ENDOMORPHISM RINGS OF HYPERELLIPTIC JACOBIANS

Marelize Kriel

Thesis presented in partial fulfilment of the requirements for the degree of
MASTER OF SCIENCE at the UNIVERSITY OF STELLENBOSCH.

Supervisor: Professor B W GREEN
April, 2005

Declaration

I declare that this thesis contains no material which has been accepted for a degree or diploma by the University or any other institution, except by way of background information and duly acknowledged in the thesis, and that, to the best of my knowledge and belief, this thesis contains no material previously published or written by another person, except where due acknowledgement is made in the text of the thesis.

Signed: _____
Marelize Kriel

Date: _____

Abstract

The aim of this thesis is to study the unital subrings contained in associative algebras arising as the endomorphism algebras of hyperelliptic Jacobians over finite fields.

In the first part we study associative algebras with special emphasis on maximal orders. In the second part we introduce the theory of abelian varieties over finite fields and study the ideal structures of their endomorphism rings.

Finally we specialize to hyperelliptic Jacobians and study their endomorphism rings.

Opsomming

In hierdie proefskrif kyk ons na subringe in assosiatiewe algebras wat natuurlik voorkom as die endomorfisme ringe van Jacobiese varietiete van hyperelliptiese krommes oor eindige liggame.

In die eerste gedeelte kyk on na assosiatiewe algebras met klem op maksimale orde-ringe. Die tweede gedeelte bestaan uit ‘n inleiding tot die teorie van abelse varieteite en die ideaal struktuur van hulle endomorfisme ringe.

In die finale gedeelte spesialiseer ons na hyperelliptiese Jacobiese varieteite en kyk na hulle endomorfisme ringe.

Acknowledgements

I would like to dedicate this manuscript in memory of my mother, Margaretha Johanna Gertruida Kriel (29/03/1945-01/02/2004) who supported me thoughout my life and whose example, friendship and motherly love was greatly missed in the last nine months.

Great thanks go to my father for his guidance, prayers and support throughout my educational pursuits.

Thanks are also due to my current employers at EMSS for showing patience and generosity in equal measure. I am also grateful to the National Research Foundation for the financial support given while this research was undertaken.

My thanks also to Carl Maxson, his unique ability to convey his wonderful intuition and insight contributed largely to my interest in noncommutative algebra. I also express my gratitude to the rest of the lecturers at the University of Stellenbosch for the many courses, seminars, and conversations over the last two years.

Finally but not least I would like to thank my supervisor, Prof. Barry Green, his comments, corrections and constant encouragement is greatly appreciated.

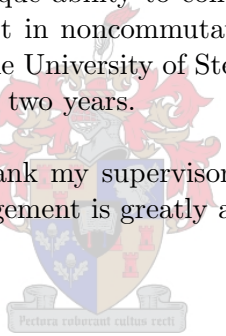


Table of Contents

Chapter 1

Introduction

Elliptic curves are among the most exciting and central objects in modern number theory. Several very deep results have been proved about elliptic curves in the last two decades. There is a vast literature dealing with the number of rational points on elliptic curves over finite fields and the determination of the endomorphism ring arises as a natural sequel to this. The theory of hyperelliptic curves has not recieved as much attention by the research community and it enters the new century with some of it's major secrets intact. This dissertation is principally concerned with the endomorphism rings of Jacobian varieties of hyperelliptic curves.

The Jacobian of a hyperelliptic curve over a finite field is a principally polarized abelian variety over the field of definition and its endomorphism ring is an order in a finite dimensional algebra over a number field. It has long been known which algebras arise as endomorphism algebras of principally polarized abelian varieties, however, if we restrict our attention to Jacobian varieties of curves of a given genus, the question is less well understood.

Pectora roborant cultus recti

The theory of hyperelliptic curves, while loath to relinquish its most pregnant secrets, has yielded a bounty of arithmetic insights in the 20th Century. It has also conjured a host of new questions, suggesting fresh avenues of exploration for the new century, and the purpose of this dissertation is to yield a better understanding of the subtle interactions between the orders in finite dimensional algebras and endomorphism rings of hyperelliptic Jacobians. Interesting unsolved problems are posed to the reader and a comprehensive list of references is included.

This thesis is organized as follows. In this introductory chapter we give a short summary of the problems we will be addressing. The theory is then split up into three chapters of nearly equal length.

The first part of Chapter 2 is based on the paper [19] and his joint work with Lajos Ronyai. The results are related to the structure of simple algebras over number fields. The methods are based on certain non-commutative generalizations of ideas from algebraic number theory. The central result stated is a deterministic algorithm that finds a maximal order (a non-commutative analogue of the ring of algebraic integers in number fields) in a semisimple algebra over a number field.

We then focus our attention on the quaternionic case and give a brief digression into the theory of quadratic spaces since it is needed in the discussions that follow. The main purpose of the next section is to provide an introduction to the arithmetic theory of quaternion algebras. In short we give a way of representing a quaternion algebra with given discriminant and give complements to the existing more ring-theoretic description of orders studied in the first half of the chapter. In particular they are more useful for computations. Finally we look at quadratic spaces associated with quaternion algebras and the integral quadratic modules which they contain.

In Chapter 3 we present results of Honda and Tate on the classification up to isogeny of abelian varieties over finite fields. After the necessary background material is covered we closely follow the work of Waterhouse. His work provides us with techniques for passing from ideals of the endomorphism ring to varieties in the isogeny class. We will see various ways in which facts about maximal orders can be transformed into facts about varieties and show why the absence of theory for non-maximal orders makes the general case so much more complicated. The content is naturally divided into the theory of ordinary and supersingular abelian varieties.

In Chapter 4 we specialize to Jacobians of hyperelliptic curves. Throughout the chapter we will consider elliptic curves as a special case in which our theory can be made explicit. Most results concerning hyperelliptic curves, which appear in the literature on algebraic geometry are couched in very general terms. And a non-specialist will have extreme difficulty specializing (not to mention finding) results in these books. Another difficulty one encounters is that the theory is usually restricted to the case of hyperelliptic curves over an algebraically closed field or the complex numbers. For a good introduction we refer the reader to [22].

Modular equations relating invariants of ℓ-isogenous elliptic curves are a fundamental tool in computational arithmetic geometry and will be of great help to us in determining the isomorphism type of the endomorphism ring. A great effort has been devoted to obtain equations sparser in degree or with smaller coefficients than the classical polynomials. Nevertheless, very little is known about similar equations for higher genus curves. Using the ideas of P. Gaudry we define modular equations for hyperelliptic curves, without appealing to modular forms and give proofs that the well-known factorization properties of genus 1 modular equations extend to the higher genus constructions which makes them amenable for use in higher genus extensions of existing algorithms. The rest of the chapter is then split up into an ordinary and a supersingular part.

In the ordinary case we state practical methods developed by Kohel to determine the isomorphism type of the endomorphism ring of an ordinary elliptic curve. This dissertation does not focus on complexity issues of these algorithms, but more on their correctness and the ideas involved. We then show how his ideas can partially be extented to hyperelliptic curves of higher genus. Most examples presented are obtained by the authors own implementation using the Magma computer algebra system.

The relation between supersingular elliptic curves and the ideal theory in a quaternion algebra appears in the classical work of Deuring. In the modern theory it is properly stated

as an equivalence of categories and we show how the rings of homomorphisms of elliptic curves correspond to quadratic modules under this equivalence.

In the final section we point out other methods which might assist in the determination of the endomorphism ring of a hyperelliptic jacobian.

Chapter 2

Associative algebras

Throughout this chapter L is a finite dimensional associative algebra over the field K. Because of associativity the product $\alpha_1\alpha_2\cdots\alpha_r$ of r elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in L$ can be defined in a straightforward way.

The centralizer $\text{centre}_L(M)$ of a subset M of L is the set consisting of elements of L commuting with every element of the subset M. Obviously $\text{centre}_L(M)$ is a K-subalgebra of L. The centre of L is the subalgebra $\text{centre}_L(L)$. We will simply denote it by $\text{centre}(L)$. An element $e \in L$ is called an identity element if $ea = ae = a$ holds for every $a \in L$. If L admits an identity element then this element is known to be unique and denoted by 1.

An algebra L is said to be simple if is contains no proper ideals. We say that a pair of nonzero elements $a, b \in L$ is a pair of zero divisors in L if $ab = 0$. From the assumption that L is finite dimensional it follows that $a \in L$ is the left member of a pair of zero divisors if and only if a is the right member of a pair of zero divisors. We call such an a a zero divisor. It turns out that a is a zero divisor if and only if the left ideal La is a proper K-subalgebra of L (if and only if for the right ideal aL is a proper K-subalgebra of L). Algebras without zero divisors (called division algebras over K or skewfield extensions of K) are simple and a commutative algebra L is simple if and only if L admits no zero divisors. Therefor every finite dimensional commutative simple algebra over K is isomorphic to a finite extension field of K.

A central simple algebra over a field K is a finite dimensional simple K-algebra L whose centre is K. If L is a division algebra we call it a central division algebra.

Let $\{a_1, a_2, \ldots a_n\}$ be a linear basis of L over K. Then multiplication can be described by representing the products a_ia_j as linear combinations of the basis elements,

$$a_ia_j = \sum_{k=1}^{n} c_{ijk}a_k.$$

The coefficients $c_{ijk} \in K$ are called structure constants and we consider associative algebras to be given as an array of structure constants.

An element a in L is nilpotent if $a^r = 0$ for some positive integer exponent r. For a positive integer j and a subset M of L we denote the set $\{a_1 \cdots a_j \mid a_1, \ldots, a_j \in M\}$ by M^j. It is straightforward to see that if M is a K-subspace (subalgebra, left ideal, right ideal, ideal) of L then M^j is a K-subspace (subalgebra, left ideal, right ideal, ideal respectively) as well. A subalgebra F is called nilpotent if $F^r = 0$ for some integer $r > 0$. This in turn is equivalent to that $F^r = 0$ for some integer $r \leq \dim_K(F) + 1$. It is known that a subalgebra F is nilpotent if and only it consists of nilpotent elements.

There exists a largest nilpotent ideal of L called the (Jacobson) radical of L and denoted by $\mathrm{Rad}(L)$. There are several characterizations of the radical such as the intersection of the maximal ideals or the set of strongly nilpotent elements, where a is said to be strongly nilpotent if a, ab, ba are nilpotent for any b in L, etc. Note that the two-sided characterizations above could be replaced by analogous left-sided or right-sided ones.

2.1 Semisimple algebras

The results presented in this section are based on methods from the paper [19] and his joint work with Lajos Ronyai. In [30] it was proved that there exists a maximal $\mathbb{Z}$-order in a central simple algebra over a number field which admits a short description and verification and that the theory of maximal orders and Hasse's principle can be used to determine the index from invariants of maximal orders. To be more specific the main technical contribution in [30] is a deterministic algorithm for testing maximality of orders. The central result of this chapter is a deterministic algorithm for constructing maximal orders in semisimple algebras over number fields.

A finite dimensional associative K-algebra, L is called semisimple if $\mathrm{Rad}(L) = 0$. It turns out that the factor algebra $L/\mathrm{Rad}(L)$ is semisimple. We call $L/\mathrm{Rad}(L)$ the radical free part of L or the semisimple part of L. There is a very strong and useful characterization of semisimple algebras, due to Wedderburn.

2.1.1 Wedderburn's structure theorem

Theorem 2.1.1 *Let L be a finite dimensional algebra over the field K.*

(a) L is semisimple if and only if L is the direct sum of simple algebras $L = L_1 \oplus \ldots \oplus L_r$ where the L_i are the only non-trivial minimal ideals of L.

(b) L is simple if and only if $L \cong \mathbb{M}_t(D)$ where D is a division algebra over K and t is a positive integer.

Proof See [29] Theorem 7.4. □

Let L be semisimple. We stick to the notation of Theorem 2.1.1. The minimal ideals $L_1, \ldots, L_r$ are also called the simple components of L and the decomposition in part (a) is called the Wedderburn decomposition of L. We remark that the Wedderburn decomposition of the centre, $\mathrm{centre}(L)$, corresponds to the decomposition of L. The minimal ideals

of centre(L) are centre$(L_1), \ldots,$ centre(L_r). A semisimple algebra L necessarily admits an identity element e. In that case we identify K with the K-subalgebra Ke of centre(L). An algebra L is central over K if centre$(L) = K$. Every simple algebra is central over its centre which is a finite extension field of K.

Assume that L is central simple over K. We know that $\dim_K(L)$ is a square n^2, the number t in Wedderburns theorem (b) is a divisor of n while D is a central division algebra over K of dimension $(nt^{-1})^2$. The number nt^{-1} is called the index of L. The minimal left ideals of L have dimension n^2t^{-1} over K.

The minimal polynomial of an element a of a K-algebra L with identity is the monic polynomial $f \in K[x]$ such that $f(a) = 0$ and f is of minimum degree among the polynomials satisfying this property. For a polynomial $g(x) = \sum_{i=0}^{d} \lambda_i x^i \in K[x]$, $g(a)$ is defined as $g(a) = \sum_{i=0}^{d} \lambda_i a^i \in L$, using the convention $a^0 = 1$. It is known that if $f(x)$ is the minimal polynomial of a then the set $\{g(x) \in K[x] \mid g(a) = 0\}$ is the principal ideal $\langle\, f(x) \,\rangle$ of $K[x]$ generated by $f(x)$.

If E is an arbitrary extension field of K then the E-space $L_E = E \otimes_K L$ can be considered as an E-algebra in a natural way. Multiplication is the K-bilinear extension of $a_1 \otimes b_1 \cdot a_2 \otimes b_2 = a_1 a_2 \otimes b_1 b_2$. L can be identified with the K-subalgebra $1 \otimes L$ of L_E. Note that if $\{a_1, \ldots, a_n\}$ is a K-basis of L then $\{a_1, \ldots, a_n\}$ is an E-basis of L_E.

L is called separable over K if L_E is semisimple over any field extension E of K. It turns out that a finite dimensional K-algebra is separable over K if and only if L is semisimple and the simple components of centre(L) are separable extension fields of K. In particular every central simple algebra is separable as well as every semisimple algebra over a perfect field.

Pectora roborant cultus recti

2.1.2 Orders in semisimple algebras

Let R be a Dedekind domain (i.e. Noetherian, integrally closed such that every prime ideal of R is a maximal ideal). Let K be the field of quotients of R and let V be a finite dimensional vector space over K. An R-lattice in V is a finitely generated R-submodule of V.

Let M and N be R-lattices in V. The index of N in M, denoted $[M : N]$, is defined to be the R-ideal generated by $\{\det(\varphi) \mid \varphi :\ V \to V$ a linear transformation such that $\varphi(M) \subseteq N\}$. In particular if both M and N have R-bases then $[M : N]$ is the ideal generated by the determinant of the matrix which takes a basis of M into a basis of N.

If, in addition to being an R-lattice, M is a K-space generating set of the entire space V, then we say M is a full R-lattice in V. Full lattices in the vector space V, of which R-orders are special cases, are of particular interest.

Let L be a finite dimensional semisimple algebra over K. An R-order in L is a subring $\mathcal{O}$ of L which satisfies the following properties

(a) $\mathcal{O}$ is a finitely generated R-module

(b) $\mathcal{O}$ has an identity element (this is necassarily the same as the identity of L)

(c) $\mathcal{O}$ generates L as a linear space over K ($\mathcal{O}$ contains a basis for L over K)

Such an $\mathcal{O}$ is a maximal R-order in L if it is not a proper subring of any other R-order in L.

Example For every matrix α in $\mathrm{GL}_n(\mathbb{Q})$, the ring $\alpha^{-1}\mathbb{M}_n(\mathbb{Z})\alpha$ is a maximal $\mathbb{Z}$-order in the central simple $\mathbb{Q}$-algebra $\mathbb{M}_n(\mathbb{Q})$. Actually every maximal $\mathbb{Z}$-order in $\mathbb{M}_n(\mathbb{Q})$ is of this form, however this fact does not generalize to the case where the ground ring R is not a principal ideal domain. □

It is known that if L is a commutative separable K-algebra (e.g. every simple component of L is a finite separable field extension of K), then the integral closure of R in L, defined by $\mathcal{O}_L = \{a \in L |$ there exists a monic polynomial $f(x) \in R[x]$ such that $f(a) = 0\}$, is the unique maximal R-order in L and is the product of the maximal R-orders in the simple components of L.

The organization of this section is as follows. The first part contains the basic statements from the theory of orders we need. We then collect some results about the radicals of orders over discrete valuation rings. These play an important role in the study of extremal orders later on which will enable us to reduce the problem of finding maximal orders over discrete valuation rings to that of decomposing associative algebras over the residue class fields. The ideas presented here are not new. They were used by Jacobinski (see [20] or [29] Chapter 39) in his approach to the theory of hereditary orders. In the statements here the completeness of R is not assumed. Also largely due to the fact that weaker results are sufficient for our purposes it was possible to simplify some of the original arguments. The last section contains an algorithm for computing maximal orders. We first provide the basic iteration step of our subsequent methods for constructing locally maximal orders and then describe an algorithm that for a given order, $\mathcal{O}$, constructs an order, Λ, containing $\mathcal{O}$ such that Λ is locally greater than $\mathcal{O}$, if such an order exists.

Reduced trace forms and discriminants

Let R be a Dedekind domain with quotient field K and L a finite dimensional semisimple algebra over K. We introduce the reduced trace function of a semisimple algebra using a sequence of progressively more general definitions (for a central simple algebra, then a simple algebra, and finally for a semisimple algebra).

We start from the trace of a left regular representation of L. To be more specific, the trace, denoted $\mathrm{trace}_{L/K}(a)$, of an element, a of L over K is the trace of the matrix representing the K-linear transformation $L_a : L \to L$ defined by $L_a(b) = ab$ for $b \in L$. If L is a full matrix algebra over the field E, where $\dim_E(L) = m^2$, then there is another way to define traces of elements in L. Namely if we have an isomorphism $\sigma : L \to \mathbb{M}_m(E)$ then we can take $\mathrm{trace}_{L/E}(a)$ as the trace of the matrix σa. Furthermore this is independant of the choice of σ.

If L is a central simple K-algebra with $\dim_K(L) = m^2$ then there exists an extension

field E of K which splits L, i.e. $L \otimes_K E \cong \mathbb{M}_m(E)$. It can be shown that $\overline{\mathrm{t}}\mathrm{race}(a) = \mathrm{trace}_{(L\otimes_K E)/E}(a) \in K$ is independant of the choice of the splitting field E and we have $m \cdot \overline{\mathrm{t}}\mathrm{race}(a) = \mathrm{trace}_{L/K}(a)$. Consequently if the characteristic of K is zero (or prime to m) then $\overline{\mathrm{t}}\mathrm{race}(a) = m^{-1}\mathrm{trace}_{L/K}(a)$.

If L is a simple K-algebra with $F = \mathrm{centre}(L)$ then we can take

$$\overline{\mathrm{t}}\mathrm{race}(a) = \mathrm{trace}_{F/K}(\overline{\mathrm{t}}\mathrm{race}_{L/F}(a)).$$

If L is a semisimple K-algebra with Wedderburn decomposition $L = L_1 \oplus L_2 \oplus \ldots \oplus L_r$ then we define

$$\overline{\mathrm{t}}\mathrm{race}(a) = \overline{\mathrm{t}}\mathrm{race}_{L_1/K}(a_1) \oplus \overline{\mathrm{t}}\mathrm{race}_{L_2/K}(a_2) \oplus \ldots \oplus \overline{\mathrm{t}}\mathrm{race}_{L_r/K}(a_r)$$

where a_i is the image of a under the projection map $L \to L_i$ onto the i^{th} simple component of L. We call $\overline{\mathrm{t}}\mathrm{race}(a)$ the reduced trace of a over K.

The map $b_L : L \times L \to K$, $(a, b) \mapsto \overline{\mathrm{t}}\mathrm{race}(ab)$ is a K-linear function and is called the bilinear trace form of L over K. If L is separable over K then, then b_L is a nondegenerate bilinear form. So for the rest of this section, assume L is a separable K-algebra.

Let $\mathcal{O}$ be an R-order in L. Then for every element $\alpha \in \mathcal{O}$, we have $\overline{\mathrm{t}}\mathrm{race}(\alpha) \in R$ ([29] Theorem 10.1). For $n = \dim_K(L)$, we define the discriminant of $\mathcal{O}$ as the R-ideal, $\mathrm{disc}(\mathcal{O}) = \langle\, D \,\rangle$, generated by the set of the non-zero determinants in

$$D = \{\det(M) \mid M = [\,\overline{\mathrm{t}}\mathrm{race}(\alpha_i\alpha_j)\,] \in \mathbb{M}_n(R),\ (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{O}^n\}\backslash\{0\}.$$

Proposition 2.1.2 *For arbitrary R-orders $\mathcal{O}$ and Λ, assume $\mathcal{O} \subseteq \Lambda$. Then* $\mathrm{disc}(\mathcal{O}) \subseteq \mathrm{disc}(\Lambda)$ *and $\mathcal{O} = \Lambda$ if and only if* $\mathrm{disc}(\mathcal{O}) = \mathrm{disc}(\Lambda)$.

Proof See [29] Exercise 10.3 and Exercise 4.13. □

From a generating set for $\mathcal{O}$ over R we can easily obtain a nonzero multiple of $\mathrm{disc}(\mathcal{O})$. Just select a subset of the generating set for $\mathcal{O}$ which is a K-basis for L.

Proposition 2.1.3 *Let $\mathcal{O}$ be an R-order and let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathcal{O}$ be a basis for L over K. Then the principal ideal, dR, generated by the nonzero determinant, $d =$* $\det([\,\overline{\mathrm{t}}\mathrm{race}(\alpha_i\alpha_j)\,])$, *is contained in* $\mathrm{disc}(\mathcal{O})$. *Furthermore let Λ be another R-order in L containing $\mathcal{O}$. Then $d\Lambda \subseteq \langle\, \alpha_1, \alpha_2, \ldots, \alpha_n \,\rangle \subseteq \mathcal{O}$ as R-modules.*

Proof The first part is obvious and the second a version of the argument given in [29] Theorem 10.3. Let $a \in \Lambda$ and put $a = \sum_{i=1}^{t} \lambda_i a_i$ with coefficients $\lambda_i \in K$. Then

$$\overline{\mathrm{t}}\mathrm{race}(aa_j) = \sum_{i=1}^{n} \overline{\mathrm{t}}\mathrm{race}(a_ia_j) \quad \text{for} \quad 1 \leq j \leq n.$$

We have $\overline{\mathrm{t}}\mathrm{race}(aa_j),\ \overline{\mathrm{t}}\mathrm{race}(a_ia_j) \in R$ because aa_j and a_ia_j are in Λ and therefore they are integral over R. If we use Cramer's rule to solve the system of linear equations above for

the λ_i's we obtain that $\lambda_i = d^{-1}\gamma_i$ for some $\gamma_i \in R$ □

Note that if R is a principal ideal domain then every R-order, $\mathcal{O}$, admits an R-basis, say $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\mathrm{disc}(\mathcal{O})$ is the principle ideal in R generated by $d = \det([\,\overline{\mathrm{t}}\mathrm{race}(\alpha_i\alpha_j)\,])$ (see [29] Theorem 10.2).

Localizations

Let R be a Dedekind domain with quotient field K and let L be a semisimple K-algebra. If P is a maximal ideal in R then we consider the localization of R at P:

$$R_{(P)} = \{\frac{a}{b} \,|\, a \in R,\ b \in R\backslash P\} = (R\backslash P)^{-1}R \subset K.$$

$R_{(P)}$ is a discrete valuation ring and we shall represent R-orders as $R_{(P)}$-orders. If $\mathcal{O}$ is an R-order in L then we consider the localization of $\mathcal{O}$ at P

$$\mathcal{O}_{(P)} = \mathcal{O}R_{(P)} = \{\frac{a}{b} \,|\, a \in \mathcal{O},\ b \in R\backslash P\}$$

We say $\mathcal{O}$ is locally maximal at P if $\mathcal{O}_{(P)}$ is a maximal $R_{(P)}$-order. It turns out that $\mathcal{O}$ is maximal if and only if it is locally maximal at every maximal ideal P of R.

