_0$. □

Algorithm 2: Constructive Deuring correspondence, from special maximal orders to j-invariants.

---

input : A prime p.

output: A supersingular j-invariant $j_0 \in \mathbb{F}_p$ such that $\mathrm{End}(E(j_0)) \simeq \mathcal{O}_0$, and an endomorphism $\phi \in \mathrm{End}(E(j_0))$ such that $\mathrm{nrd}(\phi) = q$ and $\mathrm{trd}(\phi) = 0$.

1. Compute $\mathcal{J} := \left\{\text{supersingular } j \in \mathbb{F}_{p^2} : \mathcal{O}_K \subseteq \mathrm{End}(E(j))\right\}$, where $\mathcal{O}_K$ is the integer ring of $K = \mathbb{Q}(\sqrt{-q})$.
2. For a choice of $j \in \mathcal{J}$, compute all ϕ, an endomorphism of degree q of $E(j)$.
3. Check if $\mathrm{End}(E(j)) \simeq \mathcal{O}_0$ by using the map ϕ to construct an isomorphism of quaternion algebras $\theta : B_{p,\infty} \to \mathrm{End}(E(j)) \otimes \mathbb{Q} : (1, i, j, k) \to (1, \phi, \pi, \pi\phi)$.
4. If step 3 fails, then go back to step 2 for a different choice of $j \in \mathcal{J}$. Return j and ϕ.

Chapter 5

Supersingular Isogeny Graphs

5.1 Overview

The classical modular polynomial $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$ is initially constructed as a relation between the modular functions $j(\tau)$ and $j(n\tau)$ [12] and has the following modular interpretation:

Theorem 5.1.1. Given a $j \in \mathbb{F}_p^{\text{al}}$, the roots of $\Phi_n(j, Y)$ give the j-invariants of elliptic curves over $\mathbb{F}_p^{\text{al}}$ which are n-isogenous over $\mathbb{F}_p^{\text{al}}$ to an elliptic curve with j-invariant j.

Proof. See [25, Theorem 5.5]. □

We now summarize some basic definitions and results from [3] concerning supersingular isogeny graphs.

Definition 5.1.2. Let ℓ be a prime different from the prime p. The **supersingular ℓ-isogeny graph in characteristic** p is the multigraph $G(p, \ell)$ whose vertices are j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and the number of directed edges from j to j' is equal to the multiplicity of j' as a root of $\Phi_\ell(j, Y)$.

Note that vertices in $G(p, \ell)$ are isomorphism classes of elliptic curves. By the discussion in Remark 3.2.4, an edge in $G(p, \ell)$ is represented by a unique (separable) ℓ-isogeny up to isomorphism, i.e., if $\phi : E \to E'$ is an ℓ-isogeny and $\alpha \in \text{Aut}(E')$, then ϕ and $\alpha \circ \phi$ correspond to the same edge in $G(p, \ell)$. By Theorem 3.1.22, the representation size of the isogeny is $\deg \phi = \# \ker \phi$.

From the following statement, we see that any two supersingular elliptic curves over $\mathbb{F}_{p^2}$ are connected by an isogeny of degree ℓ^m, where we can take m to be polynomial size in $\log p$.

Theorem 5.1.3. The graph $G(p, \ell)$ of ℓ-isogenies of supersingular elliptic curve is connected. The diameter of the graph is $O(\log p)$, where the constant in the bound is independent of ℓ.

Proof. See [23, Corollary 78 and Theorem 79]. □

In the next chapter, we will show that any ℓ-isogeny connecting supersingular elliptic curves have representation size polynomial in $\log p$.

Definition 5.1.4. Two edges e and e' in $G(p, \ell)$ are called **dual** if the corresponding ℓ-isogenies $\phi : E \to E'$ and $\phi' : E' \to E$ are equal to the dual of the other up to isomorphism, i.e., $\phi' = \alpha\hat{\phi}$ for some $\alpha \in \mathrm{Aut}(E)$. We say a path $(e_1, \cdots, e_k)$ **has no backtracking** if e_{i+1} is not dual to e_i for $i = 1, \ldots, k-1$.

Definition 5.1.5. By **trimming** a path in $G(p, \ell)$, we mean removing all adjacent dual edges in the path.

Definition 5.1.6. An isogeny $\phi : E \to E'$ is **primitive** if it does not factor through $[n] : E \to E'$ for any $n > 1$.

Remark 5.1.7. Two non-equivalent isogenies $E_1 \to E_2$ can have equivalent duals if $\#\mathrm{Aut}(E_2) > 2$ (see [18, Remark 25.3.2]). If $p \equiv 1 \pmod{12}$, then this phenomenon does not occur and we may uniquely identify pairs of dual edges and consider $G(p, \ell)$ as an undirected graph without any modification [11].

Given a path in $G(p, \ell)$ of length e between j and j', there is an isogeny $\phi : E(j) \to E(j')$ of degree ℓ^e obtained by composing the isogenies corresponding to the edges in the path. If this path has no backtracking, the kernel of ϕ is a cyclic subgroup of order ℓ^e. Conversely, we have the following proposition.

Proposition 5.1.8. Suppose $\phi : E(j) \to E(j')$ is an isogeny with cyclic kernel of order ℓ^e. Then there is a unique path in $G(p, \ell)$ such that the factorization of ϕ into a chain of ℓ-isogenies corresponds to the edges in the path, and the path has no backtracking.

Proof. See [3, Proposition 4.5] □

Corollary 5.1.9. Suppose $\phi \in \mathrm{End}(E)$ is an endomorphism with cyclic kernel of order ℓ^e. Then there is a unique path in $G(p, \ell)$ such that the factorization of ϕ into a chain of ℓ-isogenies corresponds to the edges in a cycle through $j(E)$, and the cycle has no backtracking.

Cycles through E with no backtracking exactly correspond to primitive endomorphisms of E with ℓ-power degree.

Lemma 5.1.10. Let $\{e_1, \ldots, e_e\}$ be a cycle in $G(p, \ell)$ through the vertex $E(j)$ with corresponding endomorphism $\phi \in \mathrm{End}(E(j))$. If the cycle has no backtracking, then the corresponding endormorphism ϕ is primitive. Conversely, if $\phi \in \mathrm{End}(E(j))$ is primitive and $\deg(\phi) = \ell^e$ for $e \in \mathbb{N}$, then the cycle in $G(p, \ell)$ corresponding to ϕ has no backtracking.

Proof. See [3, Lemma 4.6] □

It is a fact that $\Phi_n(X,Y) = \Phi_n(Y,X)$ so that we may collapse any pair of dual edges in $G(p,\ell)$ into a single undirected edge, furthermore, any multiple undirected edge into a single undirected edge, to obtain a modified undirected version of $G(p,\ell)$, which we denote by $\bar{G}(p,\ell)$. By construction, cycles in $\bar{G}(p,\ell)$ do not have backtracking.

Remark 5.1.11. In collapsing edges to obtain $\bar{G}(p,\ell)$, we may fail to detect cycles through E such that $\#\mathrm{Aut}(E) > 2$ if we use the graphs $\bar{G}(p,\ell)$. However, since there are at most two such vertices corresponding to $j(E) = 0, 1728$, so this is a mild loss of information. Another type of cycle which would not be detected are those formed by multiple undirected edges between two different vertices, after collapsing all pairs of dual edges.

The following properties are taken from [3] [9].

Theorem 5.1.12. Let $G = G(p,\ell)$ be the supersingular ℓ-isogeny graph in characteristic p. Then

(i) G is connected

(ii) G is $(\ell+1)$-regular as a directed multi-graph, with the exception of the vertices $j = 0, 1728$

(iii) $\#V(G) = [\frac{p}{12}] + \epsilon_p$, where $V(G)$ is the vertex set of G and

$$\epsilon_p = \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12}, \\ 1 & \text{if } p = 3, \\ 1 & \text{if } p \equiv 5, 7 \pmod{12}, \\ 2 & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

(iv) G is Ramanujan, i.e., they are optimal expander graphs, with the consequence that random walks on the graph quickly reach the uniform distribution (after $O(\log(N))$ steps for an expander graph with N vertices).

For applications of expander graphs, see [20].

The fastest known algorithm for finding an isogeny between two supersingular elliptic curves defined over $\mathbb{F}_q$ of characteristic p runs in $\tilde{O}(p^{1/2})$ time [15].

5.2 M-small elliptic curves

Fix a prime $p \geq 5$. Let k be a finite field of characteristic p and size q.

The proof of Theorem 3.1.28 proceeds by supposing the existence of an element not in the $\mathbb{Q}$-span of the previous case, until no such element can be found. For instance, to separate the case of $\mathrm{End}(E) = \mathbb{Z}$ from the later cases, we need to find a non-integer endomorphism.

Following [27] and motivated by the above, we make the next definition.

Definition 5.2.1. Given $M \in \mathbb{N}$, an elliptic curve E over k is M-small if there exists a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$.

Definition 5.2.2. Given $M \in \mathbb{N}$, an elliptic curve E over k is M-big if there does not exist a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$.

Proposition 5.2.3. The supersingular elliptic curves found by Algorithm 1 are $\frac{q+1}{4}$-small. Assuming GRH, they are M-small for $M = O((\log p)^2)$.

Proof. We follow the proof in [27, Proposition 2.2].

The output of the algorithm is a curve E over $\mathbb{F}_p$ with the following property: there exists a curve $\tilde{E}$ over the Hilbert class field of $K = \mathbb{Q}(\sqrt{-q})$ such that $\mathrm{End}(\tilde{E}) \simeq \mathcal{O}_K$ and E is the reduction of $\tilde{E}$ modulo a prime of $\mathcal{O}_L$ above p. In particular, $\frac{1+\sqrt{-q}}{2} \in \mathcal{O}_K$ is a non-integer endomorphism of $\tilde{E}$ with norm $\frac{q+1}{4}$. The reduction map $\mathrm{End}(\tilde{E}) \to \mathrm{End}(E)$ is a degree-preserving injection [30, Proposition II.4.4], so $\mathrm{End}(E)$ also contains a non-integer endomorphism of norm $\frac{q+1}{4}$, proving that E is $\frac{q+1}{4}$-small. As discussed in the proof of [6, Lemma 2.5], under GRH we can find $q = O((\log p)^2)$ with the desired properties. □

It is shown in [27] that M-small elliptic curves over k can be efficiently enumerated for small M and they are partitioned into pieces which are far apart.

Proposition 5.2.4. Let $3 \leq M < p$, let E be an elliptic curve over a finite field of characteristic p, and let j be the j-invariant of E. Then E is M-small if and only if $H_{\mathcal{O}}(j) = 0 \pmod{p}$ for some quadratic order $\mathcal{O}$ with discriminant $-4M \leq \mathrm{disc}\, \mathcal{O} < 0$. Further, E is supersingular if and only if p does not split in the field of fractions of $\mathcal{O}$.

Proof. See [27, Proposition 2.3]. □

By Deuring's Lifting Theorem, there is an elliptic curve $\tilde{E}$ defined over a number field L, an endomorphism $\tilde{\alpha}$ of $\tilde{E}$, and a prime $\mathfrak{p}$ of L, such that $\tilde{E}$ has good reduction at $\mathfrak{p}$, the reduction of $\tilde{E}$ at $\mathfrak{p}$ is isomorphic over $\mathbb{F}_p^{\mathrm{al}}$ to E, and that the endomorphism on E induced by $\tilde{\alpha}$ is equal to α. For some quadratic order $\mathcal{O}$ in an imaginary quadratic field K, we will have $\mathrm{End}(\tilde{E}) \simeq \mathcal{O}$.

Proposition 5.2.5. Let $\mathcal{O}$ be a quadratic order with discriminant $-4M \leq \mathrm{disc}\, \mathcal{O} < 0$. Let $C_{\mathcal{O}}$ denote the set of isomorphism classes of elliptic curves over k such that $\mathcal{O}$ embeds into $\mathrm{End}(E)$. Then

$$|C_{\mathcal{O}}| \leq \deg H_{\mathcal{O}}(x) = |\mathrm{Cl}(\mathcal{O})| = O(M^{1/2+\epsilon})$$

Proof. See [27, Proposition B.1]. □

Remark 5.2.6. In the above proposition and what follows, we count elliptic curves over k up to isomorphism over the algebraic closure of k.

The following proposition [27, Proposition B.3] implies, for $M \ll p$, the M-small elliptic curves over k are sparse among all supersingular elliptic curves over k.

Proposition 5.2.7. The number of M-small elliptic curves over k is bounded above by

$$\frac{2}{\sqrt{3}}(2M+1)M^{\frac{1}{2}} = O(M^{\frac{3}{2}}). \tag{5.1}$$

Proof. If E is an M-small elliptic curve over k, let $\alpha \in \mathrm{End}(E), \alpha \notin \mathbb{Z}$ have $\mathrm{nrd}(\alpha) \leq M$. Suppose α satisfies the polynomial $x^2 + b_\alpha x + c_\alpha$ where $b_\alpha, c_\alpha \in \mathbb{Z}$. Then $\mathrm{nrd}(\alpha) = c_\alpha$ and α lies in the quadratic order $\mathcal{O}$ of discriminant $\Delta_\alpha = b_\alpha^2 - 4c_\alpha$. We thus have the inequalities

$$|\Delta_\alpha|/4 \leq \mathrm{nrd}(\alpha) \leq M. \tag{5.2}$$

There are at most $h(\mathcal{O}) = |\mathrm{Cl}(\mathcal{O})|$ isomorphism classes of elliptic curves E over k such that $\mathcal{O}$ embeds into $\mathrm{End}(E)$ by Proposition 5.2.5. A quadratic order $\mathcal{O}$ is uniquely determined by its discriminant, and there is a bijection between $\mathrm{Cl}(\mathcal{O})$ and the set of reduced primitive positive-definite binary quadratic forms of discriminant $\mathrm{disc}\,\mathcal{O}$. Thus, it suffices to bound the number of triples $(a,b,c) \in \mathbb{Z}^3$ with $-a < b \leq a \leq c$ and $b \geq 0$ if $a = c$, $\gcd(a,b,c) = 1$, and $-4M \leq \Delta_\alpha = b^2 - 4ac < 0$. From $|b| \leq a \leq c$, we have $-4M \leq b^2 - 4ac \leq -3a^2$, so $a \leq \sqrt{4M/3}$. Likewise $-4M \leq b^2 - 4ac \leq a^2 - 4ac$ implies $a \leq c \leq \frac{a}{4} + \frac{M}{a}$. Together with $-a < b \leq a$ we conclude that there are at most

$$\left(\frac{a}{4} + \frac{M}{a} - a + 1\right)(2a) \leq 2M + 1$$

valid pairs (b,c) for a given a; summing over the $\sqrt{4M/3}$ options for a gives the upper bound. □

Proposition 5.2.8. Every supersingular elliptic curve over k is $\left(\frac{1}{2}p^{2/3} + \frac{1}{4}\right)$-small.

Proof. See [27, Proposition A.5] □

Corollary 5.2.9. The proportion of q^θ-big elliptic curves over k is bounded below by

$$1 - \frac{2}{\sqrt{3}}\frac{(2q^\theta + 1)q^{\frac{\theta}{2}}}{q}.$$

Proof. The total number of elliptic curves over k is q. The number of q^θ-small elliptic curves over k is bounded above by

$$\frac{2}{\sqrt{3}}(2q^\theta + 1)q^{\frac{\theta}{2}}.$$

□

5.3 (M, ℓ)-small and (M, S)-small elliptic curves

We now consider the bounds obtained in the previous section, but restricting the degree of the isogenies allowed.