If $\mathcal{O}$ is an R-order then $\mathcal{O}_{(P)}$ is an $R_{(P)}$-order, moreover $\mathcal{O}$ is a maximal R-order if and only if $\mathcal{O}_{(P)}$ is a maximal $R_{(P)}$-order for every prime ideal P in R. More generally,

Proposition 2.1.4 *If $\mathcal{O}$ and Λ are R-orders in L such that $\mathcal{O} \subset \Lambda$, then there exists a prime ideal P in R such that $\mathcal{O}_{(P)} \subset \Lambda_{(P)}$.*

Proof See [29] Theorem 3.15. □

The next statement demonstrates a simple but useful connection between the orders $\mathcal{O}$ and $\mathcal{O}_{(P)}$.

Proposition 2.1.5 *Let $\mathcal{O}$ be an R-order in L. The map $\varphi : \mathcal{O} \to \mathcal{O}_{(P)}/P\mathcal{O}_{(P)}$ such that $\alpha \mapsto \alpha + P\mathcal{O}_{(P)}$ induces an isomorphism of rings $\mathcal{O}/P\mathcal{O} \cong \mathcal{O}_{(P)}/P\mathcal{O}_{(P)}$.*

Proof Clearly φ is an epimorphism of rings and it is straightforward to check that $\ker(\varphi) = P\mathcal{O}$. □

To be more specific, if R happens to be a principal ideal domain and π a prime element of R, i.e. the principle ideal $P = \pi R$ is maximal in R. Then we can write

$$R_{(P)} = R_{(\pi)} = \{\tfrac{a}{b} \in K |\ a, b \in R \text{ and } \gcd(\pi, b) = 1\}.$$

where $R_{(\pi)}$ is a discrete valuation ring with unique maximal ideal $PR_{(\pi)} = \pi R_{(\pi)}$. If $\mathcal{O}$ is an R-order then we use the notation $\mathcal{O}_{(P)} = \mathcal{O}_{(\pi)} = R_{(\pi)}\mathcal{O}$

Important examples are when $R = \mathbb{Z}$ and $\pi = \ell$, a rational prime. Then we use the notation $\mathbb{Z}_{(\ell\mathbb{Z})} = \mathbb{Z}_{(\ell)}$ and $\mathcal{O}_{(\ell\mathcal{O})} = \mathcal{O}_{(\ell)}$ respectively.

Orders over extensions

Assume E is a finite separable extension of K and L is a finite dimensional separable E-algebra. Let $\mathcal{O}_E$ be the integral closure of R in E. The next statement will be useful when we change the ring of coefficients from R to $\mathcal{O}_E$.

Lemma 2.1.6 *Let E be a finite separable extension field of K, L a finite dimensional separable E-algebra, $\mathcal{O}$ an R-order in L and let $\mathcal{O}_E$ be the integral closure of R in E. Then the R-order $\Lambda = \mathcal{O}_E\mathcal{O}$ is a $\mathcal{O}_E$-order containing $\mathcal{O}$. As a consequence, if $\mathcal{O}$ is a maximal R-order then $\mathcal{O} \cap E = \mathcal{O}_E$. Morever a maximal R-order in L is a maximal $\mathcal{O}_E$-order as well.*

Proof It is straightforward to check that $\Lambda = \mathcal{O}_E\mathcal{O}$ (the finite sums of the forms $\sum a_i b_i$, $a_i \in \mathcal{O}_E$, $b_i \in \mathcal{O}$) is a ring which is a finitely generated $\mathcal{O}_E$-module. Also we have the identity element of $\mathcal{O}$ in Λ and therefore Λ is indeed a $\mathcal{O}_E$-order. □

We will use the following statement to compute local properties of $\mathcal{O}_E$-orders without explicitly computing $\mathcal{O}_E$.

Lemma 2.1.7 *Let E be a finite separable extension field of K. L a finite dimensional separable algebra over E and let $\mathcal{O}_E$ be the integral closure of R in E. Assume that $\mathcal{O}$ is an R-order in L such that $\mathcal{O}$ is locally maximal at a prime ideal P of R. Then the R-order $\Lambda = \mathcal{O}_E\mathcal{O}$ is an $\mathcal{O}_E$-order and Λ is locally maximal at every prime ideal S in $\mathcal{O}_E$ lying above P. Consider the image of $\mathcal{O} \cap E$ under the natural map $\varphi : \mathcal{O} \to \mathcal{O}/P\mathcal{O}$. The map $S \mapsto \varphi(S \cap \mathcal{O})$ is a bijection between the prime ideals of $\mathcal{O}_E$ and the maximal ideals of $\varphi(E \cap \mathcal{O})$ such that $\Lambda/S\Lambda \cong \Gamma/\varphi(S \cap \mathcal{O})\Gamma$ for $\Gamma = \mathcal{O}/P\mathcal{O}$.*

Proof The local maximality of $\mathcal{O}$ implies $\Lambda_{(P)} = \mathcal{O}_{(P)}$. Set $\Omega = E \cap \mathcal{O}$. Then $\Omega_{(P)} = E \cap \mathcal{O}_{(P)} = E \cap \Lambda_{(P)} = (E \cap \Lambda)_{(P)} = (\mathcal{O}_E)_{(P)}$, i.e. Ω is also locally maximal at P in E. Let $\lambda : \Lambda_{(P)} \to \Lambda/P\Lambda_{(P)}$ be the natural map such that $\alpha \mapsto \alpha + P\Lambda_{(P)}$. By Proposition 2.1.5 the restriction of λ to Λ induces an isomorphism $\Lambda/P\Lambda \cong \Lambda_{(P)}/P\Lambda_{(P)}$.
Similarly the restriction of λ to $\mathcal{O}$ induces an isomorphism $\mathcal{O}/P\mathcal{O} \cong \Lambda_{(P)}/P\Lambda_{(P)}$. In fact, we can identify $\Gamma = \mathcal{O}/P\mathcal{O}$ with $\Lambda_{(P)}/P\Lambda_{(P)}$ and φ with the restriction of λ to $\mathcal{O}$. Using these identification we have $\lambda(\mathcal{O}_E) = \lambda((\mathcal{O}_E)_{(P)}) = \lambda(\Omega_{(P)}) = \lambda(\Omega) = \varphi(E \cap \mathcal{O})$. The kernel of the restriction λ to $(\mathcal{O}_E)_{(P)}$ is equal to $P(\mathcal{O}_E)_{(P)}$. It follows that λ induces a bijection between ideals in $\mathcal{O}_E$ containing $P\mathcal{O}_E$ and the ideals of $\varphi(E \cap \mathcal{O})$. For every maximal ideal S of $\mathcal{O}_E$ above P, we have $\lambda(S\Lambda) = \lambda(S)\lambda(\Lambda) = \lambda(S)\Gamma$, whence λ induces an isomorphism $\Lambda/S\Lambda \cong \Gamma/\varphi(S \cap \mathcal{O})\Gamma$. □

Orders over $\mathbb{Z}$

There are some simple examples of orders. If M is a full R-lattice in L, then the left order of M defined by $\mathrm{O}_{\mathrm{left}}(M) = \{\alpha \in L \mid \alpha M \subseteq M\}$ is an R-order in L ([29] p.109). The right order is defined in a similar way and is denoted $\mathrm{O}_{\mathrm{right}}(M)$. These examples offer an important arithmetic tool for constructing orders.

For the rest of this section assume $R = \mathbb{Z}$ and thus $K = \mathbb{Q}$. The following statement

gives us a tool to reduce the problem of enlarging a $\mathbb{Z}$-order to a similar problem for $\mathbb{Z}_{(\ell)}$-orders.

Lemma 2.1.8 *Let ℓ be a prime element in $\mathbb{Z}$ and Λ a $\mathbb{Z}$-order in L. Suppose that J is an ideal in $\Lambda_{(\ell)}$ such that $\ell\Lambda_{(\ell)} \subseteq J$ and $\Lambda_{(\ell)} \subset \mathrm{O}_{\mathrm{left}}(J)$. Let I denote the inverse image of J with respect to the embedding $\Lambda \to \Lambda_{(\ell)}$. Then we have $\ell\Lambda \subseteq I$, $\Lambda \subset \mathrm{O}_{\mathrm{left}}(I)$ and $\Lambda_{(\ell)} \subset (\mathrm{O}_{\mathrm{left}}(I))_{(\ell)}$.*

Proof Clearly $\ell\Lambda \subseteq I$ and I is an ideal of Λ. Let $\{a_1, a_2, \ldots a_t\}$ be a generating set for I as a $\mathbb{Z}$-module. Then the images of the a_i (which we will also denote by a_i) form a generating set of J as an $\mathbb{Z}_{(\ell)}$-module. Now let $a \in \mathrm{O}_{\mathrm{left}}(J)\backslash\Lambda_{(\ell)}$. Then for $i = 1, \ldots, t$ we have $aa_i = \sum_{j=1}^{t} \frac{c_{ij}}{d_{ij}} \cdot a_j$ where $c_{ij},\ d_{ij} \in \mathbb{Z}$ and ℓ does not divide d_{ij}. Now put $d = \prod_{i,j=1}^{t} d_{ij}$. It is straightforward to check that $daI \subseteq I$ and consequently $da \in \mathrm{O}_{\mathrm{left}}(I)$. Finally we observe that $da \notin \Lambda_{(\ell)}$, for otherwise we would have that $a \in \Lambda_{(\ell)}$. □

Radicals of orders over local rings

Let R denote an arbitrary ring with an identity element. $\mathrm{Rad}(R)$, the Jacobson radical of R, is the set of elements $\alpha \in R$ such that $\alpha M = 0_R$ for all simple left (or equivalently simple right) R-modules M. $\mathrm{Rad}(R)$ is a two-sided ideal in R containing every nilpotent one-sided ideal of R. Furthermore $\mathrm{Rad}(R)$ can be characterized as the intersection of the maximal right ideals in R. If R is left or right artinian (this holds for example if R is a finite dimensional algebra with identity over a field) then $\mathrm{Rad}(R)$ is the maximal nilpotent ideal in R.

Assume that R is a discrete valuation ring, P its unique non-zero prime ideal and K its field of quotients. Let $\mathcal{O}$ be an R-order in a finite dimensional semisimple K-algebra L.

Proposition 2.1.9 *The residue class ring $\overline{\mathcal{O}} = \mathcal{O}/P\mathcal{O}$ is an algebra with identity over the residue class field $\overline{R} = R/P$ and $\dim_K(L) = \dim_{\overline{R}}(\overline{\mathcal{O}})$. If $\varphi :\ \mathcal{O} \to \overline{\mathcal{O}}$ is the canonical epimorphism, then $P\mathcal{O} \subseteq \mathrm{Rad}(\mathcal{O}) = \varphi^{-1}(\mathrm{Rad}(\overline{\mathcal{O}}))$ and φ induces a ring isomorphism $\mathcal{O}/\mathrm{Rad}(\mathcal{O}) \cong \overline{\mathcal{O}}/\mathrm{Rad}(\overline{\mathcal{O}})$. As a consequence, a left (or right) ideal I of $\mathcal{O}$ is contained in $\mathrm{Rad}(\mathcal{O})$ if and only if I is nilpotent modulo $P\mathcal{O}$. For example there exists a positive integer $r > 0$ such that $I^r \subseteq P\mathcal{O}$.*

Proof See [29] Theorem 6.15. The claim about the dimensions follows directly from the fact that R is a principal ideal ring and $\mathcal{O}$ is a free R-module. As for the "only if" part of the last statement, every nilpotent ideal of $\overline{\mathcal{O}}$ is contained in $\mathrm{Rad}(\overline{\mathcal{O}})$. □

Proposition 2.1.10 *If $\mathcal{O} \subseteq \Lambda$ are R-orders, then there exists a positive integer r such that $\mathrm{Rad}(\Lambda)^r \subseteq \mathcal{O}$. For any such r, $\mathrm{Rad}(\Lambda)^r \subseteq \mathrm{Rad}(\mathcal{O})$ is an ideal in $\mathcal{O}$.*

Proof See [29] Hint to Exercise 39.3. This is proved using the fact that $\mathcal{O} \subseteq \Lambda$ are full R-modules in L over a discrete valuation ring R. From Proposition 2.1.9 we infer that there exists positive integers u and t such that $P^u\Lambda \subseteq \mathcal{O}$ and $\mathrm{Rad}(\Lambda)^t \subseteq P\Lambda$. Now $r = tu$ will

suffice to prove the first claim. If for some r we have $I = \mathrm{Rad}(\Lambda)^r \subseteq \mathcal{O}$, then I is an ideal in $\mathcal{O}$ because $\mathcal{O}I \subseteq \Lambda I = I$ and $I\mathcal{O} \subseteq I\Lambda = I$. Finally for integers t and u we have

$$I^{t(u+1)} = \mathrm{Rad}(\Lambda)^{rt(u+1)} \subseteq (P\Lambda)^{r(u+1)} \subseteq (P\Lambda)^{(u+1)} = P^{u+1}\Lambda = PP^u\Lambda \subseteq P\mathcal{O}$$

and Proposition 2.1.9 implies that $I \subseteq \mathrm{Rad}(\mathcal{O})$. □

The following observation plays an important role in Jacobinski's approach to hereditary orders.

Proposition 2.1.11 *Let $\mathcal{O} \subseteq \Lambda$ be R-orders in L such that $\mathrm{Rad}(\Lambda) \subseteq \mathcal{O}$. Then for any order Ω such that $\mathcal{O} \subseteq \Omega \subseteq \Lambda$ then we have $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\Omega)$. The canonical map $\varphi : \Lambda \to \overline{\Lambda} = \Lambda/\mathrm{Rad}(\Lambda)$ induces a bijection $\Omega \to \Omega/\mathrm{Rad}(\Lambda)$ between the set of orders Ω lying between $\mathcal{O}$ and Λ and the set of subalgebras of the R/P-algebra $\overline{\Lambda}$ containing $\mathcal{O}/\mathrm{Rad}(\Lambda)$. Moreover $\mathcal{O} \subseteq \Omega \subseteq \Lambda$ implies $\mathrm{Rad}(\Omega) = \varphi^{-1}(\mathrm{Rad}(\varphi(\Omega)))$.*

Proof We have $\mathrm{Rad}(\Lambda) \subseteq \mathcal{O} \subseteq \Omega$. From this Proposition 2.1.10 implies that $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\Omega)$. The statement about the correspondence of R-orders and R/P-subalgebras is obvious once we observe that any R-subalgebra Ω such that $\mathcal{O} \subseteq \Omega \subseteq \Lambda$ is actually an R-order. As for the last statement, we note if J is a maximal left ideal of Ω then $\mathrm{Rad}(\Lambda) \subseteq J$ because $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\Omega)$. We infer that φ induces a bijection between the set of maximal left ideals of Ω and the set of maximal left ideals of $\Omega/\mathrm{Rad}(\Lambda)$ and the statement follows.□

Extremal orders

In this section R is a discrete valuation ring. For R-orders in L we introduce the following partial ordering: Λ radically contains $\mathcal{O}$ if and only if $\mathcal{O} \subseteq \Lambda$ and $\mathrm{Rad}(\mathcal{O}) \subseteq \mathrm{Rad}(\Lambda)$. The R-orders maximal with respect to this partial ordering are called extremal. Maximal orders are oviously extremal. We note that if $\mathcal{O}$ is an R-order then $P\mathcal{O} \subseteq \mathrm{Rad}(\mathcal{O})$ so that $\mathrm{Rad}(\mathcal{O})$ is a full R-lattice. Therefore $\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$ is an R-order.

Proposition 2.1.12 *For any R-order, $\mathcal{O}$ in L, the order $\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$ radically contains $\mathcal{O}$. Moreover $\mathcal{O}$ is extremal if and only if $\mathcal{O} = \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$. Equivalently $\mathcal{O}$ is extremal if and only if $\mathcal{O} = \mathrm{O}_{\mathrm{right}}(\mathrm{Rad}(\mathcal{O}))$.*

Proof Since $\mathrm{Rad}(\mathcal{O})$ is an ideal in $\mathcal{O}$, $\mathcal{O} \subseteq \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$. Also, $\mathrm{Rad}(\mathcal{O})$ is a left ideal in $\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$ and by Proposition 2.1.9 for some $r > 0$ we have $\mathrm{Rad}(\mathcal{O})^r \subseteq P\mathcal{O} \subseteq P\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$. Hence $\mathrm{Rad}(\mathcal{O}) \subseteq \mathrm{Rad}(\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O})))$. This implies that $\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$ radically contains $\mathcal{O}$. We infer that is $\mathcal{O}$ is extremal then $\mathcal{O} = \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$.
In the other direction we suppose that $\mathcal{O} = \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}))$ and Λ is an order radically containing $\mathcal{O}$. By Proposition 2.1.10 there exists an integer $r > 0$ such that $\mathrm{Rad}(\Lambda)^r \subseteq \mathrm{Rad}(\mathcal{O})$. For any $r > 1$ with this property we have $\mathrm{Rad}(\Lambda)^{r-1}\mathrm{Rad}(\mathcal{O}) \subseteq \mathrm{Rad}(\Lambda)^{r-1}\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{O})$ implying that $\mathrm{Rad}(\Lambda)^{r-1} \subseteq \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O})) = \mathcal{O}$. Proposition 2.1.10 implies that $\mathrm{Rad}(\Lambda)^{r-1} \subseteq \mathrm{Rad}(\mathcal{O})$. Continuing this way we obtain $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{O})$ and consequently $\mathrm{Rad}(\Lambda) = \mathrm{Rad}(\mathcal{O})$. We conclude that $\Lambda \subseteq \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\Lambda)) = \mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O})) = \mathcal{O}$ and $\Lambda = \mathcal{O}$.
□

Proposition 2.1.13 *Assume that $\mathcal{O} \subseteq \Lambda$ are R-orders in L. Then $\mathcal{O} + \mathrm{Rad}(\Lambda)$ is an R-order in L radically containing $\mathcal{O}$.*

Proof It is straightforward to verify that $\Omega = \mathcal{O} + \mathrm{Rad}(\Lambda)$ is an R-order in L containing $\mathcal{O}$. Next, using the characterization of radical ideals in Proposition 2.1.9, we obtain that $\mathrm{Rad}(\mathcal{O}) + \mathrm{Rad}(\Lambda)$ is an ideal of Ω and $\mathrm{Rad}(\mathcal{O}) + \mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\Omega)$. □

Proposition 2.1.14 *Let $\mathcal{O} \subseteq \Lambda$ be R-orders in L and suppose that $\mathcal{O}$ is extremal.Then* $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{O})$.

Proof An immediate consequence of Proposition 2.1.13 and Proposition 2.1.10. □

We remark that if $\mathcal{O}$ is an R-order in L such that $\mathrm{Rad}(\mathcal{O}) = P\mathcal{O} = \pi\mathcal{O}$. Then $\mathcal{O}$ is a maximal order. Indeed, $\mathrm{O}_{\mathrm{left}}(\pi\mathcal{O}) = \mathrm{O}_{\mathrm{left}}(\mathcal{O}) = \mathcal{O}$, hence $\mathcal{O}$ is extremal by Proposition 2.1.12. If $\mathcal{O} \subseteq \Lambda$, then by Proposition 2.1.14 we have $\pi\Lambda \subseteq \mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{O}) = \pi\mathcal{O}$ implying that $\pi\Lambda = \pi\mathcal{O}$ and $\Lambda = \mathcal{O}$.

Lemma 2.1.15 *Let L be a finite dimensional semisimple algebra over a field K. Let L^+ be a maximal subalgebra of L such that* $\mathrm{Rad}(L^+) \neq 0$. *Then there exists a two-sided ideal J of L^+ minimal among those containing* $\mathrm{Rad}(L^+)$ *which is also a left ideal of L.*

Proof First we reduce the statement to the special case when L is simple. In general by Wedderburn's theorem (Theorem 2.1.1) we have $L = L_2 \oplus L_2 \oplus \ldots \oplus L_r$ where the direct summands L_i are simple algebras. We observe first that L^+ contains the centre of L. Indeed for the algebra F generated by L^+ and centre(L) we have $L^+ \subseteq F$. Also it is straightforward to verify that an element $0 \neq c \in \mathrm{Rad}(L^+)$ generates a nilpotent left ideal in F as well, therefore $\mathrm{Rad}(F) \neq 0$. This implies that $F \subset L$ and it follows that $F = L^+$ and centre$(L) \subseteq L^+$. We infer that L^+ contains the identity element $e_i \in L_i$ of the ideals L_i and consequently we have $L^+ = e_1L^+ \oplus e_2L^+ \oplus \ldots \oplus e_rL^+$. Now the maximality of L^+ implies the existence of an index i, such that e_iL^+ is a maximal subalgebra of the simple algebra L_i and $e_jL^+ = L_j$ if $i \neq j$. Clearly we have $\mathrm{Rad}(e_iL^+) = \mathrm{Rad}(L^+) \neq 0$. Now a two-sided ideal J_i of e_iL^+ minimal among those containing $\mathrm{Rad}(e_iL^+)$ which is a left ideal of L_i will clearly suffice as J.
For the rest of the proof we assume L is a simple algebra. Let M be a simple left L-module and let D stand for the algebra of L-endomorphisms of M. By Schur's lemma D is a division algebra over the field K and M is a right D-space. Moreover we have $L = \mathrm{End}_D(M)$ and hence $\mathrm{Rad}(L^+)M \neq 0$. We define the strictly decreasing chain of D-subspaces $M = M_0 \supset M_1 \supset M_2$ by $M_{i+1} = \mathrm{Rad}(L^+)M_i$ for $i = 0, 1$. For this chain of subspaces we obtain a decreasing chain of subalgebras $L = L_0 \supseteq L_1 \supseteq L_2$ by letting $L_i = \{\alpha \in L |\ \alpha M_j \subseteq M_j \text{ for } j = 0, \ldots, i\}$. Here $L \neq L_1$ follows from $L = \mathrm{End}_D(M)$. Moreover, $L^+ \subseteq L_2$ implies that $L_1 = L_2 = L^+$. We infer that $M_2 = 0$ and $(\mathrm{Rad}(L^+))^2 = 0$. Then the annihilator $J = \{\alpha \in L \mid \alpha M_1 = 0\}$ is properly contained in $L_1 = L^+$ and in fact is a two-sided ideal of L^+. It is also obvious that J is a left ideal of L and this implies that $\mathrm{Rad}(L^+) \subset J$. From $L = \mathrm{End}_D(M)$ we obtain that $L^+/\mathrm{Rad}(L^+) \cong \mathrm{End}_D(M_1) \oplus \mathrm{End}_D(M)/M_1$. Thus $L^+/\mathrm{Rad}(L^+)$ is a semisimple algebra with exactly two minimal ideals, implying the minimality of J over $\mathrm{Rad}(L^+)$. □

Theorem 2.1.16 *Let $\mathcal{O} \subset \Lambda$ be R-orders in L. Suppose $\mathcal{O}$ is extremal and Λ is minimal among the R-orders properly containing $\mathcal{O}$. Then there exists an ideal I of $\mathcal{O}$, minimal among those containing* $\mathrm{Rad}(\mathcal{O})$ *such that $\Lambda \subseteq \mathrm{O}_{\mathrm{left}}(I)$.*

Proof By Proposition 2.1.14 and 2.1.11 we have that $\Omega = \mathcal{O}/\mathrm{Rad}(\Lambda)$ is a maximal proper subalgebra of the semisimple $F = R/P$-algebra $\Gamma = \Lambda/\mathrm{Rad}(\Lambda)$. Moreover $\mathrm{Rad}(\Omega) \neq 0$ since $\mathcal{O} \subset \Lambda$ and $\mathcal{O}$ is extremal. We can apply Lemma 2.1.15. There exists a minimal ideal J of Ω above $\mathrm{Rad}(\Omega)$ such that J is a left ideal in Γ. Now I, the inverse image with respect to the natural map $\Lambda \to \Gamma$ clearly satisfies the requirements of the theorem. □

Maximal orders

For this section assume $R = \mathbb{Z}$ with quotient field $K = \mathbb{Q}$.