Definition 5.3.1. Given $M \in \mathbb{N}$ and ℓ a prime, an elliptic curve E over k is (M, ℓ)-small if there exists a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ with $\deg \alpha = \ell^n \leq M$ for some $n \in \mathbb{N}$.

Definition 5.3.2. Given $M \in \mathbb{N}$ and ℓ a prime, an elliptic curve E over k is (M, ℓ)-big if there does not exist a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ with $\deg \alpha = \ell^n \leq M$ for some $n \in \mathbb{N}$.

By Corollary 5.1.9, finding $\phi \in \mathrm{End}(E)$ with cyclic kernel of order ℓ^e corresponds to finding a cycle through $j(E)$ in the ℓ-supersingular isogeny graph $G(p, \ell)$. The property that E is (M, ℓ)-big translates into the fact any cycle through $j(E)$ has length $\geq \log_\ell M$.

If $M = \Omega(p)$ and E is (M, ℓ)-big, then searching for such a cycle through $j(E)$ using breadth first search is expensive. In the next paragraphs, we give upper bounds for the number of (M, ℓ)-small elliptic curves over k. The motivation is to give a lower bound for the number of (M, ℓ)-big elliptic curves over k.

Lemma 5.3.3. For $f \geq 2$, we have the bound

$$\prod_{p|f} \left(1 + \frac{1}{p}\right) \leq 4(1 + \log\log f).$$

Proof. See [24, Lemme 2]. □

For any prime ℓ, the set of (M, ℓ)-big elliptic curves over k contains the set of M-big elliptic curves over k. Proposition 5.2.7 thus also gives an upper bound on the number of (M, ℓ)-small elliptic curves over k. However, we can refine the proof to give a sharper bound below.

Proposition 5.3.4. The number of (M, ℓ)-small elliptic curves over k is bounded above by

$$O\left(M \log M\right). \tag{5.3}$$

Proof. By adding the constraint that $c_\alpha = \ell^n \leq M$ for some n, we see that $n = \log_\ell M = O(\log M)$. For $\Delta_\alpha = b_\alpha^2 - 4c_\alpha$ to be negative, $b_\alpha^2 \leq 4c_\alpha = 4\ell^n$ so $|b_\alpha| \leq 2\ell^{n/2}$. Hence, there are at most

$$\begin{aligned}\sum_{n=0}^{\log_\ell M} 2\ell^{n/2} &= 2\frac{\ell^{\frac{1}{2}}\ell^{\frac{\log_\ell M}{2}} - 1}{\ell^{\frac{1}{2}} - 1} \\ &= O(M^{1/2})\end{aligned}$$

choices for Δ_α.

Let $K = \mathbb{Q}(\Delta^{1/2})$ and $\mathcal{O}_K$ the ring of integers of K of discriminant Δ_K. Then by the class number formula

$$h(\mathcal{O}_K) = \frac{w_K}{2\pi}|\Delta_K|^{1/2}L(1,\chi_K), \tag{5.4}$$

where χ_K is the character associated to the quadratic field K, w_K is the number of units in $\mathcal{O}_K$, and $L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ is a Dirichlet L-function [13, p. 49]. We have from [26, p. 214] that

$$|L(1,\chi_K)| \leq \log|\Delta_K|^{1/2} + 1$$

so that

$$h_K \leq O(|\Delta_K|^{1/2}\log|\Delta_K|^{1/2})$$

Suppose $\mathcal{O}$ has discriminant $\Delta = \Delta_K f^2$ and conductor f. Then

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]}\prod_{p|f}\left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \tag{5.5}$$

by [12, Corollary 7.28], and we can bound

$$\begin{aligned} h(\mathcal{O}) &\leq h(\mathcal{O}_K)f\prod_{p|f}\left(1+\frac{1}{p}\right) \\ &= O(|\Delta_K|^{1/2}f\log|\Delta_K|^{1/2}\log f) \\ &= O(|\Delta|^{1/2}\log|\Delta|^{1/2}). \end{aligned}$$

where the logarithmic terms are simplified using the fact that $a+b \leq ab+1 \leq 2ab$ if $a,b \geq 2$.

In total, we get $O(M\log M)$ number of (M,ℓ)-small elliptic curves over k using (5.2).

□

Let S be a finite subset of rational primes. For $n \neq 0, \pm 1 \in \mathbb{Z}$, we say n is S-smooth if all its prime factors lie in S.

Definition 5.3.5. Given $M \in \mathbb{N}$ and ℓ a prime, an elliptic curve E over k is (M,S)-small if there exists a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ such that $\deg\alpha$ is S-smooth.

Definition 5.3.6. Given $M \in \mathbb{N}$ and ℓ a prime, an elliptic curve E over k is (M,S)-big if there does not exist a $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ such that $\deg\alpha$ is S-smooth.

Proposition 5.3.7. Let S be a finite subset of rational primes with $|S| = t$. Then the number of (M,S)-small elliptic curves over k is bounded above by

$$O\left(M(\log M)^{t+1}\right), \tag{5.6}$$

where the constant depends on S.

Proof. Let $S = \{\ell_1, \ldots, \ell_t\}$. The inequalities

$$2^{e_1+\ldots+e_t} \leq \ell_1^{e_1} \cdots \ell_t^{e_t} = c_\alpha \leq M, \tag{5.7}$$

show that $e_1 + \ldots + e_t = O(\log M)$, hence there are $O((\log M)^t)$ choices for c_α, and for each, there are $O(M^{1/2})$ choices for b_α. The rest of the proof is similar to that of Proposition 5.3.4. □

It is remarked in [27, Remark A.4] that when $M \ll p$, roughly half of all M-small elliptic curves are supersingular based on heuristic reasons and computational experiments.

5.4 Numerical data

Definition 5.4.1. Let $\mathcal{T}$ be a tree. A cycle formed identifying two leaf vertices has furthest depth n if n is the distance from the root to the identified vertices.

In this section, we gather statistics on the following quantities:

1. The minimal length cycle through a random vertex in $\bar{G}(p, \ell)$.
2. The minimal depth of a cycle through a descendant of a random vertex in $\bar{G}(p, \ell)$.

Here, by the depth of a cycle (with respect to a vertex $v \in \bar{G}(p, \ell)$), we mean the depth of a farthest vertex in the cycle from the root. The motivation for considering these quantities is the following:

1. If for most vertices $j(E)$ in $\bar{G}(p, \ell)$, the minimal length cycle is $\Omega(\log p)$, then a breadth first search to find a cycle through $j(E)$ will be expensive.
2. If the minimal depth of a cycle through a descendant of most vertices $j(E)$ in $\bar{G}(p, \ell)$ is $\Omega(\log p)$, then a breadth first search to find a cycle through a descendant of $j(E)$ will be expensive.

Remark 5.4.2. If one finds a cycle through a descendant $j(E')$ of $j(E)$, it can be used to obtain a non-scalar endomorphism of E: The cycle through $j(E')$ corresponds to a non-integer endomorphism of E'. The path from E to E' gives an isogeny between E and E', hence the non-integer endomorphism of E' corresponds to a non-scalar endomorphism of E.

Algorithm 3: Finding the length of a minimal cycle through a vertex.

input : An undirected multigraph G and a vertex $v \in V(G)$.

output: Length of a minimal length cycle through v.

If v has a self loop, then return 1.

`// Each vertex` s `visited is labelled with a child of` v `which we refer to as the component.`

$Parents \leftarrow$ Children of v

$Visited \leftarrow \{v\} \cup Parents$

$n \leftarrow 1$

while $\#Visited < \#V(G)$ **do**

  for $s \neq t \in Parents$ **do**

    Check if there is an edge between s and t and they have different components.

    In that case, we have detected a minimal length cycle through v of length $2n+1$.

  end

  for $s \neq t \in Parents$ **do**

    Check if any child [a] of s is equal to any child of t and they have different components.

    In that case, we have detected a minimal length cycle through v of length $2n+2$.

  end

  $Parents \leftarrow$ Children of vertices in $Parents$ where the component is inherited

  $Visited \leftarrow Visited \cup Parents$

  $n \leftarrow n+1$

end

If we reach this point in the algorithm, then there is no cycle in the multigraph G.