Proposition 2.1.17 *If M is a full $\mathbb{Z}$-lattice in the $\mathbb{Q}$-algebra L given by a $\mathbb{Z}$-basis then $\mathrm{O}_{\mathrm{left}}(M)$ has a $\mathbb{Z}$-basis.*

Proof Let $b_1, \ldots, b_m$ be a given $\mathbb{Z}$-basis for M. Since $M \otimes \mathbb{Q} = L$, we can express the identity element $e \in L$ in L as a $\mathbb{Q}$-linear combination of the b_i's. Computing a common denominator leads to finding $r \in \mathbb{Z}$ such that $re \in M$. For such an r we have $\mathrm{O}_{\mathrm{left}}(M) = \{\alpha \in r^{-1}M \,|\, \alpha M \subseteq M\}$. Finding an $\mathbb{Z}$-basis of $\mathrm{O}_{\mathrm{left}}(M)$ in terms of $r^{-1}b_1, r^{-1}b_2, \ldots, r^{-1}b_m$ is equivalent to computing an $\mathbb{Z}$-basis of the $\mathbb{Z}$-integral solutions of a system of linear equations. □

The next statement provides a bound on the number of iterations in algorithms which successively increase orders until a maximal order is obtained.

Proposition 2.1.18 *Assume that we have the strictly increasing chain $\mathcal{O}_0 \subset \mathcal{O}_2 \subset \ldots \subset \mathcal{O}_m$ of $\mathbb{Z}$-orders in L. Let $d_i \in \mathbb{Z}$ be a generator of the ideal* $\mathrm{disc}(\mathcal{O}_i)$ *for $i = 0, \ldots, m$. Let $|d_i|$ denote the usual absolute value of the integer d_i. Then $m \leq \frac{1}{2}\log_2(|\frac{d_0}{d_m}|) \leq \frac{1}{2}\log_2(|d_0|)$.*

Proof For each $i = 0, \ldots, m-1, |\frac{d_i}{d_{i+1}}| > 1$ we have it as a square of an integer, $|\det(T_i)|^2$ where T_i is the linear transformation matrix transforming an $\mathbb{Z}$-basis for $\mathcal{O}_{i+1}$ into a $\mathbb{Z}$-basis for $\mathcal{O}_i$. We obtain the statement by taking logarithm of

$$\left|\frac{d_0}{d_m}\right| = \prod_{i=0}^{m} \left|\frac{d_i}{d_{i+1}}\right| \geq 2^{2m}.$$

□

For the remainder of the section assume that K is a finite extension of $\mathbb{Q}$ and L a finite dimensional separable K-algebra, and $\mathcal{O}$ an $\mathbb{Z}$-order in L. Let $\mathcal{O}_K$ stand for the integral closure of $\mathbb{Z}$ in K. Suppose L is given by structure constants over K and $\mathcal{O}$ is given by a $\mathbb{Z}$-basis. Suppose further that we are given a prime element $\ell \in \mathbb{Z}$.

Theorem 2.1.19 *There exists a $\mathbb{Z}$-order Λ such that $\mathcal{O} \subset \Lambda$ and $\mathcal{O}_{(\ell)} \subset \Lambda_{(\ell)}$ provided $\mathcal{O}$ is not maximal at ℓ.*

Proof We shall test first whether $\mathcal{O}_{(\ell)}$ is an extremal $\mathbb{Z}_{(\ell)}$-order by checking if $\mathrm{O}_{\mathrm{left}}(\mathrm{Rad}(\mathcal{O}_{(\ell)})) = \mathcal{O}_{(\ell)}$. If not, then we construct an $\mathbb{Z}$-order, Λ, such that $\mathcal{O} \subset \Lambda$ and $\mathcal{O}_{(\ell)} \subset \Lambda_{(\ell)}$. If $\mathcal{O}_{(\ell)}$ passes the test then we use the following test based on Theorem 2.1.16. If there exists an ideal J minimal among the ideals properly containing $\mathrm{Rad}(\mathcal{O}_{(\ell)})$ such that $\mathcal{O}_{(\ell)} \subset \mathrm{O}_{\mathrm{left}}(J)$ then we construct a $\mathbb{Z}$-order Λ such that $\mathcal{O} \subset \Lambda$ and $\mathcal{O}_{(\ell)} \subset \Lambda_{(\ell)}$ otherwise we correctly conclude that $\mathcal{O}$ is maximal at ℓ.
As for the first test, we compute the inverse image $I \subseteq \mathcal{O}$ of $\mathrm{Rad}(\mathcal{O}_{(\ell)})$ with respect to the embedding $\mathcal{O} \to \mathcal{O}_{(\ell)}$. By Lemma 2.1.8 $\mathcal{O}$ passes the first test if and only if $\mathrm{O}_{\mathrm{left}}(I) = \mathcal{O}$. Otherwise $\Lambda = \mathrm{O}_{\mathrm{left}}(I)$ is an order containing $\mathcal{O}$ such that $\mathcal{O}_{(\ell)} \subset \Lambda_{(\ell)}$.
We shall work with the finite algebra $\Gamma = \mathcal{O}/\ell\mathcal{O}$ over the finite field $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. From Propositions 2.1.9 and 2.1.5 we infer that I is the inverse image of $\mathrm{Rad}(\Gamma)$ with respect to the canonial map $\mathcal{O} \to \Gamma$. From a $\mathbb{F}_\ell$-basis of $\mathrm{Rad}(\Gamma)$ we can efficiently find an $\mathbb{Z}$-basis of I. Observe that any $\mathbb{Z}$-submodule M, such that $\ell\mathcal{O} \subseteq M \subseteq \mathcal{O}$, has a basis of finite size and by Proposition 2.1.17 we compute $\mathrm{O}_{\mathrm{left}}(I)$ efficiently. This finishes the desciption of the first test.
The second test can be treated in a similar way. Let $J_1, J_2, \ldots, J_m$ denote the minimal ideals of Γ which contains $\mathrm{Rad}(\Gamma)$. Note that these ideals are the inverse images, with respect to the canonical map $\varphi : \Gamma \to \Gamma/\mathrm{Rad}(\Gamma)$ of the minimal ideals of the semisimple algebra $\Gamma/\mathrm{Rad}(\Gamma)$. We have $m \leq n$. Let I_i denote the inverse image in $\mathcal{O}$ of J_i with respect to the map $\mathcal{O} \to \Gamma$. Propositions 2.1.5 and 2.1.9 imply that $I_1, \ldots, I_m$ are also the inverse images of the minimal ideals of $\Lambda_{(\ell)}$ over $\mathrm{Rad}(\Lambda_{(\ell)})$. As in the first case we obtain that we have to compute the rings $\mathrm{O}_{\mathrm{left}}(I_i)$ for $i = 0, \ldots, m$ from the ideals J_i and I_i. We can stop when $\mathcal{O} \subset \mathrm{O}_{\mathrm{left}}(I_i)$ is detected because then we have an order properly containing $\mathcal{O}$. □

Theorem 2.1.20 *Let L be a finite dimensional algebra over $\mathbb{Q}$ (given by its structure contants). Then we can construct a maximal $\mathbb{Z}$-order by means of constructing a $\mathbb{Z}$-basis.*

Proof With the methods of Theorem 2.1.19 we can construct a maximal $\mathbb{Z}$-order in L as follows. First we need a starting $\mathbb{Z}$-order. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the input basis for L over $\mathbb{Q}$. Let d be the lowest common denominator of the structure constants with respect to the basis. The $\mathbb{Z}$-module $\mathcal{O}$ generated by $\{1, d\alpha_1, d\alpha_2, \ldots, d\alpha_n\}$ is an $\mathbb{Z}$-order in L. We put $t = \det([\,\overline{\mathrm{t}}\mathrm{race}_{L/\mathbb{Q}}(d^2\alpha_i\alpha_j)\,])$. Note that the elements $\overline{\mathrm{t}}\mathrm{race}_{L/\mathbb{Q}}(\alpha_i\alpha_j)$ can be computed if we know the Wedderburn decomposition of L over $\mathbb{Q}$. Now t is a multiple of the $\mathrm{disc}(\mathcal{O})$, whence, by Proposition 2.1.3, $\mathcal{O}$ is maximal at every prime ℓ not dividing t. Let N be the set of primes in $\mathbb{Z}$ dividing t. N is obtained by factoring t in $\mathbb{Z}$. Repeated application of Theorem 2.1.19 gives us a sequence of $\mathbb{Z}$-orders $\mathcal{O} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_m$ until a maximal $\mathbb{Z}$-order is obtained. By Proposition 2.1.18 we have the bound $m \leq \frac{1}{2}\log_2(|t|)$ and we can control sizes during the iteration. By Proposition 2.1.3 we have $\mathcal{O} \subseteq \Lambda_j \subseteq \frac{1}{t}\mathcal{O}$, therefore Λ_j can be represented by an $\mathbb{Z}$-basis admitting a short description. □

Corollary 2.1.21 *Let K be a finite extension of $\mathbb{Q}$ and L a finite dimensional central simple K-algebra (given by structure constants over K). Let $\mathcal{O}_K$ denote the integral closure of $\mathbb{Z}$ in K. Then we can construct a maximal $\mathcal{O}_K$-order by means of constructing a $\mathbb{Z}$-basis.*

Proof From our knowledge of the rationals and the structure constants of L over K we can readily obtain structure constants of L over $\mathbb{Q}$. With the method of Theorem 2.1.20 we compute a $\mathbb{Z}$-basis of a maximal $\mathbb{Z}$-order $\mathcal{O}_L$ of L. By Lemma 2.1.6 we conclude that $\mathcal{O}_L$ is a maximal $\mathcal{O}_K$-order as well. □

2.1.3 Computing indices

Let R be a Dedekind domain with field of fractions K and let L be a central simple K-algebra of dimension n^2. Orders are often used for reducing computation in L modulo certain ideals, I of R (computing in the ring $\mathcal{O}/I\mathcal{O}$). In particular, if P is a maximal ideal in R and $\mathcal{O}$ a maximal R-order of L, then the structural invariants of the R/P-algebra $\mathcal{O}/P\mathcal{O}$ do not depend on the choice of $\mathcal{O}$. These invariants are called local invariants of L at P.

If K is a number field (a finite extension field of $\mathbb{Q}$) and R is the ring of algebraic integers in K then the local invariants at the prime ideals of R together with other invariants corresponding to embeddings of K into $\mathbb{C}$ determine the structure of L up to isomorphism. This fairly nontrivial fact has a beautiful unified formulation in terms of valuations and completions. Phenomena of this flavour, for example, the possibility to ascertain a global property from local ones, are often referred to as Hasse's principle for the particular property.

We first recall some standard material related to valuations and completions ([29] Section 5).

By a prime P in a number field we understand an equivalence class of nontrivial valuations. P is either finite (if it can be identified with a prime ideal of the ring of integers of K) or infinite (real if it can be identified with an embedding $K \to \mathbb{R}$ and complex if it can be identified with a pair of conjugate embeddings $K \to \mathbb{C}$). A local field is a field that is locally compact with respect to a nontrivial valuation. Local fields of characteristic zero are either archimedean ($\mathbb{R}$ or $\mathbb{C}$) or nonarchimedean (for example a finite extension of $\mathbb{Q}_\ell$ for some rational prime ℓ).

Let ν be a valuation corresponding to the prime P in K. We consider the completions K_P and $L_P = K_P \otimes_K L$ respectively. It is easy to see that L_P is a central simple K_P-algebra of dimension n^2. Therefore the index of L_P is m_P, for some m_P dividing n. (i.e $t = nm_P^{-1}$, and $L_P \cong \mathbb{M}_t(D)$ where D is a central skew field over K_P.) We call the index m_P the local index of L at P.

Since for every central simple K-algebra L we have $\mathbb{M}_t(L)_P = \mathbb{M}_t(L_P)$, the local index m_P is in fact a divisor of the index $[L_P : K_P]$.

Denote by $\mathrm{Br}(K)$ the set of isomorphism classes of central division algebras over K. If A and B are central division algebras over K, then $A \otimes_K B \cong \mathbb{M}_t(L)$ for some central division algebra L over K. We define a product on $\mathrm{Br}(K)$ by setting $[A]\cdot[B] = [L]$. This makes $\mathrm{Br}(K)$ into a commutative group (called the Brauer group of K), with identity element $[K]$. See [8].

For a local field K with maximal ideal P there is a canonical embedding

$$\mathrm{inv}_P : \ \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

If K is nonarchimedean, then inv_P is a isomorphism. If $K = \mathbb{R}$ then the image is $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and $\mathrm{Br}(\mathbb{C}) = 0$. (See [27] p.109.)

For any number field K and central division algebra, L over K, we have an exact sequence:

$$\begin{array}{ccccccc} 0 & \to & \mathrm{Br}(K) & \to & \bigoplus_P \mathrm{Br}(K_P) \to & \mathbb{Q}/\mathbb{Z} & \to 0 \\ & & [L] & \mapsto & ([L \otimes_K L_P]) & & \\ & & & & (a_P) \quad \mapsto & \sum_P \mathrm{inv}_P(a_P) & \end{array}$$

where P ranges over all primes of K. (See [27] p.198)

This says that a central division algebra, L over K, is uniquely determined up to isomorphism by its invariants $\mathrm{inv}_P([L \otimes_L L_P])$.

In K is a number field and P a prime in K corresponding to ν (a non-archimedean valuation of K) then

$$R_P = \{\alpha \in K^* \mid \nu(\alpha) \leq 1\}$$

is a subring of K, called the valuation ring of ν. $M_P = \{\alpha \in K^* \mid \nu(\alpha) < 1\}$ is the unique maximal ideal in R_P, called the valuation ideal.

Further if ν is a discrete valuation, then R_P is a discrete valuation ring (for example the only prime ideal of R_P is M_P). If R is contained in a valuation ring for some valuation ν in K, for example $\nu(\alpha) \leq 1\ \forall \alpha \in R$, then $P = \{\alpha \in R \mid \nu(\alpha) < 1\}$ is a maximal ideal in R and ν is equivalent to the usual P-adic valuation of K. We say in this case that ν corresponds to the prime ideal P of R.

The following statement, based on the classification of division algebras over local fields ([29] Chapter 3) and the theory of maximal orders over discrete valuation rings ([29] Chapter 5), relates the local index m_P of L at P to the structure of the maximal R_P-orders in L.

Proposition 2.1.22 *Let ν be a discrete valuation corresponding to the prime P in K such that the residue class field R_P/M_P is finite (this holds for every nonarchimedean valuation of K) and let $\mathcal{O}$ be a maximal R_P-order in L_P, a central simple K_P-algebra of dimension n^2. The radical $\mathrm{Rad}(\mathcal{O})$ is the unique maximal two-sided ideal in $\mathcal{O}$, $M_P\mathcal{O} = (\mathrm{Rad}(\mathcal{O}))^{m_P}$ and $\mathcal{O}/\mathrm{Rad}(\mathcal{O}) \cong \mathbb{M}_t(E)$ where E is a field extension of R_P/M_P of degree m_P and $t = nm_P^{-1}$.*

Proof Let Γ_P be the valuation ring of the valuation, ν, of the field K_P and let M_P be the maximal ideal of Γ_P. Let $\Omega = \Gamma_P \otimes_{R_P} \mathcal{O}$, then Ω is a maximal Γ_P-order in L_P (see [29] Theorem 11.5) and $\mathrm{Rad}(\mathcal{O}) = \mathcal{O} \cap \mathrm{Rad}(\Omega)$ (see [29] Theorem 18.7), whence $\mathcal{O}/\mathrm{Rad}(\mathcal{O}) \cong \Omega/\mathrm{Rad}(\Omega)$. By [29] Theorem 17.3, Ω is congruent by the inner automorphism of L_P to the order $\mathbb{M}_t(\Lambda)$ where $L_P \cong \mathbb{M}_t(D)$, D a central skew field over L_P of index m_P and Λ is the unique maximal Γ_P-order in D. We have $\mathrm{Rad}(\mathcal{O})/\mathrm{Rad}(\mathcal{O}) \cong \Omega/\mathrm{Rad}(\Omega) \cong \mathbb{M}_t(\Lambda/\mathrm{Rad}(\Lambda))$. $E = \Lambda/\mathrm{Rad}(\Lambda)$ is an extension field of degree m_P of $\Gamma_P/M_P \cong R_P/M_P$ and $\mathrm{Rad}(\Lambda)^{m_P} = M_P\Lambda$ (see [29] Theorem 14.3). If we identify Ω with $\mathbb{M}_t(\Lambda)$, we have $\mathrm{Rad}(\Omega) = \mathbb{M}_t(\mathrm{Rad}(\Lambda))$ and $M_P\Omega = \mathbb{M}_t(M_P\Lambda) = \mathbb{M}_t(\mathrm{Rad}(\Lambda)^{m_P}) = \mathbb{M}_t(\mathrm{Rad}(\Lambda))^{m_P} = \mathrm{Rad}(\Omega)^{m_P}$. It follows that $M_P\mathcal{O} = \mathcal{O} \cap M_P\Omega = \mathcal{O} \cap \mathrm{Rad}(\Omega)^{m_P} = (\mathcal{O} \cap \mathrm{Rad}(\Omega))^{m_P} = \mathrm{Rad}(\mathcal{O})^{m_P}$. □

For now on assume $R = \mathbb{Z}$ with quotientfield $K = \mathbb{Q}$ and let L be a separable $\mathbb{Q}$-algebra. We next give a method to compute local indices of simple separable algebras over number fields.

Assume that the centre of L is a finite separable extension of $\mathbb{Q}$ and let $\mathcal{O}_L$ be the integral closure of $\mathbb{Z}$ in L. The following simple statement tells us that we do not have to care about the indices at primes not dividing the discriminant of an $\mathbb{Z}$-order in L.

Proposition 2.1.23 *Let L be a central simple algebra over K, a finite separable extension of $\mathbb{Q}$. Let $\mathcal{O}_L$ be the integral closure of $\mathbb{Z}$ in L and let $\mathcal{O}$ be an $\mathbb{Z}$-order in L. Assume that for some prime P in $\mathcal{O}_L$ above the prime ℓ in $\mathbb{Z}$ we have $m_P > 1$. Then ℓ divides the discriminant of $\mathcal{O}$.*

Proof Assume ℓ does not divide the discriminant of $\mathcal{O}$. The $\mathbb{Z}/\ell\mathbb{Z}$-algebra $\mathcal{O}/\ell\mathcal{O}$ has a nonsingular bilinear trace form, whence is semisimple. Therefore its factor $\mathcal{O}/P\mathcal{O} \cong \mathcal{O}_{(P)}/P\mathcal{O}_{(P)}$ is also semisimple implying that $\mathrm{Rad}(\mathcal{O})_{(P)} = P\mathcal{O}_{(P)}$. On the other hand, by Proposition 2.1.22 we have $P\mathcal{O}_{(P)} = (\mathrm{Rad}(\mathcal{O})_{(P)})^{m_P}$, giving $m_P = 1$. □

Theorem 2.1.24 *The L be a central simple $\mathbb{Q}$-algebra of dimension n^2 and $\mathcal{O}$ a maximal $\mathbb{Z}$-order in L. Then*

$$\mathrm{disc}(\mathcal{O}) = \prod_P P^{nm_P^{-1}[L:\mathbb{Q}]^{\frac{1}{2}}}$$

where P ranges over all prime ideals in $\mathbb{Z}$.

Proof [29] Theorem 32.1 □

The above statement gives the exact formula for the factorization of the discriminant of a maximal order. This makes it possible to compute local indices from the discriminant of a maximal order. Note that we can instead use a method based on the structure of the factor of a locally maximal order by the radical.

Pectora roborant cultus recti

Proposition 2.1.25 *Given a finite separable extension K of $\mathbb{Q}$, a central simple K-algebra, L, and a prime ℓ in $\mathbb{Z}$. Then we can compute the set of local indices of L at primes in $\mathcal{O}_K$ above ℓ.*

Proof With the algorithm described in the proof of Theorem 2.1.19 we first compute an $\mathbb{Z}$-order, $\mathcal{O}$ in L, which is locally maximal at ℓ. Consider the factor ring $\Gamma = \mathcal{O}/\ell\mathcal{O}$ which is a finite dimensional algebra over the finite field $\mathbb{Z}/\ell\mathbb{Z}$. We compute the the image of $\mathcal{O} \cap K$ by the natural map $\varphi : \mathcal{O} \to \Gamma$, that is the subalgebra $\Omega = \varphi(\mathcal{O} \cap K) = (\mathcal{O} \cap K)/(\ell\mathcal{O} \cap K))$. We compute $\mathrm{Rad}(\Omega)$ and decompose $\Omega/\mathrm{Rad}(\Omega)$ to find the maximal ideals of Ω.
By Lemma 2.1.7 these ideals correspond to prime ideals of $\mathcal{O}_K$ lying over ℓ. For every such ideal M (corresponding to the $\mathcal{O}_K$-ideal P) we compute the factor ring $\Gamma/M\Gamma$. By Lemma 2.1.7 this ring is isomorphic to $\Lambda/P\Lambda$ where $\Lambda = \mathcal{O}_K\mathcal{O}$. By Proposition 2.1.22 the radical-free part of $\Lambda_{(P)}/P\Lambda_{(P)} \cong \Lambda/P\Lambda$ is a full matrix algebra over an extension of degree m_P of $\mathcal{O}_K/P$ Therefore by Lemma 2.1.7 the index m_P can be obtained as the dimension of the centre of the radical-free part of $\Gamma/M\Gamma$ over the field Ω/M. □

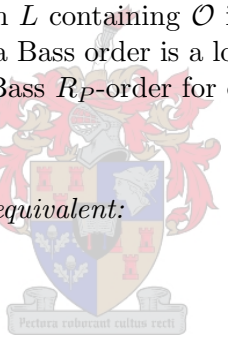
The last three statements suggest a method to compute the set of all local indices for valuations corresponding to prime ideals P in $\mathcal{O}_K$ based on factoring the discriminant of the starting order. Note that we do not need to compute the order $\mathcal{O}_K$.

Theorem 2.1.26 *If L is a central simple algebra over a number field K, then the index of L is the least common multiple of the elements in the set $\{m_P \mid P \text{ is a prime of } K\}$.*

Proof We show how to compute the local indices for valuations not corresponding to primes in $\mathbb{Z}$. Suppose P corresponds to an archimedean valuation such that the completion K_P corresponds to an embedding $\iota : K \to \mathbb{C}$. In that case $K_P \cong \mathbb{C}$ or $K_P \cong \mathbb{R}$. Note that if $K_P \cong \mathbb{R}$ then the only proper skewfield is that of the Hamiltonian quaternions. The non-archimedean valuations of the algebraic number field K correspond to prime ideals in the ring $\mathcal{O}_K$ of algebraic integers in K and can therefore be treated by the method describes in the proof of Proposition 2.1.22. The statement in the theorem is then just a reformulation of the celebrated and deep Albert-Brauer-Hasse-Noether theorem (see [29] Theorem 32.19). □

2.1.4 Bass orders

Here we assume all rings are commutative and all modules are finitely generated. Let K be an algebraic number field, R its ring of integers, and let L be a finite dimensional separable K-algebra. We call an R-order $\mathcal{O}$ a Gorenstein order if every exact sequence of $\mathcal{O}$-modules $0 \to \mathcal{O} \to M \to N \to 0$ in which M and N are $\mathcal{O}$-lattices is split over $\mathcal{O}$. If $\mathcal{O}$ has the additional property that every R-order in L containing $\mathcal{O}$ is also a Gorenstein order, then we call $\mathcal{O}$ a Bass order. Note that being a Bass order is a local property, in other words, $\mathcal{O}$ is a Bass R-order if and only if $\mathcal{O}_P$ is a Bass R_P-order for every prime P in R. Let $\mathcal{O}_L$ be the maximal R-order in L.



Proposition 2.1.27 *The following are equivalent:*

(a) $\mathcal{O}$ is a Bass R-order.

(b) $\mathcal{O}_L/\mathcal{O}$ is a cyclic $\mathcal{O}$-module.

(c) Every ideal of $\mathcal{O}$ can be generated by two elements.

(d) For every maximal ideal P of $\mathcal{O}$ we have $\dim_{\mathcal{O}_P/P}((\mathcal{O}_L)_P/P(\mathcal{O}_L)_P) \leq 2$.

(e) The multiplicity of $\mathcal{O}$ at each maximal ideal P is ≤ 2.

Proof The first three parts are equivalent according to [26] Theorem 2.1 and the last two parts are equivalent to (a) by [12] Theorem 2.1. □

Example All maximal $\mathbb{Z}$-orders in number fields are Bass orders. If L is a quadratic field extension over K and $\mathcal{O}$ an R-order in L, then $(O_L)_P/\mathcal{O}_P$ is cyclic for every prime P of R and thus $\mathcal{O}$ is a Bass R-order. □

Let L be a finite field extension over K and let P be a prime of R. For any prime ideal S of $\mathcal{O}_L$ lying over a prime P of R, let $\mathrm{ram}(S/P)$, $\mathrm{rcd}(S/P)$ and $\mathrm{inert}(S/P)$ be the ramication index, residue field degree and decomposition degree, respectively.

Let $\mathcal{O}$ be an R-order in L and consider M, a torsion-free module of rank r over $\mathcal{O}_P$.

Note that $\mathcal{O}_P$ is an artinian ring whose prime ideals are those prime ideals S lying over P. We remark here that there is a decomposition

$$\mathcal{O}_P \cong \prod_{S \mid P} M_S,$$

and that $\alpha \in \mathcal{O}_P$ is a unit if and only if α is coprime to P.

If $\mathcal{O}_P$ is maximal, then M_S is torsion-free over the principal ideal domain $(\mathcal{O}_L)_S$ of rank r, so $M_S \cong (\mathcal{O}_S)^r$. Thus $M \cong (\mathcal{O}_P)^r$. In general, if $\mathcal{O}_P$ is not maximal, it is hard to describe the modules M.

We can however describe torsion-free modules over Bass orders in the local case. Let K be a local field with ring of integers R. For $\mathcal{O}$, be a Bass R-order in a finite field extension L, over K, every indecomposable torsion-free $\mathcal{O}$-module is a projective Λ-module for some R-order Λ in L containing $\mathcal{O}$.

2.2 Quadratic spaces

In this section we introduce the basic notation and definitions regarding quadratic forms and their associated modules. This will be used when we study quaternion algebras later.

We will set the stage in very general terms. Let R be a commutative (and associative) ring with identity. A quadratic form in n variables over R is a homogeneous polynomial of degree 2, $q = q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ with coefficients a_{ij} in R.

If K is a field of characteristic different from 2, then to every quadratic form

$$q = q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

with coefficients a_{ij} in K we can associate a symmetric $n \times n$ matrix M_q with entries

$$m_{ij} = \begin{cases} a_{ij} & i < j \\ 2a_{ij} & i = j \\ a_{ji} & i > j \end{cases}$$

and a bilinear form $b(u, v) = u^t A v$. A direct inspection gives $q(u) = \frac{1}{2} b(u, u)$. This is where problems arise in characteristic 2. We will only consider non-degenerate forms, that is forms for which $\det(M_q) \neq 0$.

Let R be a subring of K with identity. A quadratic form q over K is said to represent $c \in K$ over R, if there exists $u \in R^n$ such that $q(u) = c$ and we call q isotropic, if there is a non-trivial representation of 0.

Two quadratic forms q and f over K are called isometric over R if there is an invertible linear substitution of variables that transforms the one into the other in which case

we write $q \equiv f$. More precisely q is isometric to f if there exists a $T \in \mathrm{GL}_n(R)$ such that $M_q = T^t M_f T$. They are said to be similar over R, denoted $q \sim f$, if there exists a $u \in R^*$ such that uq is isometric to f. Both isometry and similarity are equivalence relations, similarity obviously being coarser.

A form like q is called integral over R if the coefficients a_{ij} are in R. It is called primitive if the ideal generated by the coefficients is equal to R.

The discriminant $\mathrm{disc}(q)$ of a non-degenarate quadratic form q over K is defined to be the class of $\det(M_q)$ in $K/(K^*)^2$. The reason for taking classes modulo $(K^*)^2$ is to make it an invariant of isometry classes. Note that it is only an invariant of similarity classes in even dimensions, since multiplication by u multiplies the determinant by u^n.

If the quadratic form q is integral over R, then the discriminant of q regarded as a form over R is the class of $\det(M_q)$ as an element in the multiplicative set $R\backslash\{0\}$ modulo $(R^*)^2$. In the case of quadratic forms of odd dimensions, it is customary and natural to take the discrimant to be the class of $\frac{1}{2}\det(M_q)$ instead, and we will follow this convention.

Let M be a finitely generated left R-module with basis $\{a_1, \ldots, a_n\}$. A quadratic form q over R in n variables determines a quadratic map on M given by $q_M : M \to R$, $q_M(r_1a_1 + \ldots + r_na_n) = q(r_1, \ldots, r_n)$. With the properties of this example in mind, we now turn to a more general concept of quadratic form.

2.2.1 Quadratic modules

Let R be a commutative (and associative) ring with identity. Let M be any R-module. A quadratic form on M is a map $q_M : M \to R$ such that $q_M(ru) = r^2 q_M(u)$ for all $r \in R$, $u \in M$ and the associated map $b_M : M \times M \to R$ given by $b_M(u, v) = q_M(u+v) - q_M(u) - q_M(v)$ is bilinear.

The pair (M, q_M) is called a quadratic module over R.

If M is a finitely generated projective R-module and q_M is non-singular or regular (this means that for all $v \in M$, the condition $b_M(u, v) = 0$ implies $u = 0$) then (M, q_M) is a quadratic space over R.

Determinants

Let R be an integral domain with field of fractions K and assume (V, q_V) is a quadratic space over K. The quadratic space (V, q_V) determines a quadratic form q over K. If $B = \{\alpha_1, \ldots, \alpha_n\}$ is a K-basis for V, then

$$q = q_V(\alpha_1 x_1 + \ldots + \alpha_n x_n) = \sum_{i \leq j} \alpha_{ij} x_i x_j$$

is a quadratic form over K. If B is also a R-basis for a quadratic module over R then q is a quadratic form over R. If R happens to be a principal ideal domain then every quadratic

module over R has a R-basis.

Let (V, q_V) be a quadratic space over K and let M be a R-lattice in V (a finitely generated R-submodule of V containing a K-basis for V) then (M, q_M) is a quadratic module over R if $q_M(M) \subseteq R$ and (M, b_M) is a bilinear module over R if $b_M(M, M) \subseteq R$. If in addition we have that $b_M(u, u) \in 2R$ for all $u \in M$ then we say (M, b_M) is even. For the bilinear module (M, b_M) over R we can define the determinant as follows. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for M over R then $\det(M, b_M) = \det([\, b_M(\alpha_i, \alpha_j)\,])$

By definition $q_M(u) = \frac{1}{2} b_M(u, u)$ and there is a bijective correspondence between bilinear modules (M, b_M) over R and quadratic modules (M, q_M) over R. We define the determinant of a quadratic module (M, q_M) over R as the determinant of the associated bilinear module (M, b_M). The determinant is non-zero if and only if q_M is regular. The determinant is not independant of the choice of basis. However $\det(M, q_M)$ is well defined modulo R^{*2}. Under inclusion the determinant behaves as follows.

Proposition 2.2.1 *Let (M, q_M) and (N, q_N) be regular quadratic modules over R such that M and N are free of rank n over R. If $M \subseteq N$ then $\det(N, q_N)$ divides $\det(M, q_M)$. If also $\det(M, q_M) = \det(N, q_N) \bmod R^{*2}$ then $M = N$.*

Proof Let $\{\gamma_1, \ldots, \gamma_n\}$ be a R-basis for M and let $\{\lambda_1, \ldots, \lambda_n\}$ be a R-basis for N. Then $\gamma_j = \sum_{i=1}^{n} a_{ij} \lambda_i$ for some $a_{ij} \in R$. Defining matrices $A = [\, a_{ij}\,]$, $B = [\, b_M(\gamma_i, \gamma_j)\,]$ and $C = [\, b_N(\lambda_i, \lambda_j)\,]$ we have $\det(M, q_M) = \det(B) = \det(A^t C A) = (\det(A))^2 \det(N, q_N)$. Thus $\det(N, q_N)$ divides $\det(M, q_M)$. If equality holds modulo R^{*2} then A is invertible and $M = N$. □

Pectora roborant cultus recti

Representations

Let (M, q_M) and (N, q_N) be quadratic modules over an integral domain R. A R-module homomorphism $\varphi : M \to N$ is a called a representation if it satisfies $q_N(\varphi(u)) = q_M(u)$.

If φ is a R-module isomorphism (an invertible linear map) then the representation is called an isometry. We say two quadratic modules over R is equivalent or isometric is there exists an isometry in which case we write $(M, q_M) \equiv (N, q_N)$. Let $f = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j$ be a quadratic form over R in n variables. The notation $(M, q_M) \equiv f$ means that the quadratic module (M, q_M) is isometric to a quadratic module constructed from the quadratic form f in the way described above.

For a quadratic module (M, q_M) over R, an element $r \in R$ is said to be represented by (M, q_M) if $q_M(m) = r$ for some non-zero m in M. We say (M, q_M) is isotropic if (M, q_M) represents 0. It is easy to check that if $(M, q_M) \equiv x_1 x_2$, then (M, q_M) is a two-dimensional isotropic quadratic space over R.

Let $\mathcal{O}$ be a commutative ring containing R. The quadratic form $f = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ over R is also a quadratic form over $\mathcal{O}$. In terms of quadratic modules this is captured by going from (M, q_M) to the tensor product $(M \otimes_R \mathcal{O}, q_{M \otimes_R \mathcal{O}})$. The diagonalization theorem from the theory of quadratic forms says that if K is a field of characteristic different from 2 and

(M, q_M) is a quadratic module over K then $(M, q_M) \equiv a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$ where n is the dimension of M and $a_i \in K$.

For quadratic modules (M, q_M) and (N, q_N) over R. We define a similitude as a R-homomorphism $\varphi : M \to N$ satisfying the weaker condition that $q_N(\varphi(u)) = cq_M(u)$ for some $c \in K^*$. We call c the similitude factor. If φ is a R-module isomorphism then we call the similitude a similarity. If such a φ exists then (M, q_M) is said to be similiar to (N, q_N) and we write $(M, q_M) \sim (N, q_N)$.

A representation or similitude $\varphi : M \to N$ is said to be primitive if the R-module N/M is torsion-free.

Tensor algebras

Let M be a R-module over an unital commutative (and associative) ring R. We define a sequence of R-modules by setting $\text{Tensor}_0(M) = R$ and

$$\text{Tensor}_r(M) = \bigotimes_{i=1}^{r} M \quad \text{for} \quad r > 0.$$

Note that '$\otimes$' gives a natural multipication

$$\otimes : \ \text{Tensor}_r(M) \times \text{Tensor}_s(M) \to \text{Tensor}_{r+s}(M)$$

where $(\alpha, \beta) \mapsto \alpha \otimes \beta$. As a result, if we set

$$\text{Tensor}(M) = \bigoplus_{r=0}^{\infty} \text{Tensor}_r(M)$$

we have a natural R-algebra structure on $\text{Tensor}(M)$. The algebra so determined is called the tensor algebra of M. If we denote by $\iota_M : \text{Tensor}_1(M) \hookrightarrow \text{Tensor}(M)$, the composition $M = \text{Tensor}_1(M) \hookrightarrow \text{Tensor}(M)$, then we have the following universal mapping property. If L is any R-algebra and if $\varphi_M : M \to L$ is any R-module homomorphism, then there exists a unique R-algebra homomorphism $\varphi : \text{Tensor}(M) \to L$ that extends φ_M.

If L is any R-algebra admitting a direct sum decomposition

$$L = \bigoplus_{r=0}^{\infty} L_i$$

such that for all indices r, s we have $L_rL_s \subseteq L_{r+s}$ then we call L a graded algebra. Therefor it is clear that $\text{Tensor}(M)$ is a graded algebra.

Clifford algebras

Let (M, q_M) (with associated bilinear form b_M) be a quadratic module over a unital commutative (and associative) ring R. A Clifford algebra of (M, q_M) is a pair $(\text{Cliff}(M), \iota_M)$

such that

(a) $\mathrm{Cliff}(M)$ is an R-algebra.

(b) $\iota_M : M \to \mathrm{Cliff}(M)$ is a R-module map satisfying

  (i) $\iota_M(\alpha)^2 = q_M(\alpha) \cdot 1$ and

  (ii) $\iota_M(\alpha)\iota_M(\beta) + \iota_M(\beta)\iota_M(\alpha) = b_M(\alpha, \beta) \cdot 1$ for all α and β in M.

(c) $(\mathrm{Cliff}(M), \iota_M)$ is minimal in the sense of an universal mapping property with respect to (a) and (b).

The following very basic facts introduce concepts that will be relevant in the discussions that follow.

Any quadratic module (M, q_M) over R has a unique Clifford algebra and it can be constructed as the quotient of $\mathrm{Tensor}(M)$ by the ideal $\langle\, v \otimes v - q_M(v) \cdot 1 \mid v \in M \,\rangle$.

If M is a finitely generated, projective R-module, then ι_M is injective and there is a unique anti-automorphism on $\mathrm{Cliff}(M)$ taking $\iota_M(\alpha)$ to $\iota_M(\alpha)$ for all α. Note that this anti-automorphism is an involution, as two successive applications of it give the identity map on $\mathrm{Cliff}(M)$.

Let $S = \{\alpha_i\}_{i \in I}$ where I is an index set be a spanning set for M as R-module, then the set $\{\prod_{j=1}^{k} \iota_M(\alpha_{i_j}) |\ \alpha_{i_j} \in S$ and $k \geq 1$ with the indices satisfying $i_1 < \ldots < i_k\}$ along with the identity span $\mathrm{Cliff}(M)$ as R-module. Taking the R-submodule of $\mathrm{Cliff}(M)$ spanned by all the elements above with k even, and then in turn the R-submodule spanned by all the elements above with k odd, splits $\mathrm{Cliff}(M)$ into an even and odd part $\mathrm{Cliff}(M) = \mathrm{Cliff}_0(M) \oplus \mathrm{Cliff}_1(M)$, and provides $\mathrm{Cliff}(M)$ with a $\mathbb{Z}_2$-grading, in otherwords, a two-component grading. Note in particular that $\mathrm{Cliff}_0(M)$ is a R-subalgebra of $\mathrm{Cliff}(M)$ and $\mathrm{Cliff}_1(M)$ is a $\mathrm{Cliff}_0(M)$-module.

If M is free with finite R-basis $B = \{\alpha_1, \ldots, \alpha_n\}$, then $\mathrm{Cliff}(M)$ is a free R-module with basis

$$\{\prod_{j=1}^{k} \iota_M(\alpha_{i_j}) |\ \alpha_{i_j} \in B \text{ and } 1 \leq k \leq n \text{ with the indices satisfying } i_1 < \ldots < i_k\} \cup \{1\}.$$

So $\mathrm{Cliff}(M)$ is a free R-module of dimension 2^n. It follows that $\mathrm{Cliff}_0(M)$ and $\mathrm{Cliff}_1(M)$ are free R-modules as well and that both have dimension 2^{n-1}.

The discriminant algebra $\mathrm{Disc}(M)$ is the centralizer of $\mathrm{Cliff}_0(M)$ in $\mathrm{Cliff}(M)$. More precisely, $\mathrm{Disc}(M) = \{c \in \mathrm{Cliff}(M) \mid cd = dc,\ \forall\ d \in \mathrm{Cliff}_0(M)\}$. The next theorem illustrates the important role that $\mathrm{Disc}(M)$ plays in the structure theory of $\mathrm{Cliff}(M)$ and $\mathrm{Cliff}_0(M)$.

Theorem 2.2.2 *Let K be a field and (V, q_V) a quadratic space over K. Then*

(a) $\mathrm{Disc}(V) \cong K[x]/\langle\, x^2 - ax - b \,\rangle$ *with* $a^2 + 4b \neq 0$.

(b) Suppose $\dim_K(V)$ *is even. Then there is a division algebra,* D *over* K*, such that* $\mathrm{Cliff}(V) \cong \mathbb{M}_k(D)$ *with* $\dim_K(D)$ *and* k *both powers of* 2*. So* $k = 2^m$ *for some* m*.*

(i) Suppose $x^2 - ax - b$ *has a root in* K*. Then* $\mathrm{Disc}(V) \cong K \oplus K$*, and* $\mathrm{Cliff}_0(V) \cong \mathbb{M}_m(D) \oplus \mathbb{M}_m(D)$*.*

(ii) Suppose $x^2 - ax - b$ *does not have a root in* K*, but does have a root in* D*. Then* $\mathrm{Disc}(V)$ *is a subfield of* D*, the centralizer* C *of the root in* D *is a central division algebra over* $\mathrm{Disc}(V)$*, and* $\mathrm{Cliff}_0(V) \cong \mathbb{M}_m(C)$*.*

(iii) Suppose $x^2 - ax - b$ *does not have a root in* D*. Then* $D \otimes_K \mathrm{Disc}(V)$ *is a central division algebra over* $\mathrm{Disc}(V)$ *and* $\mathrm{Cliff}_0(V) \cong \mathbb{M}_m(D \otimes_K \mathrm{Disc}(V))$*.*

(c) Suppose $\dim_K(V)$ *is odd. Then there is a division algebra* D *over* K *such that* $\mathrm{Cliff}_0(V) \cong \mathbb{M}_k(D)$*, with* $\dim_K(D)$ *and* k *both powers of* 2*. Statements analogous to those for* $\mathrm{Cliff}_0(V)$ *above hold for the algebra* $\mathrm{Cliff}(V)$*.*

So for a quadratic space (V, q_V) over a field K we have that if $\dim_K(V)$ is even, then $\mathrm{Cliff}(V)$ is a central simple algebra over K. If $\dim_K(V)$ is odd, then $\mathrm{Cliff}_0(V)$ is a central simple algebra over K.

We have seen that the existence of an involution and (over a field) the property of being central and simple are basic features of the Clifford algebra. Could it possibly be that any finite dimensional central simple algebra that comes equipped with an involution is isomorphic to a Clifford algebra? If the requirement isomorphic is replaced by the weaker is Brauer equivalent to then the answer is yes.

Let K be a field and L a finite dimensional central simple algebra over K with an involution. Then there is a quadratic space (V, q_V) where V is of even rank (and discriminant 1) such that L is Brauer equivalent to $\mathrm{Cliff}(V)$.

Let K be an algebraic number field and let L be a finite dimensional central simple algebra over K with an involution. The result becomes sharper. There is a quadratic space (V, q_V) of dimension 2 such that L is Brauer equivalent to $\mathrm{Cliff}(V)$. This follows from the fact that the only division algebras with involution over such a K are the quaternion division algebras (and K itself). This fact also provides the stronger isomorphism result for algebraic number fields in the sense that in this case there is a quadratic space (V, q_V) of even dimension such that L is isomorphic to $\mathrm{Cliff}(V)$.

Let R be an integral domain with field of fractions K. Let (M, q_M) be a quadratic module over R and let $(V, q_V) = (M \otimes K, q_{M \otimes K})$ be the quadratic space containing it. The R-algebra $\mathrm{Cliff}(M)$ is a R-order in $\mathrm{Cliff}(V)$ and the R-algebra $\mathrm{Cliff}_0(M)$ is a R-order in $\mathrm{Cliff}_0(V)$.

Exterior algebras

Let M be a module over a unital commutative (and associative) ring R. An Exterior algebra of the R-module M is a pair $(\mathrm{Ext}(M), \iota_M)$ such that

(a) $\mathrm{Ext}(M)$ is an R-algebra.

(b) $\iota_M : M \to \mathrm{Ext}(M)$ is a R-module map satisfying

(i) $\iota_M(\alpha)^2 = 0$ for all α in M.

(ii) $\iota_M(\alpha)\iota_M(\beta) + \iota_M(\beta)\iota_M(\alpha) = 0$ for all α and β in M.

(c) If $\varphi_M : M \to L$ is a R-module homomorphism to an R-algebra L such that $\varphi_M(\alpha)^2 = 0$ for all α in M then there exists an unique R-algebra homomorphism

$$\varphi : \mathrm{Ext}(M) \to L \text{ such that } \varphi\iota_M = \varphi_M.$$

We can construct $\mathrm{Ext}(M)$ explicitly as follows. Let $\mathrm{Tensor}(M)$ be the tensor algebra of M and let L be the quotient of $\mathrm{Tensor}(M)$ by the ideal $J = \langle\, v \otimes v \mid v \in M \,\rangle$. Then L is isomorphic to $\mathrm{Ext}(M)$ via an unique isomorphism commuting with the inclusion of M into each.

That is $\mathrm{Ext}(M) \cong \mathrm{Tensor}(M)/J$. If we let $\bigwedge^r(M) = \mathrm{Tensor}_r(M)/(\mathrm{Tensor}_r(M) \cap j)$, then

$$\mathrm{Tensor}(M) = \bigoplus_{r=0}^{\infty} \bigwedge^r(M)$$

is a graded algebra generated by the set $\{\iota_M(\alpha) \mid \alpha \in M\}$ with the generators being anti-commuting quantities. We call $\mathrm{Ext}_r(M)$ the r^{th}-graded submodule of $\mathrm{Ext}(M)$ and we have $\mathrm{Ext}_r(M)\mathrm{Ext}_s(M) \subseteq \mathrm{Ext}_{r+s}(M)$.

Example If $q_M = 0$, then $\mathrm{Cliff}(M)$ is a unital associative exterior R-algebra generated by a set, S subject to the relation $ab + ba = 0$ for any $a, b \in S$. □

If M a free rank d module over an integral domain R, then $\mathrm{Ext}(M)$ is free of rank 2^d over R and $\mathrm{Ext}_r(M)$ has rank $\binom{d}{r}$ over R.

Let (M, b_M) be a bilinear module over R. The determinant map

$$\det_R : \mathrm{Ext}_r(M) \to R$$

on each r^{th}-graded R-submodule of $\mathrm{Ext}(M)$ given by $\alpha_1 \wedge \ldots \wedge \alpha_r \mapsto \det(A)$ with $A = [\, b_M(\alpha_i, \alpha_j)\,]$ is well defined. Thus we can define a bilinear map Φ_r on the whole of $\mathrm{Ext}_r(M)$ as

$$\begin{aligned} \Phi_r : \mathrm{Ext}_r(M) \times \mathrm{Ext}_r(M) &\to R \\ (\alpha_1 \wedge \ldots \wedge \alpha_r, \beta_1 \wedge \ldots \wedge \beta_r) &\mapsto \det(A) \text{ with } A = [\, b_M(\alpha_i, \beta_j)\,] \end{aligned}$$

and extending linearly to sums. Thus the bilinear form Φ_r gives us a well defined determinant map on each graded submodule $\mathrm{Ext}_r(M)$ of $\mathrm{Ext}(M)$.

Moreover the inclusion $\iota_M : M \to \mathrm{Ext}(M)$ gives and isometry of the bilinear module (M, b_M) with $(\mathrm{Ext}_1(M), \Phi_1)$.

Theorem 2.2.3 *Let (M, b_M) be a regular bilinear module of rank n over R. $\mathrm{Ext}(M)$ gets a quadratic module structure from the determinant maps Φ_r on the submodules $\mathrm{Ext}_r(M)$.*

For every quadratic submodule (N, q_N) of (M, q_M) of rank r over R, the determinant of the quadratic submodule $\mathrm{Ext}_r(N) \cdot M$ of $\mathrm{Ext}_{r+1}(M)$ is equal to $\det(N, q_N)^{n-r-1}\det(M, q_M)$.