[a] We do not consider a parent to be its own child.

Theorem 5.4.3. Given an undirected multigraph G and a vertex $v \in V(G)$, Algorithm 3 computes the length of a minimal cycle through v, if there exists a cycle in G.

Proof. As we enter the **while** loop the nth time, the subgraph induced by the vertices in *Visited* has the property that any cycle through v in this subgraph has length $\geq 2n+1$.

If a collision in the same component occurs in the first **for** loop, then we have detected a cycle of length $2n+1$.

If no collision in the same component occurs in the first **for** loop, then the subgraph induced by the vertices in *Visited* now has the property that any cycle through v in this subgraph has length $\geq 2n+2$.

If a collision in the same component occurs in the second **for** loop, then we have detected a cycle of length $2n+2$.

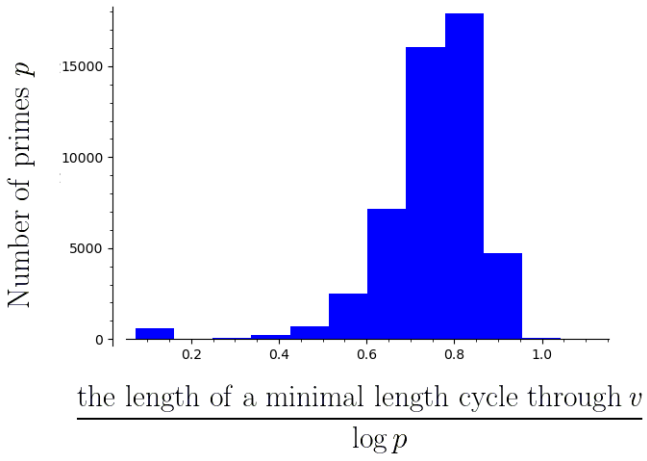
□

Below we analyze a sample of vertices in $\bar{G}(p,3)$ and compute the minimal length of cycles through them. We randomly choose 50000 primes of length less than 20 bits. For each prime p chosen, we pick a vertex v in $\bar{G}(p,3)$ by taking a random walk of length $\lfloor \log p \rfloor$ from $j=0$. Then we compute the relative length of a minimal length cycle through v

$$\frac{\text{the length of a minimal length cycle through } v}{\log p}. \tag{5.8}$$

Then we used a histogram to display the data of the samples. The data suggests that for most of vertices taken randomly from $\bar{G}(p,3)$ for different primes, the minimal length cycle is $\Omega(\log p)$.

Figure 5.1: A histogram (with 12 bins) of the quantity (5.8) for v in $\overline{G}(p,3)$, $p>3$ varies over 50000 random primes of length less than 20 bits and v is picked randomly by taking a random walk of length $\lfloor \log p \rfloor$.



Algorithm 4: Finding a minimal depth cycle through a descendant of a vertex.

input : An undirected multigraph G and a vertex $v \in V(G)$.

output: The minimal depth of cycles through descendants of v

If v has a self loop, then return 0.

$Parents \leftarrow$ Children of v

$Visited \leftarrow \{v\} \cup Parents$

$n \leftarrow 1$

while $\#Visited < \#V(G)$ **do**

  for $s, t \in Parents$ **do**

    Check if there is an edge between s and t.

    In that case, we have detected a cycle through a descendant of v of minimal depth n

  end

  for $s \neq t \in Parents$ **do**

    Check if any child [a] of s is equal to any child of t.

    In that case, we have detected a cycle through a descendant of v of minimal depth $n+1$

  end

  $Parents \leftarrow$ Children of vertices in $Parents$ and the component is inherited

  $Visited \leftarrow Visited \cup Parents$

  $n \leftarrow n+1$

end

If we reach this point in the algorithm, then there is no cycle in the multigraph G.

[a] We do not consider a parent to be its own child.

Theorem 5.4.4. Given an undirected multigraph G and a vertex $v \in V(G)$, Algorithm 4 computes a minimal depth cycle through a descendant of v, if there exists a cycle in G.

Proof. As we enter the **while** loop the nth time, the subgraph induced by the vertices in *Visited* has the property that any cycle in this subgraph has depth $\geq n$.

If a collision in the first **for** loop, then we have detected a cycle of minimal depth n.

If no collision in the first for loop, then the subgraph induced by the vertices in Visited now has the property that any cycle in this subgraph has depth $n+1$

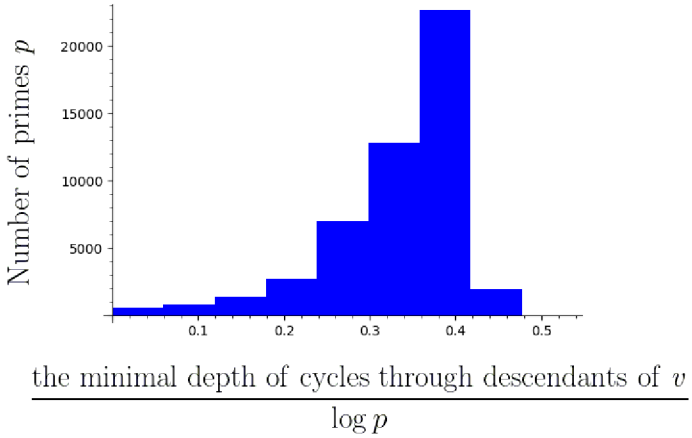
If a collision in the second **for** loop, then we have detected a cycle of minimal depth $n+1$. □

Below we analyze a sample of vertices in $\bar{G}(p,3)$ and compute the minimal depth of cycles through descendants of them. We randomly choose 50000 primes of length less than 20 bits. For each prime p chosen, we pick a vertex v in $\bar{G}(p,3)$ by taking a random walk of length $\lfloor \log p \rfloor$ from

$j = 0$. Then we compute the relative depth of a minimal depth cycle through descendants of v

$$\frac{\text{the minimal depth of cycles through descendants of } v}{\log p}. \tag{5.9}$$

Figure 5.2: A histogram (with 9 bins) of the quantity (5.9) for v in $\overline{G}(p, 3)$, $p > 3$ varies over 50000 random primes of length less than 20 bits and v is picked randomly by taking a random walk of length $\lfloor \log p \rfloor$.



5.5 Examples

A further in depth study of some of the structural features of supersingular isogeny graphs can be found in [1]. Below we give a number of small examples for p in each congruence class modulo 12, $l = 2, 3$, and where we have colored the vertices in $\mathbb{F}_p$ green and the labels of the vertices are the discrete logarithm with respect to a primitive root, with the label p^2 if the vertex is $j = 0$.