Proof Let $V = M \otimes \mathbb{Q}$ and let $U = N \otimes \mathbb{Q}$. Define W to be the $n-r$ dimensional orthogonal complement of U in V relative to the bilinear form b_M, and let Λ to be the projection of M on W. Then $\mathrm{Ext}_r(N) \wedge M$ and $\mathrm{Ext}_r(N) \wedge \Lambda$ are equal as submodules of $\mathrm{Ext}(V)$, so it suffices to prove the result for $\mathrm{Ext}_r(N) \wedge \Lambda$. Let $\{\omega_i\}$ be a basis for Λ and let α be a generator for $\mathrm{Ext}_r(N)$. Since Λ is orthogonal to N, by definition of the bilinear form Φ_{r+1} on $\mathrm{Ext}_{r+1}(M)$, we have $[\,\Phi_{r+1}(\alpha \wedge \omega_i, \alpha \wedge \omega_j)\,] = \det(N, q_N)[\,b_M(\omega_i, \omega_j)\,]$. We also have that for $I = N \oplus \Lambda$, we have $\det(M, q_M) = \det(I, q_I) = \det(N, q_N)\det(\Lambda, q_\Lambda)$. Hence it follows that if $I = \mathrm{Ext}_r(N) \wedge \Lambda$ and $J = \det(N, q_N) \wedge \Lambda$, then

$$\det(I, q_I) = \det(J, q_J) = \det(N, q_N)^{n-r} \frac{\det(M, q_M)}{\det(N, q_N)}$$

and the result holds. □

2.3 Quaternion algebras

In this section we give basic definitions concerning quaternion algebras. If K is an algebraic number field with ring of integers R, then let Ω denote the set of places (normalized valuations) on K, Ω_f the finite (non-archimedean) and Ω_∞ the infinite (archimedean) valuations. Let $P \in \Omega$, then K_P will denote the completion of K with respect to P as usual. If $P \in \Omega_f$, then R_P will denote the ring of integers in K_P. When a ring R is understood, then $\langle\, \lambda_1, \lambda_2, \ldots, \lambda_n \,\rangle$ will denote then free R-module generated by the elements $\lambda_1, \lambda_2, \ldots, \lambda_n$.

2.3.1 The structure of quaternion algebras

Here we will give the definition and some fundamental properties of quaternion algebras. We will emphasize the connection between quadratic forms and quaternion algebras and give a quite general solution to the problem of representing a quaternion algebra with given discriminant.

We will reduce in generality along the way to make the exposition as simple and clear as possible.

Let K be an arbitrary field. A quaternion algebra L over K is a simple central algebra of dimension 4 over K. Here central means L has centre K and simple means that there are no two-sided ideals in L except for $\{0\}$ and L itself. The smallest examples of non-commutative simple algebras are of dimension 4.

Example If K is a field and (M, q_M) is a quadratic module over K of dimension 2 and q_M is non-singular, then $\mathrm{Cliff}(M)$ is a quaternion algebra over K. □

From Wedderburn's structure theorem on simple algebras (Theorem 2.1.1) one deduces that either $L \cong \mathbb{M}_2(K)$ or $L \cong D$, where D is a divisional algebra with centre K. We will from now on assume that $\mathrm{char}(K) \neq 2$. With this condition, it is always possible to find a

convenient diagonal basis $\{1, i, j, ij\}$ of L over K, which satisfies the relations $i^2 = a,\ j^2 = b$ and $ij = -ji$ where $a, b \in K$. We denote such an algebra as $(a, b)_K$. We remark that it is possible to embed $(a, b)_K$ in $\mathbb{M}_2(K(\sqrt{a}))$. For example

$$i \mapsto \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix},\ j \mapsto \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

From this it is clear that if a is a square in K, then $(a, b)_K \cong \mathbb{M}_2(K)$. A necessary and sufficient condition for $(a, b)_K \cong \mathbb{M}_2(K)$ is that a is the norm of some element in $K(\sqrt{b})$ with respect to K. Of course, one may interchange a and b in this remark.

There is a natural involution, ι_L on L, which in terms of a basis as described above is given by

$$\iota_L(\lambda) = \iota_L(\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 ij) = \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 ij.$$

One defines the reduced trace and reduced norm from L into K by

$$\overline{\mathrm{t}}\mathrm{race}(\lambda) = \lambda + \iota_L(\lambda) \quad \text{and} \quad \overline{\mathrm{n}}\mathrm{orm}(\lambda) = \lambda \iota_L(\lambda).$$

The norm is a quaternary quadratic form over K, with corresponding symmetric bilinear form given by $\overline{\mathrm{t}}\mathrm{race}(\lambda \iota_L(\beta))$. A direct calculation gives $\overline{\mathrm{n}}\mathrm{orm}(\lambda) = \lambda_0^2 - a\lambda_1^2 - b\lambda_2^2 + ab\lambda_3^2$, if $\lambda = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 ij \in (a, b)_K$. From this we see that the determinant of the norm form on $(a, b)_K$ is equal to $16a^2b^2$. Hence the discriminant of the norm form of a quaternion algebra is equal to 1.

Now define the set of pure quaternions to be the set $L^+ = \{\lambda \in L |\ \overline{\mathrm{t}}\mathrm{race}(\lambda) = 0\}$ and denote the norm restricted to L^+ by $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$. If we have chosen a basis of L satisfying the conditions in the previous paragraph, then obviously $L^+ = \langle\, i, j, ij \,\rangle$. We conclude that L^+ is a 3-dimensional K-vector space and $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ a ternary quadratic form. A nontrivial and interesting fact is that $\overline{\mathrm{n}}\mathrm{orm}_{L/K}$ is isotropic if and only if $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ is isotropic. The norm form determines the quaternion algebra in the following way.

Proposition 2.3.1 *Let K be a field with characteristic different from 2 and let L and H be quaternion algebras over K with corresponding norm forms $\overline{\mathrm{n}}\mathrm{orm}_{L/K}$ and $\overline{\mathrm{n}}\mathrm{orm}_{H/K}$. Then the following are equivalent.*

(a) $L \cong H$

(b) $\overline{\mathrm{n}}\mathrm{orm}_{L/K}$ *and* $\overline{\mathrm{n}}\mathrm{orm}_{H/K}$ *are isometric*

(c) $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ *and* $\overline{\mathrm{n}}\mathrm{orm}_{H^+/K}$ *are isometric*

Moreover, L being a division algebra is equivalent to $\overline{\mathrm{n}}\mathrm{orm}_{L/K}$ being anisotropic, which in turn is equivalent to $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ being anisotropic.

Proof See [28] Section 57. □

This correspondence between quaternion algebras and quaternary quadratic forms will be

used in the sequel. We now specialize to the fields of our main interest. So for now on assume that K is an algebraic number field. If P is a place on K, then $L_P = L \otimes_K K_P$ is a quaternion algebra over K_P.

Proposition 2.3.2 *Let K be an algebraic number field. Then there is a one-to-one correspondence between*

(a) isomorphism classes of quaternion algebras over K and

(b) isometry classes of quaternary quadratic forms over K with discriminant equal to 1, which are not negative definite at any real place.

Futhermore, if P is a place on K, then there is a one-to-one correspondence between

(a) isomorphism classes of quaternion algebras over K_P and

(b) isometry classes of quaternary quadratic forms over K_P with discriminant equal to 1, which are not negative definite if $K_P = \mathbb{R}$.

Proof Every quaternary quadratic form q over K represents 1 if and only if it is not negative definite at any real place. Hence, we may conclude that $q = 1x_0^2 + ax_1^2 + bx_2^2 + cx_3^2$ for some $a, b, c \in K$ if q is not negative definite at any real place. If the discriminant of q is equal to 1, then we may assume that $c = ab$ and the statement follows from Proposition 2.3.1. □

The classification of quadratic forms over general number fields is due to Hasse. Using his results and Proposition 2.3.2 one derives the following two theorems on the classification of quaternion algebras up to isomorphism.

Pectora roborant cultus recti

Theorem 2.3.3 *Let K_P be the completion of a number field K. The there are exactly two quaternion algebras over K_P up to isomorphism, $\mathbb{M}_2(K_P)$ and a division algebra.*

We say a quaternion algebra L over K is ramified at P if L_P is a division algebra, otherwise L is said to be split at P. If P is a real place, then one often uses definite/indefinite instead of ramified/split, especially if $K = \mathbb{Q}$.

Theorem 2.3.4 *Let K be an algebraic number field and L and H two quaternion algebras over K. The following statements are equivalent.*

(a) $L \cong H$,

(b) $L_P \cong H_P$ for all $P \in \Omega$,

(c) L and H are ramified at the same places.

Moreover, L is always ramified at an even number of places. Conversely given an even number of places, it is always possible to find a quaternion algebra over K which is ramified at exactly these places.

The reduced discriminant $\overline{\mathrm{d}}\mathrm{isc}(L)$ of a quaternion algebra L is defined to be the product of prime ideals P at which L is ramified. This is a well defined invariant of the isomorphism classes defined in the previous theorem. If $K = \mathbb{Q}$ then the discriminant determines the isomorphism class, but for other fields one clearly needs information on the infinite ramifications.

With this classification at hand, it is of course of interest to be able to easily determine the ramifications of a given quaternion algebra over K. It turns out the Hilbert symbol solves the problem. If $P \in \Omega$ and $a, b \in K_P^*$, then the Hilbert symbol $(a,b)_P$ in K_P is defined by

$$(a,b)_P = \begin{cases} 1 & \text{if } x^2 - ay^2 - bz^2 \text{ is isotropic over } K_P \text{ and} \\ -1 & \text{otherwise.} \end{cases}$$

We remark that if $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ is the restricted norm form on $(a,b)_K$, then

$$ab \cdot \overline{\mathrm{n}}\mathrm{orm}_{L^+/K} \cong -ax_0^2 - bx_1^2 + x_3^2.$$

From this we conclude that $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$ is isotropic at P if and only if $(a,b)_P = 1$. Hence it is immediate from Proposition 2.3.1 that $(a,b)_K$ is ramified at P if and only if $(a,b)_P = -1$.

Proposition 2.3.5 *The Hilbert symbol satisfies the following properties:*

(a) $(a,bc)_P = (a,b)_P \cdot (a,c)_P$, $(a,-a)_P = 1$ and $(a,b^2)_P = 1$.

(b) If P is real, then $(a,b)_P = -1$ if and only if $a < 0$ and $b < 0$.

(c) If P is non-dyadic prime, then
$$\begin{cases} (a,b)_P = 1 & \text{if } a, b \in R_P^*, \\ (a,P)_P = 1 & \text{if } a \in R_P^* : a \text{ is a square modulo } P, \\ = -1 & \text{otherwise.} \end{cases}$$

(d) $\prod_{P \in \Omega} (a,b)_P = 1 \ \forall \ a, b \in K^*$.

Proof See [28] Section 63 and 71. □

We remark that property (d) is exactly what is needed to prove that L is always ramified at an even number of places. The dyadic case this solves the problem, but otherwise we might have to do some calculations. However it is possible to prove the following general result.

Proposition 2.3.6 *If π is a prime element in R_P, $\gamma \in R_P^*$ and $\alpha \in R_P^*$ is an element of quadratic defect $\gamma_P(\alpha) = 4R_P$ (α is not a square but congruent to a square modulo $4R_P$), then $(\pi, \alpha)_P = -1$ and $(\gamma, \alpha)_P = 1$.*

Proof See [28] Section 63.11a. □

The concluding result of this section addresses the following problem. Given the ramifications of a quaternion algebra over K, find $a, b \in R$ such that $L \cong (a,b)_K$.

If $\overline{\mathrm{d}}\mathrm{isc}(L) = P_1 P_2 \cdots P_r$, then let n_i be positive integers such that $J = P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r}$

is principal. The principal ideal J (or a generator of J) will be called a representative for $\overline{\mathrm{d}}\mathrm{isc}(L)$. The following proposition gives an answer when $\overline{\mathrm{d}}\mathrm{isc}(L) = R$ or $\overline{\mathrm{d}}\mathrm{isc}(L)$ has a representative $P_1^{n_1}P_2^{n_2}\cdots P_r^{n_r}$ such that all n_i are odd integers, in particular when $\overline{\mathrm{d}}\mathrm{isc}(L)$ is principal. It is also a very explicit proof of the last conclusion in Theorem 2.3.4 in this restricted case. In principal, it follows the same idea as in Hasse's original proof.

Proposition 2.3.7 *Let L be a quaternion algebra over an algebraic number field K. Suppose $\overline{\mathrm{d}}\mathrm{isc}(L) = R$ or $\overline{\mathrm{d}}\mathrm{isc}(L) = P_1P_2\cdots P_r$ has representative $dR = P_1^{n_1}P_2^{n_2}\cdots P_r^{n_r}$ such that all integers n_i are odd. Then choose $a \in R$ to be a generator of a prime ideal satisfying*

$$\gcd(a,d) = 1 \text{ and } \begin{cases} a < 0 & P \text{ real, if } L \text{ ramified at } P, \\ a > 0 & P \text{ real, if } L \text{ split at } P, \\ \left(\frac{a}{P}\right) = -1 & \text{at } P \text{ nondyadic, if } L \text{ ramified at } P, \text{ and} \\ \delta_P(a) = 4R_P & \text{at all dyadic primes } P. \end{cases}$$

Then $L \cong (a,-d)_K$.

Proof The existence of such an a is assured by the generalisation to arbitrary number fields of Dirichlet's theorem on primes in linear progressions. The ramifications of L and $(a,-d)_K$ obviously agree at all real places. If P is a non-dyadic prime dividing d, then Proposition 2.3.5 implies that $(a,-d)_P = (a,P)_P = -1$. This is where it is necessary to have P to an odd power in dR. The only other non-dyadic prime at which $(a,-d)_K$ could possibly be ramified is a, since $a, d \in R_P^*$ for all other non-dyadic primes.
If P is a dyadic prime then Proposition 2.3.6 implies $(a,-d)_P = -1$ if and only if $P \mid d$. Hence the ramifications of L and $(a,-d)_K$ differ at most at a and then Proposition 2.3.4 implies that $L \cong (a,-d)_K$. □

For the field of rational numbers Proposition 2.3.7 simplifies further.

Corollary 2.3.8 *Let L be an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant $d = p_1\cdots p_{2r}$ Choose an ℓ to be a prime such that $\ell \equiv 5$ mod 8 and ℓ is not a quadratic residue modulo p_i $\forall p_i > 2$. Then $L \cong (\ell,d)_{\mathbb{Q}} \cong (\ell,-d)_{\mathbb{Q}}$.*

Corollary 2.3.9 *Let L be a definite quaternion algebra over $\mathbb{Q}$ with discriminant $d = p_1\cdots p_{2r-1}$. Choose ℓ to be prime such that $\ell \equiv 3$ mod 8 and ℓ is not a quadratic residue modulo p_i $\forall p_i > 2$. Then $L \cong (-\ell,-d)_{\mathbb{Q}}$.*

2.3.2 Quaternion orders

Let R be a Dedekind domain, K its field of quotients and L a quaternion algebra over K. For the rest of this section $\mathcal{O}$ will denote a R-order in L. We remark that it is not always possible to find a R-basis for $\mathcal{O}$. However it is always possible to find a K-basis $\{e_1,e_2,e_3,e_4\}$ for L and a R-ideal I such that $\mathcal{O} = Ie_1 \oplus Re_2 \oplus Re_3 \oplus Re_4$.

The most important invariant of a quaternion R-order $\mathcal{O}$ is its reduced discriminant. Let $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ be a R-basis for $\mathcal{O}$, then the reduced discriminant is defined as the R-ideal,

$$\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \langle \det([\,\overline{\mathrm{t}}\mathrm{race}(\alpha_i\iota_L(\alpha_j))\,])\rangle^{\frac{1}{2}}$$

Let Λ and $\mathcal{O}$ be R-orders in a quaternion K-algebra L. Then the discriminants satisfy $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \overline{\mathrm{d}}\mathrm{isc}(\Lambda)[\Lambda : \mathcal{O}]$.

Example Let $L = (a,b)_K$ be a quaternion algebra. Suppse that $a, b \in R$. This is no restriction, since $(a,b)_K \cong (ac^2, bd^2)_K$ for all $c,\ d \in K$. Then $\mathcal{O} = R + ri + rj + Rij$, where i, j satisfies the relations given in the definition of $(a,b)_K$ is an R-order in L. We will denote this order by $(a,b)_R$. The discriminant if $\mathcal{O}$ is given by $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \langle \det([\,\overline{\mathrm{t}}\mathrm{race}(\alpha_i \iota_L(\alpha_j))\,]) \rangle^{\frac{1}{2}}$ where $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{1, i, j, ij\}$. A simple calculation shows that $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = 4abR$. $\square$

Recall that a maximal R-order is an R-order, which is not strictly contained in any other R-order. The concept of maximal R-orders is more complicated than in the commutative case, since there can be more than one maximal R-order. This complication occurs since $\{\alpha \in L \,|\, \overline{\mathrm{t}}\mathrm{race}(\alpha), \overline{\mathrm{n}}\mathrm{orm}(\alpha) \in R\}$ need not be a ring. However, we will see that the discriminants of all maximal R-orders in a quaternion algebra agree.

The task to classify all quaternion R-orders is of course much more complicated than for quaternion algebras. In particular, there is no analogue of Theorem 2.3.4, that is, isomorphism at all places no longer implies global isomorphism. However the investigation of $\mathcal{O}_P = \mathcal{O} \otimes_R R_P$ is still essential and useful in order to classiy quaternion R-orders $\mathcal{O}$ in algebras over algebraic number fields.

In order to get a structure on the set of R-orders in a quaternion algebra, we recall the definitions of the special classes of R-orders. A R-order, $\mathcal{O}$, is called Gorenstein if $\hat{\epsilon}(\mathcal{O})$ is a projective $\mathcal{O}$-module, and it is called a Bass R-order if every R-order in L containing $\mathcal{O}$ is a Gorenstein R-order.

If $\mathcal{O}$ contains the maximal R-order in a quadratic field extension of the ground field then $\mathcal{O}$ is a Bass R-order. For quaternion R-orders, the converse is true in the local case but in the global case, this is an open question.

For all $\mathcal{O}$ there exists a unique Gorenstein R-order $\mathrm{O_G}(\mathcal{O})$, called the Gorenstein closure, and a unique R-ideal $\mathrm{B_{inv}}(\mathcal{O}) \subseteq R$ (the Brandt invariant) such that

$$\mathcal{O} = R + \mathrm{B_{inv}}(\mathcal{O}) \cdot \mathrm{O_G}(\mathcal{O}).$$

An R-order is called primitive if it contains a maximal R-order of a quadratic subfield of L. It is easy to show that every primitive R-order is a Bass R-order however the converse seems to be an open question in general.

A R-order is called hereditary if every fractional one-sided $\mathcal{O}$-ideal is $\mathcal{O}$-projective. It is well know that hereditary R-orders are exactly those with square free discriminant. These classes of R-orders obviously satisfy the inclusions

$$\{\text{Gorenstein}\} \supset \{\text{Bass}\} \supset \{\text{Hereditary}\} \supseteq \{\text{Maximal}\}.$$

Ternary quadratic forms

We will in this section refine the correspondence between quaternions and ternary quadratic forms. A classification of the ternary quadratic forms wil provide us with an efficient tool to consider arbitrary R orders instead of having to restrict to special classes of them. Existing results are mostly restricted to special classes of orders, most notably to so called Eichler orders.

We will have to assume that R is a principal ideal domain. If f is a non-degenerate ternary quadratic form integral over R. Then define $\mathrm{Cliff}_0(f)$ to be the even Clifford algebra over R associated to f. Then $\mathrm{Cliff}_0(f)$ is an R-order in a quaternion algebra over K. If $f = \sum_{i,j=1}^{3} a_{ij}x_ix_j$, then a direct computation shows that $\mathrm{Cliff}_0(f)$ has a R-basis $\{1, e_1, e_2, e_3\}$ such that for an even permutation (i, j, k) of $(1, 2, 3)$

$$\begin{aligned} e_i^2 &= a_{jk}e_i - a_{jj}a_{kk}, \\ e_ie_j &= a_{kk}(a_{ij} - e_k), \\ e_je_i &= a_{1k}e_1 + a_{2k}e_2 + a_{3k}e_3 + a_{ik}a_{jk}. \end{aligned} \tag{2.1}$$

From this we get the norm form for $\mathrm{Cliff}_0(f)$ in this basis is

$$q = x_0^2 + \sum_{(i,j,k)} (a_{ij}x_0x_k + a_{ii}a_{jj}x_k^2 + ((a_{ik}a_{jk} - a_{ij}a_{kk})x_ix_j)$$

where the sum is over all even permutations (i, j, k) of $(1, 2, 3)$. It is trivial to check from the relations that if $\gamma \in R^*$, then $\mathrm{Cliff}_0(f) = \mathrm{Cliff}_0(\gamma f)$. Conversely assume that $\mathcal{O} = \langle\, 1, e_1, e_2, e_3 \,\rangle$ is an R-order in a quaternion algebra L. Then $\Lambda = \hat{\epsilon}(\mathcal{O}) \cap L^+$ is a 3-dimensional R-lattice in L^+. If $\hat{\epsilon}(\mathcal{O}) = \langle\, \hat{e}_0, \hat{e}_1, \hat{e}_2, \hat{e}_3 \,\rangle$ where $\{\hat{e}_i\}$ is the dual basis of $\{e_i\}$, then $\Lambda = \langle\, \hat{e}_1, \hat{e}_2, \hat{e}_3 \,\rangle$. Given this we define a ternary quadratic form $\hat{e}_{\mathcal{O}}$ associated to $\mathcal{O}$ by

$$\hat{e}_{\mathcal{O}} = \overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) \cdot \overline{\mathrm{n}}\mathrm{orm}(x_1\hat{e}_1 + x_2\hat{e}_2 + x_3\hat{e}_3).$$

Here multiplication by the (principal) ideal $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})$ is understood as multiplication by a generator of $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})$. Hence $\hat{e}_{\mathcal{O}}$ is only defined up to multiplication by units in R.