Figure 5.3: $\bar{G}(p, \ell)$ for $p = 79$ and $\ell = 2$

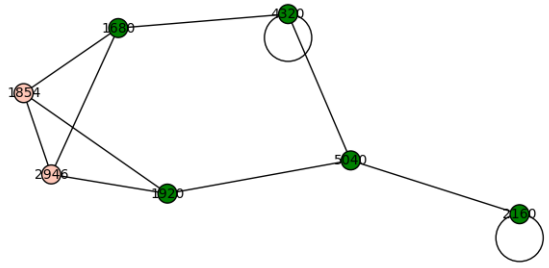


Figure 5.4: $\bar{G}(p, \ell)$ for $p = 79$ and $\ell = 3$

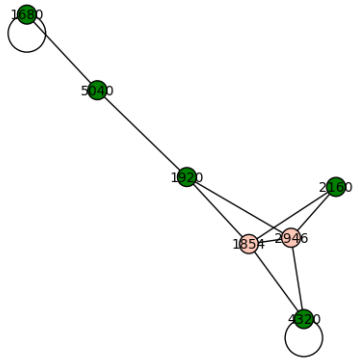


Figure 5.5: $\bar{G}(p, \ell)$ for $p = 83$ and $\ell = 2$

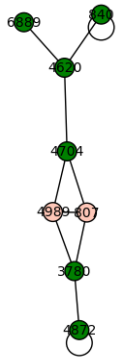


Figure 5.6: $\bar{G}(p, \ell)$ for $p = 83$ and $\ell = 3$

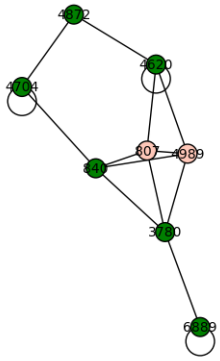


Figure 5.7: $\bar{G}(p, \ell)$ for $p = 97$ and $\ell = 2$

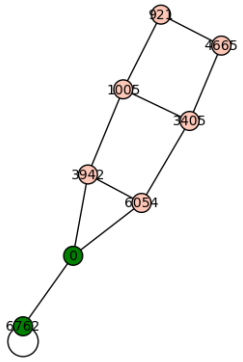


Figure 5.8: $\bar{G}(p, \ell)$ for $p = 97$ and $\ell = 3$

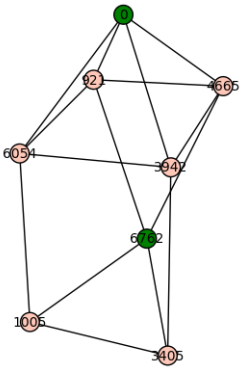


Figure 5.9: $\bar{G}(p, \ell)$ for $p = 101$ and $\ell = 2$

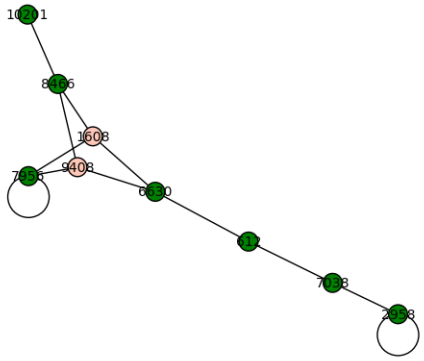


Figure 5.10: $\bar{G}(p, \ell)$ for $p = 101$ and $\ell = 3$

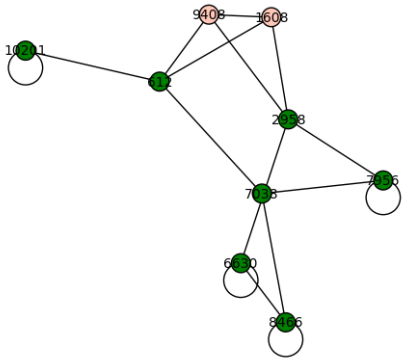


Figure 5.11: $\bar{G}(p, \ell)$ for $p = 997$ and $\ell = 2$

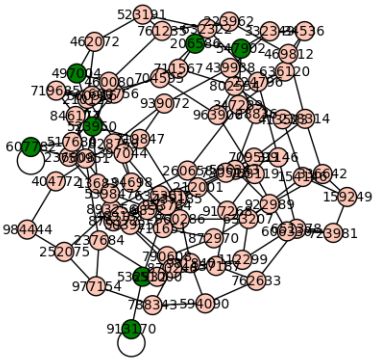
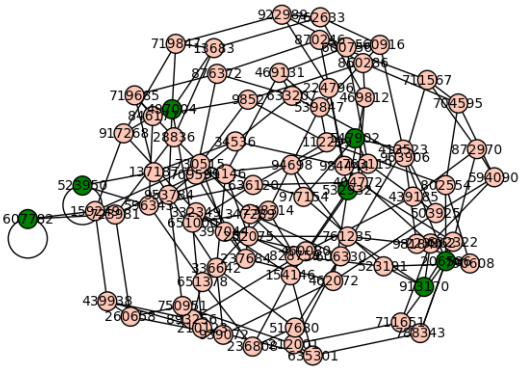


Figure 5.12: $\bar{G}(p, \ell)$ for $p = 997$ and $\ell = 3$



Chapter 6

Computationally Hard Problems

6.1 Overview

In cryptography, the security of hash functions can be measured by checking how difficult the inversion is, which leads to the following standard problems:

Suppose $f : X \to Y$ is a hash function for some finite sets X and Y.

1. Preimage problem: Given $y \in Y$, find $x \in X$ such that $f(x) = y$.
2. Second Preimage problem: Given $x_1 \in X$, find $x_2 \neq x_1 \in X$ such that $f(x_1) = f(x_2)$.
3. Collision problem: Find $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.

In practice, the domain X is taken to be a set of bit strings of arbitrary finite length and the codomain Y is the set of bit strings of fixed finite length n, where the size of Y is relatively smaller than X. The running time of algorithms solving the three problems is measured in terms of n. If there are only exponential time algorithms to solve one of the problems, we say the hash function is resistant to that problem.

Charles, Goren, and Lauter [9] introduced the hardness of finding paths in Supersingular Isogeny Graphs $G(p, \ell)$ into cryptography and used it for constructing cryptographic hash functions. In the CGL hash function, the input is used as directions for walking around a graph without backtracking and the output is the ending vertex of the walk. For a fixed hash function, the walk starts at a fixed vertex in the given graph. A family of hash functions can be defined by allowing the starting vertex to vary. Explicitly finding a collision in this hash function is equivalent to finding two isogenies of ℓ-power degrees between a pair of supersingular elliptic curves. Detecting a collision in CGL hash function can be rephrased to the following problem.

Problem 1. (Path Finding Problem) For a pair of elliptic curves E, E' in a supersingular isogeny graph $G(p, \ell)$, find a path from E to E', which is represented by a chain of $m = O(\log p)$ isogenies of degree ℓ.

Recall that such a path from E to E' exists by Theorem 5.1.3. If the graph does not have small cycles then this problem is very hard, since constructing isogenies of large degree between elliptic curves is a well-known computationally hard problem.

If we can get two distinct paths from E to E' forming a cycle, then that cycle corresponds to a nonscalar endomorphism on E. By doing this multiple times, we can obtain four linearly independent endomorphisms on E with respect to scalar multiplication, which will form a $\mathbb{Z}$-basis of $\mathrm{End}(E)$. Hence, finding a path in a supersingular isogeny graph is related to computation of the endomorphism ring.

Problem 2. (Endomorphism Ring Problem) Given a prime p and a supersigular j-invariant $j \in \mathbb{F}_{p^2}$, compute $\mathrm{End}(E(j))$ by returning four rational maps that form a $\mathbb{Z}$-basis of $\mathrm{End}(E(j))$.

The maps themselves can usually not be returned in their canonical expression as rational maps, as in general this representation will require a space larger than the degree, and the degrees can be as big as p. Meanwhile we want an algorithm of running time polynomial in $\log p$ that computes endomorphism rings, we also want the endomorphism rings to have polynomial representation size. For this, we will introduce the notion of a compact representation of an endomorphism introduced in [17] and use it to define Compact Endomorphism Ring Problem.

Four isogenies representing $\mathrm{End}(E)$ can be given by points in its kernel using Vélu's formula. Hence, we want to avoid having an endomorphism of exponential degree or endomorphism that has the kernel with exponentially many points in the basis for efficient computation of endomorphism ring. To do this we will define compact representation of endomorphisms of polynomial size and show that the endomorphism ring of supersingular elliptic curve has a basis with such a representation.

Let $\mathcal{O}_0 \subseteq B_{p,\infty}$ be chosen as in Proposition 2.6.2 and $b_1, \ldots, b_4$ the chosen ordered basis for $\mathcal{O}_0$ taken in this proposition. Let $E_0 = E(j_0)$ be a supersingular elliptic curve with $\mathrm{End}(E_0) \simeq \mathcal{O}_0$. We showed that there is an isomorphism $B_{p,\infty} \simeq \mathrm{End}(E_0) \otimes \mathbb{Q}$ given by $1, i, j, k \mapsto 1, \phi, \pi, \pi\phi$, where π is the pth power Frobenius map and ϕ is the output of Algorithm 2. In particular, this isomorphism maps the basis of $\mathcal{O}_0$ given in Proposition 2.6.2 to a basis $\beta_1, \cdots, \beta_4$ for $\mathrm{End}(E_0)$. We will use $\beta_1, \cdots, \beta_4$ to define compact representation for endomorphisms of any supersingular elliptic curves.

Definition 6.1.1. (Compact Representation of an Endomorphism)
Let E_0 be the supersingular elliptic curve and $\beta_1, \cdots, \beta_4$ be the endomorphisms of E_0 as above. Let $E/\mathbb{F}_{p^2}$ be another supersingular elliptic curve, and let $\rho \in \mathrm{End}(E)$. Define a compact representation of ρ to be a list

$$\left[d, [c_1, \cdots, c_4], [\phi_1, \cdots, \phi_m], \left[\widehat{\phi_1}, \cdots, \widehat{\phi_m}\right]\right],$$

where $c_1, \cdots, c_4, d \in \mathbb{Z}$, ϕ_i are isogenies on a path from E_0 to E, the total size of the list

$$\log(|d|) + \log(|c_1|) + \cdots + \log(|c_4|) + \sum_{i=1}^{m} \log(\deg(\phi_m))$$

is at most polynomial in $\log p$, and

$$\rho = \frac{1}{d}\left(\phi_m \circ \cdots \circ \phi_1 \circ \left(\sum_{i=1}^{4} c_i\beta_i\right) \circ \widehat{\phi_1} \circ \cdots \circ \widehat{\phi_m}\right).$$

Recall that the existence of the chain of isogenies ϕ_i's was shown in Theorem 5.1.3. In particular, $m = O(\log p)$.

Theorem 6.1.2. Assume GRH holds. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. Then there exist two lists of four compact representatives of endomorphisms of E, such that each list represents a $\mathbb{Z}$-basis of $\mathrm{End}(E)$. Moreover, assume $\rho \in \mathrm{End}(E)$ is a linear combination of the endomorphisms corresponding to one such basis, and assume that its coefficient vector in terms of this basis is of size polynomial in $\log p$. Using the two lists we can evaluate ρ at arbitrary points of E in time polynomial in $\log p$ and the size of the point P.

Proof. We follow the proof in [17, Theorem 15] for $p \equiv 3 \pmod 4$, noting the general case follows under GRH because of Proposition 2.6.2.

Let $\mathcal{O}_0$ be the maximal order in $B_{p,\infty}$ with basis $\{b_1, \cdots, b_4\}$. Then $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ and $b_1, \cdots, b_4$ correspond to $\beta_1, \cdots, \beta_4$ under an isomorphism. There exist chains of isogenies $\phi_1, \cdots, \phi_m$ and $\psi_1, \cdots, \psi_n$ from E_0 to E with $\deg(\phi_k) = 2$ and $\deg(\psi_k) = 3$, and with $m, n = O(\log p)$. Set $\phi = \phi_m \circ \cdots \circ \phi_1$ and $\psi = \psi_n \circ \cdots \circ \psi_1$. Let $I \subseteq \mathcal{O}_0$ and $J \subseteq \mathcal{O}_0$ be the left $\mathcal{O}_0$-ideals corresponding to ϕ and ψ respectively.

There exist rational numbers c_{rs}^I whose denominators are divisors of $2\,\mathrm{nrd}(I)$ such that

$$\gamma_r^I := \sum_s c_{rs}^I b_s, 1 \le r \le 4$$

is a Minkowski-reduced basis of $\mathcal{O}_R(I)$, and rational numbers c_{rs}^J whose denominators are divisors of $2\,\mathrm{nrd}(J)$ such that

$$\gamma_r^J := \sum_s c_{rs}^J b_s, 1 \le r \le 4$$

is a Minkowski-reduced basis of $\mathcal{O}_R(J)$. Furthermore, γ_r^I and γ_r^J have polynomial representation size in terms of $1, i, j, ij$, and hence polynomial representation size in terms of $b_1, \ldots, b_4$ because of the last part of Proposition 2.6.2 (hence the need for GRH). This follows from Theorem 2.6.6 and its proof since $\mathcal{O}_R(I)$ and $\mathcal{O}_R(J)$ are maximal orders by Corollary 4.1.7.

Then $\rho_r^J := \frac{1}{2^m}\phi\gamma_r^I\widehat{\phi}$ and $\rho_r^I := \frac{1}{3^n}\psi\gamma_r^J\widehat{\psi}, r = 1, \cdots, 4$ each form a basis for $\mathrm{End}(E)$. Thus, for $r = 1, \cdots, 4$,

$$[\mathrm{nrd}(I), c_{r1}^I, \cdots, c_{r4}^I, [\phi_1, \cdots, \phi_m], [\widehat{\phi_1}, \cdots, \widehat{\phi_m}]],$$

$$[\mathrm{nrd}(J), c_{r1}^I, \cdots, c_{r4}^I, [\psi_1, \cdots, \psi_n], [\widehat{\psi_1}, \cdots, \widehat{\psi_n}]]$$

satisfy the conditions to be a compact representation of an endomorphism.

Observe that we can efficiently evaluate ρ_r^J at any point P of E whose order is coprime to 2. This is because $[2^m]\rho_r^I$ can be evaluated at P as it is a composition of the $\widehat{\phi_k}$, an integer linear combination of the β_k and then ϕ_k, all of which we can efficiently evaluate in terms of the size of P. Set $Q = [2^m]\rho_r^I(P)$. Let N be the inverse of 2^m modulo the order of P. Then $[N]Q = \rho_r^I(P)$.

Note that we can efficiently find $v \in B_{p,\infty}$ such that $v\mathcal{O}_R(I)v^{-1} = \mathcal{O}_R(J)$ [21]. If we want to evaluate ρ_r^I at a point P with $P \in E[2^f]$, we will instead express $v\rho_r^I v^{-1}$ as an integral linear combination of $\rho_1^J, \cdots, \rho_4^J$. We can evaluate each $\rho_1^J, \cdots, \rho_4^J$ at any point of order coprime to 3 by the same argument.

Thus we can evaluate at arbitrary points P: if P has order $2^f M$ with $(2, M) = 1$, then we can write P as a sum of a point P_2 of order 2^f and P_M of order M. We can then evaluate at P by evaluating it at each summand with the two above strategies. □

Now by computing the endomorphism ring of a supersingular elliptic curve with compact representations, we mean the following problem.

Problem 3. (Compact Endomorphism Ring Problem) Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find a list of total length bounded by $O(\log p)$ of compact representations of endomorphisms of E such that using this list, we can evaluate the corresponding endomorphisms at points of E, and such that the corresponding endomorphism generate $\mathrm{End}(E)$ as a $\mathbb{Z}$-module.

By Deuring's correspondence (Theorem 4.1.9) between maximal orders in a quaternion algebra and supersingular elliptic curves, an alternative way to compute the endomorphism ring is to find the corresponding maximal order. However, this requires to construct such a maximal order with a $\mathbb{Z}$-basis. Hence, we also consider the following problem.

Problem 4. (Maximal Order Problem) Given a prime p, the standard basis for $B_{p,\infty}$, and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, output vectors $\beta_1, \beta_2, \beta_3, \beta_4 \in B_{p,\infty}$ that form a $\mathbb{Z}$-basis of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. In addition, the output basis is required to have representation size polynomial in $\log p$.

Indeed, we already discussed the other direction in the correspondence. Under GRH, Algorithm 5 solves the following problem.

Problem 5. (Constructive Deuring Correspondence) Given a maximal order $\mathcal{O} \subset B_{p,\infty}$, return a supersingular j-invariant such that $\mathrm{End}(E(j)) \simeq \mathcal{O}$.

Note that the authors in [17] also refer to Maximal Order Problem as the "Inverse Deuring Correspondence."