Theorem 2.3.10 *Let R be a principal ideal domain. The maps $f \mapsto \mathrm{Cliff}_0(f)$ and $\mathcal{O} \mapsto f_{\mathcal{O}}$ are inverses to each other and the discriminants satisfy $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \mathrm{disc}(f_{\mathcal{O}})R$. Furthermore the maps give a bijection between similarity classes of non-degenerate ternary quadratic forms integral over R and isomorphism classes of quaternion R-orders.*

Proof First we prove that $\mathrm{Cliff}_0(\hat{a}_{\mathcal{O}}) = \mathcal{O}$. Suppose $\mathcal{O} = \langle\, a_0, a_1, a_2, a_3 \,\rangle$ and $\hat{\epsilon}(\mathcal{O}) = \langle\, \hat{a}_0, \hat{a}_1, \hat{a}_2, \hat{a}_3 \,\rangle$ where $\{\hat{a}_i\}$ is the dual basis of $\{a_i\}$ and $a_0 = 1$. By definition these bases satisfy $\overline{\mathrm{t}}\mathrm{race}(a_i\iota_L(\hat{a}_j)) = \delta_{ij}$. In particular $\overline{\mathrm{t}}\mathrm{race}(\hat{a}_0) = 1$ and $\overline{\mathrm{t}}\mathrm{race}(\hat{a}_i) = 0$ if $i > 0$. It is straightforward to check that $a_i = \overline{\mathrm{t}}\mathrm{race}(\hat{a}_1\hat{a}_2\hat{a}_3)^{-1}(\overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0)) - \hat{a}_j\hat{a}_k)$ where (i, j, k)

is an even permutation of $(1,2,3)$. For example

$$\begin{aligned} & \overline{\mathrm{t}}\mathrm{race}((\overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0)) - \hat{a}_j\hat{a}_k)\iota_L(\hat{a}_i)) \\ = \; & \overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0))\overline{\mathrm{t}}\mathrm{race}(\iota_L(\hat{a}_i)) - \overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_i)) \\ = \; & \overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\hat{a}_i) \\ = \; & \overline{\mathrm{t}}\mathrm{race}(\hat{a}_i\hat{a}_j\hat{a}_k) \\ = \; & \overline{\mathrm{t}}\mathrm{race}(\hat{a}_1\hat{a}_2\hat{a}_3) \end{aligned}$$

since $(\omega_1,\omega_2,\omega_3) \mapsto \overline{\mathrm{t}}\mathrm{race}(\omega_1\omega_2\omega_3)$ is trilinear and alternating on L^+, and $\iota_L(\omega) = -\omega$ on L^+. Now $d = \overline{\mathrm{t}}\mathrm{race}(\hat{a}_1\hat{a}_2\hat{a}_3)^{-1}$ is a generator of $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})$ and $d\,\hat{a}_j\hat{a}_k$ is integral over R. Hence we can write $d\,\hat{a}_j\hat{a}_k = d\,\overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0)) - a_i$ and conclude that $d\,\overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0)) \in R$. From this definition of $\hat{a}_{\mathcal{O}}$ we get that

$$\hat{a}_{\mathcal{O}} = d\sum_{i\le j} b_{ij}x_ix_j \text{ where } b_{ij} = \begin{cases} \overline{\mathrm{t}}\mathrm{race}(\hat{a}_i\iota_L(\hat{a}_j)) & \text{if } i \neq j. \\ \overline{\mathrm{n}}\mathrm{orm}(\hat{a}_i) & \text{if } i = j. \end{cases}$$

Now it is straightforward to check that $\{e_i = d\,\hat{a}_i\iota_L(\hat{a}_k)\}$, with (i,j,k) an even permutation of $(1,2,3)$ and $\{b_{ij}\}$ as above, satisfy the relations in (2.1). Hence we can identify $\mathrm{Cliff}_0(\hat{a}_{\mathcal{O}})$ with the order $\Gamma = \langle\, 1, d\,\hat{a}_1\iota_L(\hat{a}_2), d\,\hat{a}_2\iota_L(\hat{a}_3), d\,\hat{a}_3\iota_L(\hat{a}_1)\,\rangle$. But since $d\,\hat{a}_j\iota_L(\hat{a}_k) = -d\,\hat{a}_j\hat{a}_k = a_i - d\,\overline{\mathrm{t}}\mathrm{race}(\hat{a}_j\hat{a}_k\iota_L(\hat{a}_0))$, we get $\mathcal{O} = \Gamma = \mathrm{Cliff}_0(\hat{a}_{\mathcal{O}})$. To prove the other direction, that is, $\hat{a}_\Lambda = f$ with $\Lambda = \mathrm{Cliff}_0(f)$ is a straightforward calculation. All one has to do is to determine the dual basis $\{\hat{a}_0,\hat{a}_1,\hat{a}_2,\hat{a}_3\}$ of the basis satisfying the relations in (2.1) and then calculate $\overline{\mathrm{n}}\mathrm{orm}(x_1\hat{a}_1 + x_2\hat{a}_2 + x_3\hat{a}_3)$. The fact that isometric forms gives isomorphic Clifford algebras folllows directly from the universal property of Clifford algebras. Hence $f \sim g$ implies $\mathrm{Cliff}_0(f) \cong \mathrm{Cliff}_0(g)$ since as we remarked above $\mathrm{Cliff}_0(f) = \mathrm{Cliff}_0(\gamma f)$ if $\gamma \in R^*$. Conversely, let $\mathcal{O}_1$ and $\mathcal{O}_2$ be R-orders in L. Then there is an $c \in L$ such that $\mathcal{O}_1 = c^{-1}\mathcal{O}_2$ and $\Lambda_1 = c^{-1}\Lambda_2 c$ where $\Lambda_i = \hat{\epsilon}(\mathcal{O}_i) \cap L^+$. But $a \mapsto c^{-1}ac$ is an isometry of L^+ with respect to $\overline{\mathrm{n}}\mathrm{orm}_{L^+/K}$. Hence $f_{\mathcal{O}_1}$ is isometric to $f_{\mathcal{O}_2}$. Finally it is an easy calculation to show that $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \langle\, \overline{\mathrm{d}}\mathrm{isc}(f_{\mathcal{O}})\,\rangle$. □

Proposition 2.3.11 *Let f be a non-degenerate ternary quadratic form, integral over R and $\mathcal{O} = \mathrm{Cliff}_0(f)$. If $f = bg$ where $b \in R$ and g is primitive, then the Brandt invariant $\mathrm{B}_{\mathrm{inv}}(\mathcal{O})$ of $\mathcal{O}$ is equal to bR and the Gorenstein closure $\mathrm{O}_{\mathrm{G}}(\mathcal{O})$ of $\mathcal{O}$ is equal to $\mathrm{Cliff}_0(g)$. In particular $\mathcal{O}$ is a Gorenstein R-order if and only if f is primitive.*

Proof It follows immediately from the relations in (2.1) that if $f = gb$ then $\mathrm{Cliff}_0(f) = R + \mathrm{B}_{\mathrm{inv}}(\mathcal{O}) \cdot \mathrm{Cliff}_0(g)$. □

Isomorphism classes of quaternion orders

In this section we will investigate the isomorphism classes of orders in quaternion algebras over P-adic fields. We will derive representatives of isomorphism classes in the non-dyadic and the 2-adic cases.

So let K will be an P-adic field with ring of integers R and $P = \pi R$. It is very much more elaborate in the dyadic than in the non-dyadic case. Therefore we will restrict to 2-adic fields in the dyadic case, i.e. field in which $2R$ is prime. We will show in this section

that the maximal R-orders are unique up to isomorphism in the P-adic case. However in the case of a division algebra one can say more.

Proposition 2.3.12 *Let $\mathcal{O}$ be an R-order in a quaternion algebra L over a local field K, and let P be the maximal ideal in R. If $L \cong \mathbb{M}_2(K)$ then $\mathcal{O}$ is conjugate to $\mathbb{M}_2(R)$ so $\overline{\text{d}}\text{isc}(\mathcal{O}) = R$, and if L is a division algebra then $\mathcal{O}$ is unique and $\overline{\text{d}}\text{isc}(\mathcal{O}) = P$.*

Proof See [38] Chapter 2. □

We next define an invariant of an R-order in the local case introduced by Eichler. Let $\mathcal{O}$ be an R-order, let F be the residue class field of K and let $\text{Rad}(\mathcal{O})$ denote the radical of $\mathcal{O}$. If $\mathcal{O} \ncong \mathbb{M}_2(K)$ then then Eichler invariant $\text{E}_{\text{inv}}(\mathcal{O})$ is defined to be

$$\text{E}_{\text{inv}}(\mathcal{O}) = \begin{cases} 1 & \text{if } \mathcal{O}/\text{Rad}(\mathcal{O}) \cong F \oplus F, \\ 0 & \text{if } \mathcal{O}/\text{Rad}(\mathcal{O}) \cong F \text{ and} \\ -1 & \text{if } \mathcal{O}/\text{Rad}(\mathcal{O}) \text{ is a quadratic field extension of } F. \end{cases}$$

Eichler also showed how to compute $\text{E}_{\text{inv}}(\mathcal{O})$ easily. If $a \in L$ then the discriminant of a is defined to be $\overline{\text{d}}\text{isc}(a) = \overline{\text{t}}\text{race}(a)^2 - 4\overline{\text{n}}\text{orm}(a)$.

For all $a \in \mathcal{O}$, define

$$\omega_P(a) = \begin{cases} 1 & \text{if } \overline{\text{d}}\text{isc}(a) \text{ is a square mod } P, \\ 0 & \text{if and only if } a \in P \text{ and} \\ -1 & \text{if } \overline{\text{d}}\text{isc}(a) \text{ is not a square mod } P. \end{cases}$$

The Eichler invariant can be determined using the fact that

$$\text{if } \text{E}_{\text{inv}}(\mathcal{O}) = \begin{cases} 1 & \text{then } \omega_P(a) \neq -1 \text{ and } \exists a \in \mathcal{O} : \omega(a) = 1. \\ 0 & \text{then } \omega_P(a) = 0. \\ -1 & \text{then } \omega_P(a) \neq 1 \text{ and } \exists a \in \mathcal{O} : \omega(a) = -1. \end{cases}$$

In particular if $\mathcal{O}$ is not a Bass R-order, then $\text{E}_{\text{inv}}(\mathcal{O}) = 0$.

Let f be a ternary quadratic form, integral over R. We can restrict to f primitive since if $f_1 = b_1 g_1$ and $f_1 = b_2 g_2$ with $b_i \in R$ and g_i primitive forms, then $f_1 \sim f_2$ if and only if $g_1 \sim g_2$ and the ideals $b_1 R$ and $b_2 R$ are equal. There is a classification of quadratic lattices in the local case which we will use below. See [28] Sections 92 and 93 for details.

In the non-dyadic case every form is isometric to a diagonal form, but this is not true in the 2-adic case. We define the 2-dimensional quadratic forms h_1 and h_2 with the corresponding matrices

$$h_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; h_2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Proposition 2.3.13 *Let f be a primitive ternary quadratic form over R. If P is a non-dyadic prime, then $f \sim x_0^2 + \delta\pi^r x_1^2 + \gamma\pi^s x_2^2$.*

If $P = 2R$ then $f \sim f_i$ for some $1 \leq i \leq 5$, where $\gamma,\ \delta \in R^*$ and $0 \leq r \leq s$ such that

$$\begin{aligned} f_1(r,s) &= x_0^2 + \delta 2^r x_1^2 + \gamma 2^s x_2^2 \\ f_2(r) &= x_0^2 + 2^r h_1 \\ f_3(r) &= h_1 + 2^r x_2^2 \\ f_4(r) &= x_0^2 + 2^r h_2 \\ f_5(r) &= h_2 + 2^r x_2^2 \end{aligned}$$

In the sequel these quadratic forms will be called standard forms.

Proof Since we may multiply f by elements in R^*, the proposition follows from the results in [28]. □

The only cases in Proposition 2.3.13 when any of the non-diagonal forms $f_2, \ldots, f_5$ are similar to a diagonal form are

$$x_0^2 + 2h_1 \sim x_0^2 + x_1^2 - x_2^2 \quad \text{and} \quad x_0^2 + 2h_2 \sim x_0^2 + x_1^2 + x_2^2. \tag{2.2}$$

Furthermore we also have

$$f_2(0) = f_3(0) \sim f_4(0) = f_5(0) \text{ and } f_2(2) \sim f_4(2). \tag{2.3}$$

However $f_i \not\sim f_j$ if $i \neq j$ for all except the above cases. The following Proposition gives us a simple criteria on f whether $\mathrm{Cliff}_0(f)$ is a Bass order or not.

Proposition 2.3.14 *If P is non-dyadic and $f \sim x_0^2 + \delta\pi^r x_1^2 + \gamma\pi^s x_2^2$ with $r \leq s$, then $\mathrm{Cliff}_0(f)$ is a Bass order if and only if $r \leq 1$.*
If $P = 2R$ then $\mathrm{Cliff}_0(f)$ is a Bass order if and only if f is similar to any of the forms

(a) $x_0^2 + \delta x_1^2 + \gamma 2^r x_2^2$, with $\delta \equiv 1 \bmod 4$ or $r \leq 1$,

(b) $x_0^2 + \delta 2 x_1^2 + \gamma 2^r x_2^2$,

(c) $f_3(r)$ or

(d) $f_5(r)$

Proof It follows from the definition of the norm form for $\mathrm{Cliff}_0(f)$ that if $f = x_0^2 + \delta\pi^r x_1^2 + \gamma\pi^s x_2^2$ then the norm form on $\mathcal{O} = \mathrm{Cliff}_0(f)$ is given by $x_0^2 + \delta\pi^r x_1^2 + \gamma\pi^s x_2^2 + \delta\gamma\pi^{r+s} x_3^2$. It is easy to see that $\mathcal{O}$ contains a primitive element (and hence is a Bass order) exactly in the cases in the Proposition. The non-diagonal cases are analogous. □

If we have a standard form f, then it is easy to calculate the Eichler invariant of $\mathrm{Cliff}_0(f)$. A direct computation gives us the following result.

Proposition 2.3.15 *If $\mathcal{O} = \mathrm{Cliff}_0(f)$, then the Eichler invariant $\mathrm{E}_{\mathrm{inv}}(\mathcal{O})$ satisfies:*

(a) If P is non-dyadic and $f \sim x_0^2 + \delta\pi^r x_1^2 + \gamma\pi^s x_2^2$ with $r \leq s$ then:

(i) $\mathrm{E}_{\mathrm{inv}}(\mathcal{O}) = 1$ *if and only if* $r = 0$, $s \geq 1$ *and* $\omega_P(-\delta) = 1$.

(ii) $\mathrm{E}_{\mathrm{inv}}(\mathcal{O}) = -1$ *if and only if* $r = 0$, $s \geq 1$ *and* $\omega_P(-\delta) = -1$.

(b) If $P = 2R$ *then:*

(i) $\mathrm{E}_{\mathrm{inv}}(\mathcal{O}) = 1$ *if and only if* $f \sim h_1 + 2^r x_2^2$ *for* $r \geq 1$.

(ii) $\mathrm{E}_{\mathrm{inv}}(\mathcal{O}) = -1$ *if and only if* $f \sim h_2 + 2^r x_2^2$ *for* $r \geq 1$. □

Next we will give a set of primitive ternary quadratic forms T such that

$$S = \{\mathrm{Cliff}_0(f) |\ f \in T\}$$

is a set of all isomorphism classes of Gorenstein R-orders in L. Then

$$M = \{\mathrm{Cliff}_0(\pi^b f) |\ f \in T,\ b \geq 0\}$$

is a set of representatives of all isomorphism classes of R-orders. One of the advantages of this description is that it is very well suited for explicit calculations, since f in standard form gives a convenient basis of $\mathrm{Cliff}_0(f)$.

Proposition 2.3.16 *Let P be a non-dyadic prime and let $\mathcal{O}$ be a Gorenstein R-order in a quaternion algebra L over K. Then $\mathcal{O} \cong \mathrm{Cliff}_0(f)$, where f is uniquely chosen among the following quadratic forms:*

(a) $x_0^2 + x_1^2 + x_2^2$

(b) $x_0^2 - \gamma_1 x_1^2 + \pi^s x_2^2$, $s \geq 1$

(c) $x_0^2 + \pi^r x_1^2 + \gamma_1 \pi^r x_2^2$, $r \geq 1$

(d) $x_0^2 + \gamma_1 \pi^r x_1^2 + \gamma_2 \pi^s x_2^2$, $s > r \geq 1$

Here γ_1 and γ_2 are to be chosen arbitrarily in $\{1, \delta\}$ where $\omega_P(\delta) = -1$.

Pectora roborant cultus recti

Proof If $f_1 = x_0^2 + \delta_1 \pi^{r_1} x_1^2 + \gamma_1 \pi^{s_1} x_2^2 \sim f_2 = x_0^2 + \delta_2 \pi^{r_1} x_1^2 + \gamma_2 \pi^{s_1} x_2^2$ then $r_1 = r_2$, $s_1 = s_2$. Conversely let $r_1 = r_2$, $s_1 = s_2$, $\omega_P(\delta_1) = \omega_P(\delta_2)$ and $\omega_P(\gamma_1) = \omega_P(\gamma_2)$, then $f_1 \sim f_2$ Hence, we have at most 4 different classes given r and s. But if $r = 0$ or $r = s$, then the number of classes is divided by 2 (see [28]). □

With Proposition 2.3.14 and Proposition 2.3.16 at hand, we are able to determine the number of isomorphism classes of Bass R-orders and Gorenstein R-orders with given discriminant.

Proposition 2.3.17 *Let P be a non-dyadic prime, let $t(n)$ denote the number of isomorphism classes of R-orders with discriminant P^n and let $g(n)$ denote the number of isomorphism classes of Gorenstein R-orders with discriminant P^n. Then*

$$t(n) = g(n) + t(n-3).$$

Proof An R-order $\mathcal{O}$ is either Gorenstein or else $\mathcal{O} = R + P\Lambda$ with $[\Lambda : \mathcal{O}] = P^3$. Moreover of $\mathcal{O}_1 = R + P\Lambda_1$ and $\mathcal{O}_2 = R + P\Lambda_2$, then $\mathcal{O}_1 \cong \mathcal{O}_2$ if and only if $\Lambda_1 \cong \Lambda_2$. The linear recursion $t(n) = g(n) + t(n-3)$ is easy to solve, since $g(n)$ proves to be more or less a linear function. □

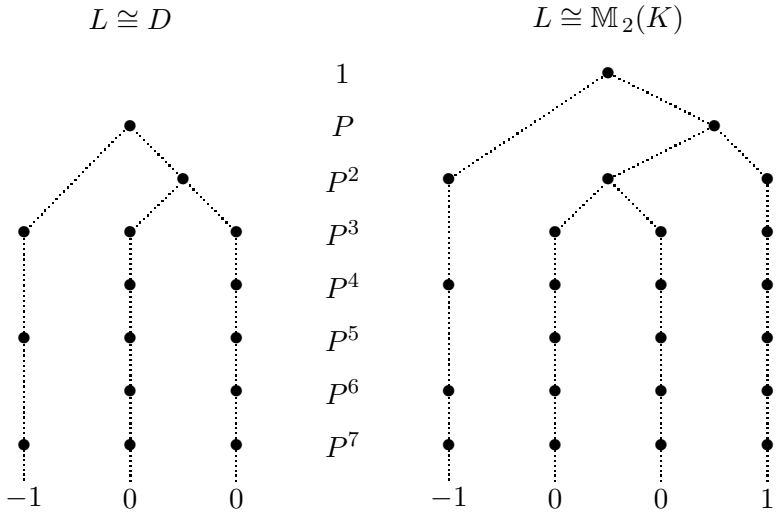
We summarise everything in the table below. We give the number of isomorphism classes of R-orders when P is a non-dyadic prime and separate R-orders in the case where $L \cong D$ is a division algebra and the case where $L \cong \mathbb{M}_2(K)$. The variables n and α in the table satisfies

$$n \geq 3 \text{ and } \alpha = \begin{cases} \frac{1}{3} & \text{if } n \equiv 0 \bmod 3 \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

	Bass		Gorenstein		Totally	
Discriminant	D	$\mathbb{M}_2(K)$	D	$\mathbb{M}_2(K)$	D	$\mathbb{M}_2(K)$
1	0	1	0	1	0	1
P	1	1	1	1	1	1
P^2	1	3	1	3	1	3
P^n, n odd	3	3	n	n	$\frac{1}{8}(n^2+4n+3)$	$\frac{1}{24}(5n^2+12n+7)+\alpha$
P^n, n even	2	4	$\frac{n}{2}$	$\frac{3n}{2}$	$\frac{1}{8}(n^2+2n)$	$\frac{1}{24}(5n^2+18n+16)+\alpha$

If we restrict to Bass R-orders then we can also very easily draw conclusions on the relations between the classes by using results first proved by Eichler. We illustrate these relations by trees. Every node in a tree represents an isomorphism class of Bass orders. Different isomorphism classes with the same discriminant are on the same level. There is an edge between nodes N_1 and N_2 if and only if given $\mathcal{O}_1 \in N_1$, then there exists $\mathcal{O}_2 \in N_2$ such that $\mathcal{O}_1$ is a maximal R-suborder in $\mathcal{O}_2$ or vice versa. The number at the bottom are the Eichler invariant of the R-orders in that column. Moreover the R-order $\mathcal{O}$ in the division algebra $D \cong L$ with discriminant $\overline{\text{disc}}(\mathcal{O}) = P$ is the maximal R-order and has $\text{E}_{\text{inv}}(\mathcal{O}) = 1$.

The figure below give the trees of isomorphism classes of Bass R-orders in the non-dyadic case.



We now turn to the 2-adic case.

Proposition 2.3.18 *Let $P = 2R$ and let $\mathcal{O}$ be a Gorenstein R-order in a quaternion algebra over K. Then $\mathcal{O} \cong \mathrm{Cliff}_0(f)$, where f is uniquely chosen among the quadratic forms in the following table:*

1.	$h_1 + 2^r x_2^2$, $r \geq 0$	*12.*	$x_0^2 + \gamma_4 2^2 x_1^2 + \gamma_4 2^r x_2^2$, $r \geq 2$
2.	$h_2 + 2^r x_2^2$, $r \geq 1$	*13.*	$x_0^2 + 2^2 x_1^2 + (3 \cdot 2^r) x_2^2$, $r \geq 2$
3.	$x_0^2 + 2^r h_1$, $r \geq 2$	*14.*	$x_0^2 + (3 \cdot 2^2) x_1^2 + 2^r x_2^2$, $r \geq 3$
4.	$x_0^2 + 2^r h_2$, $r \geq 3$	*15.*	$x_0^2 + \gamma_7 2^2 x_1^2 + (7 \cdot 2^r) x_2^2$, $r \geq 5$
5.	$x_0^2 + x_1^2 + \gamma_1 2^r x_2^2$, $r \geq 0$	*16.*	$x_0^2 + \gamma_2 2^2 x_1^2 + 2^r x_2^2$, $r \geq 5$
6.	$x_0^2 + 3x_1^2 + 2^r x_2^2$, $r \geq 2$	*17.*	$x_0^2 + 2^r x_1^2 + \gamma_5 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 0$
7.	$x_0^2 + 7x_1^2 + 2^r x_2^2$, $r \geq 3$	*18.*	$x_0^2 + (7 \cdot 2^r) x_1^2 + \gamma_6 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 0$
8.	$x_0^2 + 5x_1^2 + \gamma_1 2^r x_2^2$, $r \geq 3$	*19.*	$x_0^2 + (3 \cdot 2^r) x_1^2 + \gamma_3 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 1$
9.	$x_0^2 + (3 \cdot 2) x_1^2 + \gamma_1 2^r x_2^2$, $r \geq 1$	*20.*	$x_0^2 + (7 \cdot 2^r) x_1^2 + \gamma_3 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 3$
10.	$x_0^2 + 2x_1^2 + \gamma_3 2^r x_2^2$, $r \geq 3$	*21.*	$x_0^2 + (3 \cdot 2^r) x_1^2 + \gamma_6 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 3$
11.	$x_0^2 + \gamma_2 2x_1^2 + \gamma_3 2^r x_2^2$, $r \geq 4$	*22.*	$x_0^2 + (5 \cdot 2^r) x_1^2 + \gamma_5 2^{r+s} x_2^2$, $r \geq 3$, $s \geq 3$

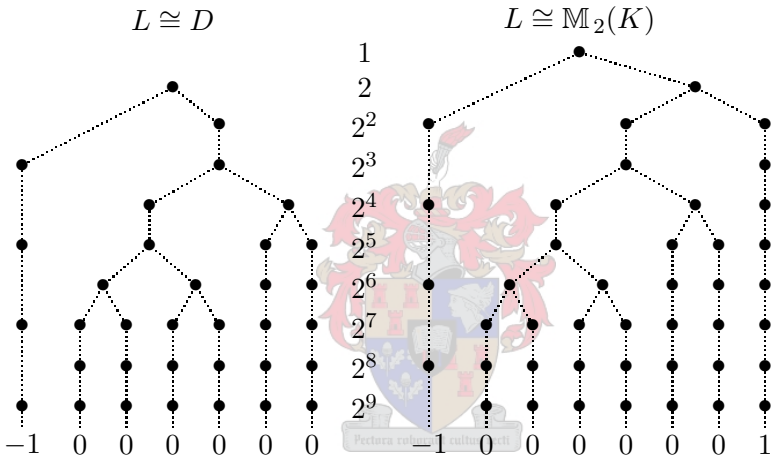
Proof For the diagonal forms we have as in the non-dyadic case $f_1 \sim x_0^2 + \gamma_1 \pi^{r_1} x_1^2 + \epsilon_1 \pi^{s_1} x_2^2 \sim f_2 = x_0^2 + \gamma_2 \pi^{r_2} x_1^2 + \epsilon_2 \pi^{s_2} x_2^2$ which implies that $r_1 \sim r_2$, $s_1 = s_2$, $\gamma_1 \equiv \gamma_2 \bmod 8$ and $\epsilon_1 \equiv \epsilon_2 \bmod 8$, then $f_1 \sim f_2$. Hence we get at most 16 classes for every pair (r, s). But if $r < 3$ or $s - r < 3$, then the number of classes is reduced.
The table in the statement gives the representatives of the similarity classes of primitive ternary quadratic forms over the 2-adic integers. The γ_i's are to be chosen arbitrarily according to $\gamma_1 \in \{1, 3\}$, $\gamma_2 \in \{5, 7\}$, $\gamma_3 \in \{1, 5\}$, $\gamma_4 \in \{1, 7\}$, $\gamma_5 \in \{1, 3, 5, 7\}$, $\gamma_6 \in \{3, 7\}$ and $\gamma_7 \in \{3, 5\}$. For example nr.11 in the table gives rise to 4 classes for every $r \geq 4$, namely $(\gamma_2, \gamma_3) \in \{(5, 1), (5, 5), (7, 1), (7, 5)\}$. The only relations for the non-diagonal forms are given by (2.2) and (2.3). □

We conclude using Proposition 2.3.14 that the Bass R-orders are those in $\{1, 2, 5, 8, 9, 10, 11\}$. Now with Proposition 2.3.18 at our disposal, we can determine the number of isomorphism classes of R-orders in the 2-adic case. This is summarized in the table below. The numbers n and β satisfy

$$n \geq 9 \text{ and } \beta = \begin{cases} \frac{1}{3} & \text{if } n \equiv 2 \bmod 3 \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

	Bass		Gorenstein		Totally	
Discriminant	D	$\mathbb{M}_2(K)$	D	$\mathbb{M}_2(K)$	D	$\mathbb{M}_2(K)$
1	0	1	0	1	0	1
2	1	1	1	1	1	1
2^2	1	3	1	3	1	3
2^3	2	2	2	2	2	3
2^4	2	4	2	6	3	7
2^5	4	4	5	5	6	8
2^6	4	6	6	11	8	14
2^7	7	7	10	10	13	17
2^8	6	8	10	18	16	26
2^n, n odd	7	7	$4(n-5)$	$4(n-5)$	$\frac{1}{12}(7n^2-46n+135)+\beta$	$\frac{1}{4}(3n^2-22n+75)+3\beta$
2^n, n even	6	8	$3(n-5)$	$5(n-5)$	$\frac{1}{12}(7n^2-52n+156)+\beta$	$\frac{1}{4}(3n^2-20n+68)+3\beta$

The trees of isomorphism classes of Bass orders in the 2-adic case is shown below.



Maximal orders

Here we will make a connection between quaternion algebras over P-adic fields and quaternion algebras over number fields. At the end of this section we will give an explicit basis of a maximal order when the discriminant of the algebra is a principle ideal.

We let K be an algebraic number field with ring of integers R. A powerful tool when studying orders in quaternion algebras over algebraic number fields is to consider completions $\mathcal{O}_P = \mathcal{O} \otimes_R R_P$ with respect to the prime ideals in R. The basic result which makes this so useful is the following local-global correspondence.

Proposition 2.3.19 *If $\mathcal{O}$ is a R-lattice in the quaternion K-algebra L, then there is a bijection between $\{\Lambda \mid \Lambda$ is a $R-$lattice in $L\}$ and $\{\Lambda_P \mid P \in \Omega_f$, Λ_P is a R_P-lattice in L_P, $\mathcal{O}_P = \Lambda_P$ for almost all $P\}$ given by $\Lambda \mapsto \Lambda_P$ and $\Lambda_P \mapsto \Lambda = \{a \in L \mid a \in \Lambda_P,\ \forall P \in \Omega_f\}$.*

Proof See [38] Proposition 5.1 □

The local-global principle remains true if we restrict to R-orders, since $\mathcal{O}$ is an R-order if and only if $\mathcal{O}_P$ is a R_P-order for all $P \in \Omega_f$. It is immediate from the definitions that the index and discriminant satisfy

$$\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})_P = \overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}_P) \text{ and } [\Lambda_P : \mathcal{O}_P] = [\Lambda : \mathcal{O}]_P.$$

A direct consequence of Proposition 2.3.19 is that $\mathcal{O}$ is maximal if and only if $\mathcal{O}_P$ is maximal for all $P \in \Omega_f$. From this and Proposition 2.3.12 we get that $\mathcal{O}$ is maximal in L if and only if $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \overline{\mathrm{d}}\mathrm{isc}(L)$. It is also clear that $\mathcal{O}$ is a Bass (Gorenstein) R-order if and only if $\mathcal{O}_P$ is a Bass (Gorenstein) R-order for all $P \in \Omega_f$.

As already metioned, the local-global principle does not apply to isomorphism classes since $\mathcal{O}_P \cong \Lambda_P,\ \forall P \in \Omega_f$ does not imply $\mathcal{O} \cong \Lambda$ in general. We say that $\mathcal{O}$ and Λ are in the same genus if $\mathcal{O}_P \cong \Lambda_P,\ \forall P \in \Omega_f$, and that they are of the same type if $\mathcal{O} \cong \Lambda$. The number of types (isomorphism classes) in the same genus as $\mathcal{O}$ is called the type number of $\mathcal{O}$ and will be denoted by $\mathrm{t}(\mathcal{O})$.

Closely related to $\mathrm{t}(\mathcal{O})$ are the one- and two-sided class numbers of $\mathcal{O}$, which are defined as follows. Take the set of locally principle left $\mathcal{O}$-ideals. We define an equivalence relation on by $\Lambda_1 \equiv \Lambda_2$ if and only if there exists a $\lambda \in L$ such that $\Lambda_1 = \Lambda_2\lambda$. The number of equivalence classes in with respect to this relation is the one-sided class number $\mathrm{h}(\mathcal{O})$ of $\mathcal{O}$. In the literature this is simple referred to as the class number of $\mathcal{O}$. The fact that $\mathrm{h}(\mathcal{O}) < \infty$ and that we get the same number of classes if we take right ideals instead where proved by Brandt.

If we restrict to two-sided ideals instead and do the same construction, then the number of equivalence classes is called the two-sided class number of $\mathcal{O}$ and will be denoted by $\tilde{\mathrm{h}}(\mathcal{O})$.

We remark that there do exists R-orders with ideals which is not locally principle.

Example Let $P = \pi R$ be a principle ideal in R and $\mathcal{O} = (\pi, \pi)_R$. If

$$\Lambda = \{\alpha \in \mathcal{O} \mid \overline{\mathrm{n}}\mathrm{orm}(\alpha) \in P\} = P + Ri + Rj + Rij,$$

then clearly Λ is a two-sided $\mathcal{O}$-ideal. Furthermore $[\mathcal{O} : \Lambda] = P$ and $\Lambda = \mathcal{O}i + \mathcal{O}j$. If $g = \pi\alpha + \beta i + \gamma j + \delta ij \in \Lambda_P$, then

$$\begin{bmatrix} g\cdot 1 \\ g\cdot i \\ g\cdot j \\ g\cdot ij \end{bmatrix} = \begin{bmatrix} \pi\alpha & \beta & \gamma & \delta \\ \pi\beta & \pi\alpha & -\delta & -\gamma \\ \pi\gamma & \pi\delta & \pi\alpha & \beta \\ -\pi^2\delta & -\pi\gamma & \pi\beta & \pi\alpha \end{bmatrix} \begin{bmatrix} 1 \\ i \\ j \\ ij \end{bmatrix} = A \begin{bmatrix} 1 \\ i \\ j \\ ij \end{bmatrix}.$$

Hence $[\mathcal{O}_P : \mathcal{O}_P g] = \det(A) \cdot R \subseteq P^2$ and this implies that Λ_P is not principle since $[\mathcal{O}_P : \Lambda_P] = P$. □

Proposition 2.3.20 *Let $\mathcal{O}$ be an arbitrary R-order in a quaternion algebra L over K. Then*

$$\mathrm{h}(\mathcal{O}) = \sum_{i=1}^{\mathrm{t}(\mathcal{O})} \tilde{\mathrm{h}}(\mathcal{O}_i),$$

where $\mathcal{O}_1, \ldots, \mathcal{O}_{\mathrm{t}(\mathcal{O})}$ are the set of representatives of the types which are in the same genus as $\mathcal{O}$. In particular $\mathrm{h}(\mathcal{O}) = \mathrm{h}(\Gamma)$ if $\mathcal{O}$ and Γ are in the same genus.

Proof Let $\Lambda_1, \ldots, \Lambda_{\mathrm{h}(\mathcal{O})}$ be the set of representatives of left $\mathcal{O}$-ideal classes. Then every R-order in the genus of $\mathcal{O}$ is isomorphic to at least one of the right R-orders $\mathrm{O}_{\mathrm{right}}(\Lambda_i)$. In fact if Γ is in the genus of $\mathcal{O}$, then Γ is isomorphic to exactly $\tilde{\mathrm{h}}(\Gamma)$ of the right R-orders $\mathrm{O}_{\mathrm{right}}(\Lambda_i)$. □

Some confusion on notions of class numbers regarding quadratic forms versus quaternion orders might arise. Let $\overline{\mathrm{n}}\mathrm{orm}$ be the norm form of an order $\mathcal{O}$. The class number of the quadratic form $\overline{\mathrm{n}}\mathrm{orm}$ is defined to be the number of isometry classes in the genus of $\overline{\mathrm{n}}\mathrm{orm}$, that is, forms locally isometric to $\overline{\mathrm{n}}\mathrm{orm}$. Hence the class number of $\overline{\mathrm{n}}\mathrm{orm}$ is equal to the type number of $\mathcal{O}$.

Moreover if L is a not totally definite quaternion algebra over a number field K, and $\mathcal{O}$, an arbitrary R-order contained in a maximal R-order, $\mathcal{O}_L$, then we can express the class number of $\mathcal{O}$ as

$$\begin{aligned} \mathrm{h}(\mathcal{O}) &= \mathrm{h}(\mathcal{O}_L)\frac{\prod_P[(\mathcal{O}_L)_P^* : \mathcal{O}_P]}{[\mathcal{O}_L : \mathcal{O}]} \\ &= \mathrm{h}(\mathcal{O}_L)\frac{\prod_P[R_P^* : \overline{\mathrm{n}}\mathrm{orm}_{L_P/K_P}(\mathcal{O}_P*)]}{[\overline{\mathrm{n}}\mathrm{orm}(\mathcal{O}_L^*) : \overline{\mathrm{n}}\mathrm{orm}(\mathcal{O}^*)]}. \end{aligned}$$

We finish this section of by giving an explicit basis of a maximal R-order in an arbitrary quaternion algebra L over K such that the discriminant $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = dR$ is principle.

Theorem 2.3.21 *Let L be a quaternion algebra over a number field K. A maximal R-order $\mathcal{O}$ in L can be constructed explicitly such that the R-order $(a,-d)_R$ has index $4aR$ in $\mathcal{O}$.*

Proof First choose a generator a of a prime ideal satisfying the conditions of Proposition 2.3.7 so that $L \cong (a,-d)_K$. We start with the order $\Lambda = (a,-d)_R$, which has $\overline{\mathrm{d}}\mathrm{isc}(\Lambda) = 4abR$. Since $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \overline{\mathrm{d}}\mathrm{isc}(\Lambda)[\Lambda : \mathcal{O}]$ and since $\mathcal{O}$ is maximal in L if and only if $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \overline{\mathrm{d}}\mathrm{isc}(L)$ we get that a R-order $\mathcal{O}$ which satisfies $\Lambda \subseteq \mathcal{O}$ is maximal if and only if $[\mathcal{O} : \Lambda] = 4aR$. The last condition in Proposition 2.3.7 implies that $\exists c \in R \ : \ a \equiv c^2 \bmod 4$. We have $\left(\frac{-d}{a}\right) = 1$, since L is not ramified at a, and hence $\exists m : \ -d \equiv m^2 \bmod a$. Now if $e_1 = \frac{c+i}{2}$ and $e_2 = \frac{mi+ij}{a}$, then the norms and traces of e_1, e_2 and their products belong to R, since

$$\begin{array}{ll} \overline{\mathrm{n}}\mathrm{orm}(e_1) = \frac{c^2-a}{4}, & \overline{\mathrm{t}}\mathrm{race}(e_1) = c, \\ \overline{\mathrm{n}}\mathrm{orm}(e_2) = -\frac{d+m^2}{a}, & \overline{\mathrm{t}}\mathrm{race}(e_2) = 0, \end{array} \quad \text{and} \quad \overline{\mathrm{t}}\mathrm{race}(e_1e_2) = m.$$

Hence we get $\mathcal{O} = \langle 1, e_1, e_2, e_1e_2\rangle$ is an R-order. The matrix which takes $\{1,i,j,ij\}$ to $\{1,e_1,e_2,e_1e_2\}$ has determinant equal to $\frac{1}{4a}$. Hence $[\mathcal{O} : \Lambda] = 4aR$ and we have proven the

statement. □

We remind the reader that there might be many non-isomorphic maximal orders in L. However if L is a totally indefinite quaternion algebra over a field K of class number 1, then the maximal order is unique up to isomorphism.

Example As an example, we will determine the number of isomorphism classes of orders $\mathcal{O}$ in rational quaternion algebras with $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \langle 72 \rangle$. If $\mathcal{O}$ is an order in an quaternion algebra L, then $\overline{\mathrm{d}}\mathrm{isc}(L)$ divides $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})$. Since the discriminant determines the rational quaternion algebra, we get 4 possibilities: $\overline{\mathrm{d}}\mathrm{isc}(L) \in \{1, 2, 3, 6\}$. The cases $\overline{\mathrm{d}}\mathrm{isc}(L) \in \{2, 3\}$ are definite algebras and the other two are indefinite. We get that there is 1 isomorphism class of orders with $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}_3) = \langle 72 \rangle = \langle 3^2 \rangle$ in the divisional case and 4 in $\mathbb{M}_2(\mathbb{Q}_3)$. Further there are 2 isomorphism classes of orders with $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}_2) = \langle 72 \rangle = \langle 2^3 \rangle$ in the divisional case and 3 in $\mathbb{M}_2(\mathbb{Q}_2)$. Of all these orders only one is not Gorenstein or Bass. □

Quadratic modules

Let R be an integral domain with field of fractions K. In this section we look at quadratic spaces and quadratic modules derived from quaternion algebras over K. We will restrict to studying four dimensional regular quadratic spaces (V, q_V) over K such that $\det(V, q_V)$ is trivial in K^*/K^{*2}. By Theorem 2.2.2 the K-algebra $\mathrm{Cliff}(V)$ is isomorphic to a matrix algebra over a quaternion K-algebra L, which might be split, and $\mathrm{Cliff}_0(V)$ is isomorphic to two copies of L. This enables up to characterize the quadratic modules arising from projective modules over R-orders in L.

We are interrested in quadratic modules over R in the sets

$$S = \{(M, q_M) \mid \exists \text{ a pair } (\mathcal{O}, \mathcal{O} \times M \to M)\}$$

where $\mathcal{O}$ is a R-order in a quaternion algebra over K and $\mathcal{O} \times M \to M$ a left $\mathcal{O}$-module structure on M such that, as $\mathcal{O}$-module, M is projective and of rank 1.

Theorem 2.3.22 *Let (M, q_M) be quaternary quadratic module over R contained in (V, q_V) such that $q_M(M)$ is not contained in any proper ideal of R. Let e be a nontrivial central idempotent of $\mathrm{Cliff}_0(V)$. Then $(M, q_M) \in S$ if and only if the following equivalent statements hold true.*

(a) $eM = e\mathrm{Cliff}_1(M)$.

(b) eM is a projective left $e\mathrm{Cliff}_0(M)$-module.

(c) Me is a projective right $e\mathrm{Cliff}_0(M)$-module.

(d) eMa is a fractional left ideal of $e\mathrm{Cliff}_0(M)$ for all $a \in M$.

(e) eMa is a fractional left ideal of $e\mathrm{Cliff}_0(M)$ for some $a \in M$.

(f) aMe is a fractional right ideal of $e\mathrm{Cliff}_0(M)$ for some $a \in M$.

Proof See [23] Proposition 61. □

If we restrict to quadratic modules (M, q_M) over R satisfying the equivalent conditions of Theorem 2.3.22 we can find an invariant of the quaternary quadratic module (M, q_M). More precisely for a choice of idempotent e we define the left order of (M, q_M) as $\mathrm{O}_{\mathrm{left}}(M, q_M) = e\mathrm{Cliff}_0(M)$ and the right order as $\mathrm{O}_{\mathrm{right}}(M, q_M) = \hat{e}\mathrm{Cliff}_0(M)$.

M is a projective left $\mathrm{O}_{\mathrm{left}}(M, q_M)$-module and by symmetry we have that M is a projective right $\mathrm{O}_{\mathrm{right}}(M, q_M)$-module. For any such quadratic module $(M, q_M) \in S$ there exists precisely two different pairs $(\mathcal{O}, \mathcal{O} \times M \to M)$ such that q_M respects the $\mathcal{O}$-module stucture, $\mathcal{O} \times M \to M$. That is $q_M(au) = \overline{\mathrm{n}}\mathrm{orm}(a)q_M(u)$ for all $a \in \mathcal{O},\ u \in M$.

These pairs are dual to one another in the sense that $\mathrm{O}_{\mathrm{left}}(M, q_M)$ under the first structure is equal to $\mathrm{O}_{\mathrm{right}}(M, q_M)$ under the second stucture. Thus $(\mathrm{O}_{\mathrm{left}}(M, q_M), \mathrm{O}_{\mathrm{right}}(M, q_M))$ is thus an invariant of the quaternary quadratic module (M, q_M). In the next section we go further and look at the structure of $\mathcal{O}$-modules viewed as modules over commutative subrings.

Optimal embeddings

Gauss showed that if K is an imaginary quadratic field extension of $\mathbb{Q}$ of discriminant d different from -3 and -4 then the number of times d can be represented by a quadratic form

$$q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 \text{ equals either } \begin{cases} 12 \cdot \mathrm{h}(K) & \text{if } d \equiv 0 \bmod 4, \text{ or} \\ 24 \cdot \mathrm{h}(K) & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

Eichler interpreted this in terms of the number of embeddings of $\mathbb{Z}$-orders in imaginary quadratic extensions of $\mathbb{Q}$ into the maximal $\mathbb{Z}$-orders of quaternion algebras over $\mathbb{Q}$.

Let $\mathcal{O}$ be a maximal order in a definite quaternion algebra L over $\mathbb{Q}$. A subring R of $\mathcal{O}$ is said to be optimally embedded if $\mathcal{O}/R$ is torsion-free.

Theorem 2.3.23 *If $R \to \mathcal{O}$ is an optimal embedding of rank 2 commutative subring R in $\mathcal{O}$, then the exact sequence of left R-modules*

$$0 \to R \to \mathcal{O} \to \mathcal{O}/R \to 0$$

splits and the cokernel $\mathcal{O}/R$ is projective as a left R-module. In particular $\mathcal{O}$ is projective as a left R-module over every optimally embedded subring R.

Proof See [23] Theorem 66. □

Theorem 2.3.24 *Let (M, q_M) be a quadratic module over $\mathbb{Z}$ with associated left $\mathcal{O}$-module structure making M into a projective rank 1 left $\mathcal{O}$-module. Let (N, q_N) be a binary quadratic $\mathbb{Z}$-submodule such that $q_N(N)$ is not contained in any proper ideal of $\mathbb{Z}$ and such that the quotient M/N is a torsion-free $\mathbb{Z}$-module. Then*

(a) $\overline{\mathrm{d}}\mathrm{isc}(\mathrm{O}_{\mathrm{left}}(N, q_N)) = \det(M, q_M)$.

(b) $\mathrm{O}_{\mathrm{left}}(N, q_N)$ *optimally embeds into* $\mathrm{O}_{\mathrm{left}}(M, q_M)$ *and* $\mathrm{O}_{\mathrm{right}}(M, q_M)$.

(c) The exact sequence of left $\mathrm{O}_{\mathrm{left}}(N, q_N)$*-modules*

$$0 \to N \to M \to M/N \to 0$$

splits and the cokernel M/N *is a projective left* $\mathrm{O}_{\mathrm{left}}(N, q_N)$*-module. In particular* M *is a projective left* $\mathrm{O}_{\mathrm{left}}(N, q_N)$*-module.*

Proof See [23] Theorem 67. □

In the case of the quadratic form q of Gauss, the number of representations of a number d can be interpreted as the number of embeddings of a $\mathbb{Z}$-order in K into a maximal $\mathbb{Z}$-order, of the definite quaternion algebra L over $\mathbb{Q}$ ramified at 2 and ∞ and it follows that every $\mathbb{Z}$-order which optimally embeds into a maximal $\mathbb{Z}$-order of L does so in $\mathcal{O}$.

Redused norm forms and determinants

Suppose L be a quaternion algebra over a $\mathbb{Q}$. For any finite prime ℓ in K. If L_ℓ is a division algebra over $\mathbb{Q}_\ell$ then there is a unique maximal $\mathbb{Z}_\ell$-order. If L_ℓ is isomorphic to $\mathbb{M}_2(\mathbb{Q}_\ell)$, then all maximal orders are conjugate to $\mathbb{M}_2(\mathbb{Z}_\ell)$ under this isomorphism.

Suppose that $\mathcal{O}$ is a maximal $\mathbb{Z}$-order in L. Then every integral left ideal of $\mathcal{O}_\ell$ is principle at all finite primes ℓ ([29] Theorem 17.3.) and it follows that an integral left $\mathcal{O}$-ideal is projective if and only at each finite prime ℓ, $M_\ell = \mathcal{O}_\ell\alpha_\ell$ for some invertible element $\alpha_\ell \in L^*$. So an integral left $\mathcal{O}$-ideal is projective if and only if it is locally free at all finite primes.

If M is a projective fractional left $\mathcal{O}$-ideal, we define the reduced norm of M as the positive integer

$$\overline{\mathrm{n}}\mathrm{orm}(M) = \prod_\ell \#(\mathbb{Z}_\ell/\langle\, \overline{\mathrm{n}}\mathrm{orm}(\alpha_\ell) \mid \alpha_\ell \in M_\ell \,\rangle)$$

where the product ranges over all finite primes ℓ.

If M is a projective fractional left $\mathcal{O}$-ideal. Then the right order $\mathrm{O}_{\mathrm{right}}(I)$ is a maximal $\mathbb{Z}$-order in L. If $\Lambda_1, \ldots, \Lambda_{\mathrm{h}(\mathcal{O})}$ is a complete set of representatives of fractional left $\mathcal{O}$-ideal classes, then the set of right orders $\mathrm{O}_{\mathrm{right}}(\Lambda_1), \ldots, \mathrm{O}_{\mathrm{right}}(\Lambda_{\mathrm{h}(\mathcal{O})})$ represent all the isomorphism classes of maximal $\mathbb{Z}$-orders in L.

Let M be a projective left $\mathcal{O}$-module of rank one. We can define the reduced norm map on elements in M from the reduced norm map on the $\mathbb{Z}$-order $\mathcal{O}$. For each finite prime ℓ, fix a generator α_ℓ for M_ℓ as a $\mathcal{O}_\ell$-module. Then each α in M is of the form $\alpha_\ell\lambda_\ell$ for some λ_ℓ in $\mathcal{O}_\ell$ Since α_ℓ is defined up to an element in $\mathcal{O}_\ell^*$ and $\overline{\mathrm{n}}\mathrm{orm}(\mathcal{O}_\ell^*) = \mathbb{Z}_\ell^*$. We define the reduced norm on elements α in M as

$$\begin{array}{rccl} \overline{\mathrm{n}}\mathrm{orm}: & M & \to & \mathbb{Z} \\ & \alpha & \mapsto & \overline{\mathrm{n}}\mathrm{orm}(\alpha_\ell) \bmod \mathbb{Z}_\ell^*. \end{array}$$

Note that since L is definite at ∞, we have that the image of the reduced norm on $L \otimes \mathbb{R}$ is contained in the positive part of $\mathbb{R}$. So the reduced norm on elements, $\alpha \in M$ is the unique positive generator of $\cap_\ell(\overline{\mathrm{n}}\mathrm{orm}(\alpha_\ell)\mathbb{Z} \cap \mathbb{Z})$.