6.2 Known reductions between the problems

Now, we give an overview of the reductions in [17] between the hard problems of supersingular ℓ-isogeny graphs. Let $\mathcal{O}_0$ be chosen as in Proposition 2.6.2. The reductions use the algorithms

in [22, 19] to compute a representative of a class of left $\mathcal{O}_0$-ideals with a given norm N, where $N \approx p^{7/2}$. The heuristics used in [22] can be summarized as saying that the distribution of outputs of quadratic forms arising from the norm form of a maximal order in $B_{p,\infty}$ is approximately like the uniform distribution on numbers of the same size.

Lemma 6.2.1. There exists a probabilistic algorithm, for a given left $\mathcal{O}_0$-ideal I, which returns another left $\mathcal{O}_0$-ideal in the same class as I of norm $\ell^e \approx p^{7/2}$ for some integer e and some small prime ℓ. Under heuristic assumptions on randomness of representations of integers by quadratic forms and uniform distributions of primes, the complexity of this algorithm is polynomial in $\log p$.

Proof. See [22]. □

Recall that a number $N = \prod p_i^{e_i}$ is S-powersmooth if $p_i^{e_i} < S$ for all i. The algorithm in Lemma 6.2.1 has a modification to construct representatives of powersmooth norms under similar heuristic assumptions.

Lemma 6.2.2. There is a probabilistic algorithm, for a given left $\mathcal{O}_0$-ideal I, which returns another left $\mathcal{O}_0$-ideal in the same class as I of norm $\prod p_i^{e_i} \approx p^{7/2}$ with $p_i^{e_i} < \log p$. Under heuristic assumptions on randomness of representations of integers by quadratic forms and uniform distributions of primes, the complexity of this algorithm is polynomial in $\log p$.

Proof. See [19]. □

The reductions in [17] would make the same heuristic assumptions depending on which algorithms in Lemma 6.2.1 and Lemma 6.2.2 they use.

The reductions in [17] also require several other algorithms. To compute a random connecting ideal of two given maximal orders in $B_{p,\infty}$ of size polynomial in $\log p$, we need the following.

Proposition 6.2.3. There is a algorithm, for given Eichler orders $\mathcal{O}, \mathcal{O}'$ of the same level, computes a connecting ideal I with $\mathcal{O}_R(I) = \mathcal{O}$ and $\mathcal{O}_L(I) = \mathcal{O}'$.

Proof. See [21, Algorithm 3.5]. □

We also need an algorithm translating $\mathcal{O}_0$-ideals to corresponding isogenies given by Deuring's correspondence.

Proposition 6.2.4. There exists an algorithm an algorithm which, given an left $\mathcal{O}_0$-ideal I of norm $N = \prod p_i^{e_i}$ with $N = O(\log p)$ and $p_i^{e_i} = O(\log p)$, returns an isogeny corresponding to I through Deuring's correspondence. The complexity of this algorithm is polynomial in $\log p$.

Proof. See [19, Lemma 5]. □

Proposition 6.2.5. There is an algorithm giving a reduction from Endomorphism Ring Problem to Maximal Order Problem, which can be implemented to run in time polynomial in $\log p$ under plausible heuristic assumptions.

Proof. We summarize the proof in [17].

Suppose we have an efficient algorithm for Maximal Order Problem. Given a supersingular j-invariant j, Algorithm 4 in [17] returns four maps generating $\mathrm{End}(E(j))$ of the form $\frac{\sum_{i=1}^{4} c_{ij}\phi\beta_i\hat{\phi}}{N}$, where $c_{ij} \in \mathbb{Z}$, $\phi : E_0 \to E(j)$ is an isogeny of powersmooth degree N, and β_i are four maps generating $\mathrm{End}(E_0)$. Note that ϕ was obtained by computing a connecting ideal of maximal orders $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ and $\mathcal{O} \simeq \mathrm{End}(E(j))$ with powersmooth norm N using Proposition 6.2.2, and then constructing ϕ using Proposition 6.2.4. Under heuristic assumptions as in Proposition 6.2.2, Algorithm 4 runs in time polynomial in $\log p$ [17, Proposition 5].

Unlike the compact representation we defined in Definition 6.1.1, the four maps don't have ℓ-power norm. However, we can still efficiently evaluate them at arbitrary points in $E(j)$ using Algorithm 5 in [17]. For the complexity analysis and the validation of Algorithm 5, see [17, Lemma 3]. □

The authors in [17] also presented an algorithm returning compact representations of four maps forming a basis of the endomorphism ring of a given supersingular elliptic curve E in terms of ℓ-power isogenies. To give such compact representations, we need to know additional information other than the solution to Maximal Order Problem, namely the actions of the maps on $E[\ell]$ for some small primes ℓ, which can be summarized as follows.

Problem 6. (Action-on-ℓ-Torsion) Given a prime p, a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, and four elements $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ in a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ such that there exists an isomorphism $\theta : \mathrm{End}(E) \to \mathcal{O}$, output eight pairs of points on E, $(P_1, Q_{1r}), (P_2, Q_{2r}), r = 1, \cdots, 4$ such that P_1, P_2 form a basis for the ℓ-torsion $E[\ell]$ of E, and such that $Q_{1r} = \theta^{-1}(\beta_r)(P_1)$ and $Q_{2r} = \theta^{-1}(\beta_r)(P_2)$ for $r = 1, \cdots, 4$.

Proposition 6.2.6. There is an algorithm giving reductions from each of Path Finding Problem and Endomorphism Ring Problem to Maximal Order Problem together with Action-on-ℓ-Torsion. Assuming $\ell = O(\log p)$ and plausible heuristic assumptions, the algorithm runs in time polynomial in $\log p$ and makes $O(\log p)$ queries of Maximal Order Problem and Action-on-ℓ-Torsion

Proof. We summarize the proof in [17].

Suppose we have an efficient algorithm for Maximal Order Problem and Action-on-ℓ-Torsion. Algorithm 9 in [17] takes supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$ with a prime $\ell \neq p$ as inputs and return a chain of ℓ-isogenies connecting E and E'.

Note that Algorithm 9, for two supersingular elliptic curves E and E', first computes a connecting ideal I of $\mathcal{O} \simeq \mathrm{End}(E)$ and $\mathcal{O}' \simeq \mathrm{End}(E')$, whose norm is ℓ^e for some $e = O(\log p)$ using

Proposition 6.2.1. Suppose this ideal corresponds to an isogeny $\phi : E \to E'$ of degree ℓ^e under Deuring Correspondence. To find a factorization $\phi = \psi_e \circ \cdots \circ \psi_1$ into ℓ-isogenies which are of polynomial representation size, we find a factorization of the ideal I

$$I = I_e \subseteq I_{e-1} \subseteq \cdots \subseteq I_1 \subseteq I_0 = \mathcal{O}$$

so that the isogeny corresponding to I_k is a map ϕ_k from E to some intermediate curve E_k of degree ℓ^k and $\phi_k = \psi_k \circ \cdots \circ \psi_1$. Indeed, we can take $I_k = I + \mathcal{O}\ell^k$. The ideal connecting the maximal orders $\mathcal{O}_R(I_K)$ to $\mathcal{O}_R(I_{k+1})$ is $J_k := I_{k-1}^{-1} I_k$, and this will correspond to ψ_k. We compute ψ_k iteratively as follows; Suppose we have computed ψ_k, the curve E_k, and J_{k+1} as above. We use the oracle for Maximal Order Problem to find generators of J_{k+1} as identified with endomorphisms of E_k. On the other hand, J_{k+1} corresponds to the isogeny ψ_{k+1}, whose kernel we compute using the information from the oracle Action-on-ℓ-Torsion. Then we can compute ψ_{k+1} from its kernel using Vélu's formula. For full details of the algorithm with complexity analysis, see [17, Theorem 10].

To get a reduction from Endomorphism Ring Problem to Maximal Order Problem and Action-on-ℓ-Torsion, fix $E = E_0$ so that $\mathrm{End}(E_0) \simeq \mathcal{O}_0$ as in Proposition 2.6.2 and use Algorithm 9 for $\ell = 2, 3$. By Theorem 6.1.2, we have all necessary information to give compact representations of generators of $\mathrm{End}(E')$.

Since this algorithm uses Proposition 6.2.1, it has the same heuristic assumptions. □

Proposition 6.2.7. Algorithm 6 in [17] gives a reduction from Maximal Order Problem to Endomorphism Ring Problem. Under plausible heuristic assumptions, the reduction can be implemented to run in polynomial time.

Proof. For full details of the proof, see [17, Lemma 4, Lemma 5, Lemma 6, Lemma 7, and Proposition 6].

Suppose we have an efficient algorithm that, for a given supersingular elliptic curve E, returns four maps $1, \alpha, \beta, \gamma$ generating $\mathrm{End}(E)$, in some format that allows efficient evaluation of the maps at arbitrary points. Algorithm 6 constructs a sequence of linear transformations that map $1, \alpha, \beta, \gamma$ to four orthogonal maps $1, \iota, \lambda, \iota\lambda$ corresponding to $1, i, j, k \in B_{p,\infty}$. In Steps 4 and 7, the algorithm requires easy factorization of the numerators and denominators of the reduced norm of the maps, and applies a random invertible linear transformation to the four maps to find new maps satisfying such conditions. It was heuristically assumed that the process of randomization ceases after a number of steps that is polynomial in $\log p$. Also, Step 5 requires an algorithm to solve some diophantine equations, which heuristically runs in polynomial time. At the end, inverting and composing all linear transformations to express $1, \alpha, \beta, \gamma$ in the basis $(1, \iota, \lambda, \iota\lambda)$ gives a basis of $\mathcal{O} \subseteq B_{p,\infty}$. □

Proposition 6.2.8. Algorithm 7 in [17] gives a reduction from Path Finding Problem to Endomorphism Ring Problem. Under plausible heuristic assumptions, the reduction can be implemented to run in polynomial time.

Proof. We summarize the proof in [17, Proposition 7].

We use the similar method used in Proposition 6.2.6. Suppose we have an efficient algorithm computing the endomorphism ring of supersingular elliptic curves. For each of two given supersingular j-invariants j, j', we do the following; compute the endomorphism ring $\mathrm{End}(E(j))$, and then using Proposition 6.2.7, compute the maximal order $\mathcal{O} \simeq \mathrm{End}(E(j))$. Apply Proposition 6.2.1 to compute an ideal $J = \mathcal{O}_0\alpha + \mathcal{O}_0\ell^e$ with norm ℓ^e. We find the filtration of ideals $J_i = \mathcal{O}_0\alpha_i + \mathcal{O}_0\ell^i$ for $i = 0, \cdots, e$, compute an ideal K_i with powersmooth norm in the same class as J_i using Proposition 6.2.2, and translate K_i into an isogeny $\phi_i : E_0 \to E_i$. Then we get a sequence $(j_0, j(E_1), j(E_2), \cdots, j(E_e) = j(E))$, which gives a path from E_0 to $j(E)$. Repeating this process for another curve $E(j')$, and then concatenating two paths gives a path from $E(j)$ to $E(j')$.

For the algorithm to run in polynomial time, it requires heuristic assumptions used in Proposition 6.2.1 and Proposition 6.2.2. □

Proposition 6.2.9. Algorithm 8 in [17] gives a reduction from Endomorphism Ring Problem to Path Finding Problem. Under plausible heuristic assumptions, the reduction can be implemented to run in polynomial time.

Proof. We summarize the proof in [17, Proposition 8].

Algorithm 8 requires the following heuristic assumption to randomly introduce endomorphisms into the subring $\mathcal{R}$ in the loop in Step 2; given a suborder $\mathcal{O}'$ of maximal order $\mathcal{O}$ such that $\mathcal{O}'$ is generated by loops in an ℓ-isogeny graph, the probability that a randomly generated loop in the graph is in $\mathcal{O}'$ is inversely proportional to $[\mathcal{O} : \mathcal{O}']$.

Suppose the subring $\mathcal{R}$ has index N after adding some endomorphisms. Then any new randomly generated endomorphism would lie in this subring with probability $1/N$. Moreover when it does not lie in the subring, the element will decrease the index by a non-trivial integer factor of N. □

Note that we can generalize Algorithm 2 so that it will return a supersingular j-invariant whose endomorphism ring is isomorphic to a general order $\mathcal{O} \subseteq B_{p,\infty}$ by using the connecting ideal of $\mathcal{O}_0$ and $\mathcal{O}$.

Proposition 6.2.10. Given a prime p and a maximal order $\mathcal{O} \subseteq B_{p,\infty}$, Algorithm 5 computes a supersingular j-invariant j such that $\mathrm{End}(E(j)) \simeq \mathcal{O}$.

Proof. See [17, Proposition 13]. □

We remark the problems considered in this last chapter are well studied for ordinary elliptic curves as first treated by Kohel in [23]. Childs, Jao, and Soukharev [10] gave a quantum algorithm

Algorithm 5: Constructive Deuring correspondence, from general maximal orders to j-invariants.

input : Maximal order $\mathcal{O} \subset B_{p,\infty}$
output: Supersingular j-invariant j such that $\mathrm{End}(E(j)) \simeq \mathcal{O}$

1. Compute an ideal I that is a left ideal of $\mathcal{O}_0$ and a right ideal of $\mathcal{O}$.
2. Compute an ideal J in the same class as I but with powersmooth norm.
3. Compute an isogeny $\phi : E_0 \to E_I$ that corresponds to J via Deuring's correspondence.
4. Return $j(E_I)$.

for constructing isogenies between ordinary elliptic curves, which is subexponential assuming GRH. It was shown that their method yields a subexponential algorithm for computing endomorphism rings of ordinary elliptic curves under GRH by Bisson [4]. Also, Bisson and Sutherland [5] gave two algorithms for computing the endomorphism ring of ordinary elliptic curves which are subexponential under suitable heuristic assumptions.

Bibliography

[1] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, and J. Sotáková. Adventures in supersingularland. ArXiv preprint, arXiv:1909.07779v1, 2019.

[2] Eric Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[3] E. Bank, C. Camacho-Navarro, K. Eisentraeger, R. Morrison, and J. Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. ArXiv preprint, arXiv:1804.04063v2, 2018.

[4] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *J. Math. Cryptol.*, 5(2):101–113, 2011.

[5] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011.

[6] Reinier Bröker. Constructing elliptic curves of prescribed order. 2006. Thesis (Ph.D.)–Universiteit Leiden.

[7] Reinier Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.

[8] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[9] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Families of Ramanujan graphs and quaternion algebras. In *Groups and symmetries*, volume 47 of *CRM Proc. Lecture Notes*, pages 53–80. Amer. Math. Soc., Providence, RI, 2009.

[10] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[11] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskás. Ramanujan graphs in cryptography. ArXiv preprint, arXiv:1806.05709v2, 2018.

[12] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[13] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by Hugh L. Montgomery.

[14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[15] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptogr.*, 78(2):425–440, 2016.

[16] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[17] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology-EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018.

[18] Steven D. Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, Cambridge, 2012.

[19] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology—ASIACRYPT 2017. Part I*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Springer, Cham, 2017.

[20] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43(4):439–561, 2006.

[21] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[22] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS J. Comput. Math.*, 17(suppl. A):418–432, 2014.

[23] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields.* ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley.

[24] Alain Kraus. Une remarque sur les points de torsion des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 321(9):1143–1146, 1995.

[25] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[26] Stéphane Louboutin. L-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field. *Math. Comp.*, 59(199):213–230, 1992.

[27] Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphisms. In *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, 2020*, volume 4 of *Open Book Series*, pages 7–22. Mathematical Sciences Publishers, 2020.

[28] Phong Q. Nguyen and Damien Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Trans. Algorithms*, 5(4):Art. 46, 48, 2009.

[29] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[30] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[31] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[32] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[33] John Voight. *Quaternion algebras*. Version 0.9.22 edition, 2020.