Proposition 2.3.25 *Let $\mathcal{O}$ be a maximal order in a definite quaternion algebra L over $\mathbb{Q}$ and let M be a projective left $\mathcal{O}$-module of rank one. Consider the quadratic map $q_M = \overline{\mathrm{n}}\mathrm{orm}$ on elements in M. We have $\det(M, q_M) = \overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})^2$ and any isomorphism with a fractional $\mathcal{O}$-ideal N determines a similitude $\varphi : M \to \mathcal{O}$ with similitude factor $\overline{\mathrm{n}}\mathrm{orm}(N)$.*

Proof The reduced norm on M, $\overline{\mathrm{n}}\mathrm{orm}$, is defined using the local isomorphism $M_\ell \cong \mathcal{O}_\ell$. Thus $\det(M_\ell) = \det(\mathcal{O}_\ell) \bmod \mathbb{Z}_\ell^{*2}$ for all ℓ and thus the two determinants are equal. But since $\mathcal{O}$ is maximal we have that both determinants are equal to $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O})^2$. Thus the reduced norm on $\mathcal{O}$, restricted to elements of N, is given by $\overline{\mathrm{n}}\mathrm{orm}(N)$ times the reduced norm on elements in N defined by it left $\mathcal{O}$-module structure. Thus an isomorphism of M with N defines an similitude with similitude factor $\overline{\mathrm{n}}\mathrm{orm}(N)$. □

We now recall the setup of Theorem 2.3.22 and deduce the following result for projective left modules over maximal orders in quaternion algebras over $\mathbb{Q}$.

Proposition 2.3.26 *Let (M, q_M) be a positive definite quadratic module over $\mathbb{Z}$ with $\det(M, q_M) = p^2$ with p a prime in $\mathbb{Z}$. Then M is a left projective module of rank 1 over some maximal order $\mathcal{O}$ in L ramified at p and ∞.*

Proof The positive definite condition implies that the quaternion algebra $L_1 = e\mathrm{Cliff}_0(M) \otimes \mathbb{Q}$ ramifies at ∞, hence also at a finite prime. The quadratic module eM is contained in the quadratic module $e\mathrm{Cliff}_1(M)$ and by Proposition 2.2.1 and Proposition 2.3.25 equality holds and p is the unique finite ramifying prime. □

Pectora roborant cultus recti

Chapter 3

Abelian varieties over finite fields

An abelian variety over a finite field $\mathbb{F}_q$ is a complete connected group variety over $\mathbb{F}_q$. In the first few sections we will gather the necessary tools to study endomorphism rings of abelian varieties over finite fields. This was done by Deuring for elliptic curves and some of his theorems extend almost trivially to higher dimensions. An abelian variety A is nonsingular, commutative and projective as a variety and we call A simple if it has no proper abelian subvarieties. By an elementary abelian variety we mean an abelian variety that is $\mathbb{F}_q$-isogenous to a power of a simple abelian variety.

3.1 Homomorphisms

We are looking at algebraic maps between projective varieties, which are those maps defined by rational functions. Let A and B be projective varieties of dimension g over a field $\mathbb{F}_q$. A rational map from A to B is a map of the form $\varphi : A \to B$ such that $\varphi = [f_1 : f_2 : \ldots : f_g]$ with $f_i \in \overline{\mathbb{F}}_q(A)$ and $\forall P \in A$ at which $f_1, f_2, \ldots, f_g$ are all defined we have $\varphi(P) = [f_1(P) : f_2(P) : \ldots : f_g(P)] \in B$.

A map is defined over $\mathbb{F}_q$ if there exists $\lambda \in \overline{\mathbb{F}}_q \backslash 0$ such that for all $i = 1, \ldots, g$ have $\lambda f_i \in \mathbb{F}_q(A)$ and is said to be regular at a point $P \in A$ if there exists a function $\lambda \in \overline{\mathbb{F}}_q(A)$ such that for all $i = 1, \ldots, g$ we have that λf_i is regular at P and there exists an i for which $\lambda f_i(P) \neq 0$ in which case we set $\varphi(P) = [\lambda f_1(P) : \ldots : \lambda f_g(P)] \in B$. If a map is regular at every point it is called a morphism.

Note that $[f_1 : f_2 : \ldots : f_g]$ and $[\lambda f_1 : \lambda f_2 : \ldots : \lambda f_g]$ give the same map on points. If A and B are defined over $\mathbb{F}_q$ then any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on φ in the obvious way. $\varphi^\sigma(P) = [f_1^\sigma(P) : f_2^\sigma(P) : \ldots : f_g^\sigma(P)]$. So a map φ is defined over $\mathbb{F}_q \Leftrightarrow \varphi^\sigma = \varphi$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. The automorphism $\overline{\pi} : \alpha \mapsto \alpha^q$ of the field $\overline{\mathbb{F}}_q$ induces a map on points

$$\begin{array}{rcl} \mathbb{P}^n(\overline{\mathbb{F}}_q) & \to & \mathbb{P}^n(\overline{\mathbb{F}}_q) \\ [x_0 : x_1 : \ldots : x_g] & \mapsto & \left[x_0^q : x_1^q : \ldots : x_g^q\right]. \end{array}$$

which restricts to the Frobenius morphism π_A on A. If $\varphi : A \to B$ is a morphism of projective varieties over $\mathbb{F}_q$, then it follows from the binomial theorem in charateris-

tic p that $\varphi\pi_A = \pi_B\varphi$. If A is a projective variety over $\mathbb{F}_q$, then π_A induces the map $[x_0, x_1, \ldots, x_g] \mapsto [x_0^q, x_1^q, \ldots, x_g^q]$ on $A(\overline{\mathbb{F}}_q)$, and $A(\mathbb{F}_q)$ is the set of points fixed by this map. If A is an abelian variety then π_A maps 0 to 0, so its an endomorphism of A.

For every non-zero integer n, we associate to it the endomorphism of A which is given by multiplication by n on A. This is well defined since the group law on A given by $A \times A \to A$ is a morphism of varieties. Also for any morphism $\varphi : A \to B$, we have $\varphi n = n\varphi$.

3.2 Isogenies

An homomorphism of abelian varieties is called an isogeny if it is surjective and has finite kernel. We say A is isogenous to B over $\mathbb{F}_q$ and write $A \sim_{\mathbb{F}_q} B$ if there exists an isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ defined over $\mathbb{F}_q$. We define its degree to be the degree as a regular map of projective varieties. More precisely, a surjective homomorphism φ induces a injective homomorphism $\varphi^* : \mathbb{F}_q(B) \to \mathbb{F}_q(A)$ of function fields. We define the degree by $\deg(\varphi) = [\mathbb{F}_q(A) : \varphi^*(\mathbb{F}_q(B))]$. We call φ separable (respectively purely inseparable) if the field extension $\mathbb{F}_q(A)/\varphi^*(\mathbb{F}_q(B))$ is separable (respectively purely inseparable). Isogeny is an equivalence relation on abelian varieties and we will denote the equivalence class of A as $[A]_{\sim_{\mathbb{F}_q}}$. For an isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$, we denote by $A[\varphi]$ the kernel of the induced map on $A(\overline{\mathbb{F}}_q)$ as abelian groups.

Proposition 3.2.1 *Assume that A, B, and C are abelian varieties over $\overline{\mathbb{F}}_q$. Let $\alpha \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$, and $\beta \in \mathrm{Hom}_{\mathbb{F}_q}(A, C)$ be two isogenies with α separable and $\ker(\alpha) \subseteq \ker(\beta)$. Then there is a homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(B, C)$ such that $\varphi\alpha = \beta$.*

Proof Since α is separable, we can form the quotient abelian variety $A/\ker(\alpha)$. From the universal property of $A/\ker(\beta)$ we have a regular map $A/\ker(\alpha) \to B$, which is again separable and bijective. Since B is nonsingular, this implies that it is an isomorphism. Thus $B \cong A/\ker(\alpha)$. After identifying B with $A/\ker(\alpha)$ and using the universal properties of quotients again we find that there is a unique regular map such that φ such that $\varphi\alpha = \beta$. Moreover, β is automatically a homomorphism because it maps zero to zero. □

An immediate consequence is that every isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ can be factored as $\varphi = \alpha\beta$ where $\alpha \in \mathrm{Hom}_{\mathbb{F}_q}(C, B)$ is a separable isogeny and $\beta \in \mathrm{Hom}_{\mathbb{F}_q}(A, C)$ is a purely inseparable isogeny. Furthermore this factorization is unique up to isomorphism.

Let A be a g-dimensional abelian variety A over $\mathbb{F}_q$. From the complete reducibility theorem we have that there are simple abelian varieties, $A_1, A_2, \ldots, A_t$ over $\mathbb{F}_q$, such that $A_1, A_2, \ldots, A_t \subset A$ and the map

$$A_1 \times A_2 \times \cdots \times A_t \to A, \quad (a_1, a_2, \ldots, a_t) \mapsto a_1 + a_2 + \ldots + a_t$$

is an isogeny. In particular we have a unique (up to $\mathbb{F}_q$-isogeny) decomposition

$$A \sim_{\mathbb{F}_q} \prod_{i=1}^{t} A_i^{r_i}$$

where the A_i's are distinct $\mathbb{F}_q$-simple non-isogenous abelian varieties over $\mathbb{F}_q$.

The Frobenius endomorphism π_A, or just π if A is clear from context, is an example of a purely inseparable isogeny and $\deg(\pi) = q^g$.

The endomorphism of A induced by the multiplication by n map on A for a positive integer, n, is an isogeny of degree n^{2g}. It is separable if $\gcd(n, p) = 1$. Note that $\ker(\varphi) \subseteq \ker(\deg(\varphi))$. So $\deg(\varphi)$ factors as $\deg(\varphi) = \hat{\varphi}\varphi$ for an unique isogeny, $\hat{\varphi} \in \mathrm{Hom}_{\mathbb{F}_q}(B, A)$, such that $\hat{\varphi}\varphi = \deg(\varphi)$ and $\varphi\hat{\varphi} = \deg(\varphi)$. The multiplication by n maps on A for a positive integer, n, allow us to define an injective ring homomorphism $\mathbb{Z} \to \mathrm{End}_{\mathbb{F}_q}(A)$. We use this injection to identify $\mathbb{Z}$ with its image in $\mathrm{End}_{\mathbb{F}_q}(A)$.

3.3 Representations

The classical treatment of complex abelian varieties as quotients by lattices, and the study of their lattices is crucial for the theory. When we leave $\mathbb{C}$ for the wilds of positive characteristic, however these lattices abandon us. Serre has pointed out that, in characteristic p one cannot functorially attach any free abelian group of rank $2g$ to a g-dimensional abelian variety A. To replace lattices, Weil showed that for any prime ℓ, the points of ℓ power order look just as they would over $\mathbb{C}$. From them one can form a free $\mathbb{Z}_\ell$ module of rank $2g$ on which the endomorphism ring acts. Over a finite field Tate showed that the homomorphisms from one abelian variety to another correspond precisely to these various modules. We will refer to them as Tate modules.

If A is an abelian group and ℓ is a prime number, we denote by $A[\ell]$ the ℓ-torsion subgroup of $A(\overline{\mathbb{F}}_q)$ and by

$$A[\ell^\infty] = \bigcup_{r \geq 1} A[\ell^r]$$

the subgroup of all elements in $A(\overline{\mathbb{F}}_q)$ whose order is an ℓ-power. If A is finite we write $\#A$ for its order.

Let A be an abelian variety of dimension g over $\mathbb{F}_q$. We define the ℓ-adic Tate-module as the inverse limit of $A[\ell^n]$ over n. That is the projective limit

$$\mathrm{T}_\ell(A) = \varprojlim A[\ell^n].$$

with restriction maps $\ell : A[\ell^n] \to A[\ell^{n-1}]$ given by multiplication by ℓ. By thinking of the ring of ℓ-adic integers as an inverse limit

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$$

we see immediately that it acts on $\mathrm{T}_\ell(A)$ making $\mathrm{T}_\ell(A)$ into a $\mathbb{Z}_\ell$-module. It is a free $\mathbb{Z}_\ell$-module of rank $2g$ for $\ell \neq p$. It is also known that $\mathrm{T}_p(A)$ is free of rank γ over $\mathbb{Z}_p$ where $0 \leq \gamma \leq \dim(A)$. Let $\mathrm{V}_\ell(A) = \mathrm{T}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ denote the vector space of dimension $2g$ over $\mathbb{Q}_\ell$, the field of ℓ-adic numbers, obtained by tensoring $\mathrm{T}_\ell(A)$ with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$.

3.3.1 Tate modules

Let A be a g-dimensional abelian variety over $\mathbb{F}_q$ and let π be it's Frobenius endomorphism. Let $\ell \neq p$ be a rational prime in $\mathbb{Z}$ and denote by K (respectively R) the ℓ-adic completions at ℓ of the $\mathbb{Q}$-algebra $\mathbb{Q}[\pi]$ (respectively $\mathbb{Z}$-algebra $\mathbb{Z}[\pi]$) generated by π. We can view $\mathrm{T}_\ell(A)$ is a free R-module of rank $2g$.

In fact T_ℓ defines a (covariant) functor from the category of abelian varieties B over $\mathbb{F}_q$ with a $\mathbb{F}_q$-isogeny $A \to B$ to the category of R-modules $\mathrm{T}_\ell(B)$ with an injective R-homomorphism $\mathrm{T}_\ell(A) \to \mathrm{T}_\ell(B)$. For each positive integer n we have

$$A[\ell^n] \cong \ell^{-n}\mathrm{T}_\ell(A)/\mathrm{T}_\ell(A)$$

and so, taking direct limits we get an isomorphism $\tau : \mathrm{V}_\ell(A)/\mathrm{T}_\ell(A) \to A[\ell^\infty]$.
Let $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ be an isogeny. Mapping the exact sequence

$$0 \to \mathrm{T}_\ell(A) \to \mathrm{V}_\ell(A) \to A[\ell^\infty] \to 0$$

to that of B by φ induces an injective R-homomorphism

$$\varphi_R : \mathrm{T}_\ell(A) \to \mathrm{T}_\ell(B)$$

with $\mathrm{coker}(\varphi_R) = \mathrm{T}_\ell(B)/\varphi_R(\mathrm{T}_\ell(A))$ and a K-module isomorphism

$$\varphi_K : \mathrm{V}_\ell(A) \to \mathrm{V}_\ell(B).$$

Let $\varphi_K^{-1}(\mathrm{T}_\ell(B))$ be the pullback of $\mathrm{T}_\ell(B) \subset \mathrm{V}_\ell(B)$ under this isomorphism, there is an isomorphism $\mathrm{T}_\ell(B)/\varphi_R(\mathrm{T}_\ell(A)) \cong \varphi_K^{-1}(\mathrm{T}_\ell(B))/\mathrm{T}_\ell(A)$. By applying the Snake lemma we have $A[\varphi][\ell^\infty] \cong \varphi_K^{-1}(\mathrm{T}_\ell(B))/\mathrm{T}_\ell(A)$. In fact, every R-submodule of $\mathrm{V}_\ell(A)$ containing $\mathrm{T}_\ell(A)$ arises in this way.

Pectora roborant cultus recti

Proposition 3.3.1 *Suppose ℓ is a prime different from p. Let $\tau : \mathrm{V}_\ell(A)/\mathrm{T}_\ell(A) \to A[\ell^\infty]$ be the isomorphism above. For every R-submodule M of $\mathrm{V}_\ell(A)$ containing $\mathrm{T}_\ell(A)$, there is an abelian variety B with an isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ such that $M = \varphi_K^{-1}(\mathrm{T}_\ell(B)) \subseteq \mathrm{V}_\ell(A)$ and $\tau(M/\mathrm{T}_\ell(A)) = A[\varphi]$.*

The finite abelian group, $A[\varphi]$, has the decomposition

$$A[\varphi] \cong \prod_\ell A[\varphi][\ell^\infty]$$

where each component is isomorphic to $\mathrm{T}_\ell(A)/\varphi_R(\mathrm{T}_\ell(A))$. From this we deduce the following result.

Proposition 3.3.2 *For any isogeny $\varphi \in \mathrm{End}_{\mathbb{F}_q}(A)$, there is a abelian group isomorphism $A[\varphi] \cong \prod_\ell \mathrm{T}_\ell(A)/\varphi_R(\mathrm{T}_\ell(A))$ where ℓ ranges over all prime numbers.*

Proposition 3.3.3 *For every $R-$submodule M of finite index in $\mathrm{T}_\ell(A)$ there exists an abelian variety B over $\mathbb{F}_q$ and an isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(B, A)$ such that $\varphi(\mathrm{T}_\ell(B)) = M$.*

3.3.2 The characteristic polynomial

Let A be a g-dimensional abelian variety over $\mathbb{F}_q$ and let π denote the Frobenius endomorphism of A relative to $\mathbb{F}_q$. By considering the action of π on $\mathrm{V}_\ell(A)$, we define the characteristic polynomial, χ_A (or just χ if A is clear from context). It is monic of degree $2g$, has integer coefficients and as an endomorphism of A, π satisfies χ. The characteristic polynomial has the following form:

$$\chi(x) = x^{2g} + a_1 x^{2g-1} + a_2 x^{2g-2} + \ldots + a_g x^g + q a_{g-1} x^{g-1} + \ldots + q^{g-1} a_1 x + q^g \in \mathbb{Z}[x],$$

and if we factor $\chi(x)$ over the complex numbers as

$$\chi(x) = \prod_{i=1}^{2g} (x - \alpha_i),$$

then the $a_1, \ldots, a_g \in \mathbb{Z}$ are up to isomorphism the symmetric polynomials in the α_i's. It turns out that these algebraic integers have certain remarkable properties.

Theorem 3.3.4 *Let $\chi(x) = \prod_{i=1}^{2g}(x - \alpha_i)$ be the factorization of the characteristic polynomial of the Frobenius endomorphism, π.*

(a) The algebraic integers α_i satisfy $|\alpha_i| = \sqrt{q}$ (Riemann hypothesis) and

$$\#(A(\mathbb{F}_q) - q^g) \leq 2g(q^{g-\frac{1}{2}}) + (2^{2g} - 2g - 1)q^{g-1}.$$

(b) The algebraic integers α_i comes in pairs (complex conjugation) and can be ordered such that $\alpha_i \alpha_{i+g} = q$. In particular if some $|\alpha_i| = \pm\sqrt{q}$, then $|\alpha_{i+g}| = \mp\sqrt{q}$.

(c) $\#(A(\mathbb{F}_{q^m})) = \prod_{i=1}^{2g}(1 - \alpha_i^m)$ for all $m \geq 1$.

Proof See [27] p.54. □

Theorem 3.3.5 *Let A and B be abelian varieties over a finite field $\mathbb{F}_q$ and let χ_A and χ_B be the characteristic polynomials of their Frobenius endomorphisms relative to $\mathbb{F}_q$. Consider canonical factorizations*

$$\chi_A = \prod_{i=1}^{n} g_i^{a_i} \text{ and } \chi_B = \prod_{i=1}^{n} g_i^{b_i}$$

in some extension field of $\mathbb{Q}$. The integer

$$\mathrm{r}(\chi_A, \chi_B) = \sum_{i=1}^{n} a_i b_i \deg(g_i)$$

is independant of the choice of the extension field and $\mathrm{r}(\chi_A, \chi_B) = \mathrm{rank}(\mathrm{Hom}_{\mathbb{F}_q}(A, B))$.

(a) The following statements are equivalent

(i) B is $\mathbb{F}_q$-isogenous to an abelian subvariety of A defined over $\mathbb{F}_q$.

(ii) $\mathrm{V}_\ell(B)$ *is isomorphic to a subspace of* $\mathrm{V}_\ell(A)$ *for some* ℓ.

(iii) χ_B *divides* χ_A.

(b) The following statements are equivalent

(i) A *and* B *are* $\mathbb{F}_q$*-isogenous.*

(ii) $\chi_A = \chi_B$.

(iii) The zeta functions of A *and* B *are the same.*

(iv) A *and* B *have the same number of points in every finite extension field of* $\mathbb{F}_q$.

Proof See [36] Theorem 1. □

Theorem 3.3.6 *Let* A *and* B *be abelian varieties over* $\mathbb{F}_q$ *and* $\ell \neq p$ *a rational prime. The canonical map*

$$\mathrm{Hom}_{\mathbb{F}_q}(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(A), \mathrm{T}_\ell(B))$$

is bijective and $\mathrm{Hom}_{\mathbb{F}_q}(A,B)$ *is a free* $\mathbb{Z}$*-module of rank at most* $4\dim(A)\dim(B)$.

Proof See [36]. □

Note that since $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$ we have the bijective map,

$$\mathrm{Hom}_{\mathbb{F}_q}(A,B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathrm{V}_\ell(A), \mathrm{V}_\ell(B)),$$

where bijectivity holds $\forall \ell \neq p$ if and only if it hold for one such ℓ and

$$\mathrm{rank}(\mathrm{Hom}_{\mathbb{F}_q}(A,B)) = \dim_{\mathbb{Q}_\ell}(\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathrm{V}_\ell(A), \mathrm{V}_\ell(B))),$$

is independant of the choice of ℓ.

Pectora roborant cultus recti

It follows from Theorem 3.3.6 that the category of abelian varieties over $\mathbb{F}_q$ is an additive category in which all the morphism groups $\mathrm{Hom}_{\mathbb{F}_q}(A,B)$ are finitely generated free $\mathbb{Z}$-modules. We obtain an abelian (and even $\mathbb{Q}$-linear) category $\mathcal{A}_q$ by keeping the same objects and considering $\mathrm{Hom}_{\mathbb{F}_q}(A,B) \otimes \mathbb{Q}$.

Proposition 3.3.7 *A morphism* $\varphi : A \to B$ *in* $\mathcal{A}_q$ *is an isomorphism if and only if its non-zero multiples* $m\varphi$*, which belong to* $\mathrm{Hom}_{\mathbb{F}_q}(A,B)$*, are isogenies.*

Proof Let $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A,B) \otimes \mathbb{Q}$. Let $m \in \mathbb{Z}$ be such that $m\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A,B)$ is an isogeny. Then there exists $n \in \mathbb{Z}$ and an isogeny $\delta : B \to A$ such that $n = \delta m\varphi$. Let $\gamma = \delta \otimes (mn)^{-1}$, then in $\mathrm{Hom}_{\mathbb{F}_q}(A,A) \otimes \mathbb{Q}$ we have $1 = \gamma\varphi$. We can proceed similarly to get the right inverse for φ, so φ is an isomorphism. Conversely, suppose φ is invertible with inverse φ^{-1}. We have $1 - \varphi^{-1}\varphi = 0$ in $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$, so there exists $r \in \mathbb{Z}$ such that $r - r\varphi^{-1}\varphi = 0$ in $\mathrm{End}_{\mathbb{F}_q}(A)$. Let $m, n \in \mathbb{Z}$ be such that $m\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A,B)$, respectively $n\varphi^{-1} \in \mathrm{Hom}_{\mathbb{F}_q}(B,A)$. Replacing r by some integer multiple if necessary we get $r - n\varphi^{-1}m\varphi = 0$ in $\mathrm{End}_{\mathbb{F}_q}(A)$. Similarly we have $s \in \mathbb{Z}$ for which $s - m\varphi n\varphi^{-1} = 0$ in $\mathrm{End}_{\mathbb{F}_q}(B)$. If $\alpha : A \to B$ and $\beta : B \to A$ are such that $\beta\alpha = r$, then β is surjective and α has finite kernel (because r is an isogeny, so it is surjective with finite kernel). By applying

this to the above equalities in $\mathrm{End}_{\mathbb{F}_q}(B)$ and $\mathrm{End}_{\mathbb{F}_q}(A)$ we conclude that $m\varphi$ is surjective with finite kernel. □

Hence $\mathcal{A}_q$ is the category of abelian varieties up to isogeny over $\mathbb{F}_q$. We will head towards a classification of the simple objects in the category of abelian varieties up to $\mathbb{F}_q$ isogeny. We will next describe the structure of the endomorphism algebra $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ for arbitrary A. We will see that the characteristic polynomial of an abelian variety A over $\mathbb{F}_q$ completely determines the algebra L.

Let A be an arbitrary g-dimensional abelian variety over $\mathbb{F}_q$. The splitting of A up to isogeny into powers of simple abelian varieties

$$A \sim_{\mathbb{F}_q} \prod_{i=1}^{t} A_i^{r_i}$$

corresponds to the decomposition of L into simple factors

$$L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q} \cong \prod_{i=1}^{t} \mathbb{M}_{r_i}(\mathrm{End}_{\mathbb{F}_q}(A_i) \otimes \mathbb{Q}) \cong \prod_{i=1}^{t} \mathbb{M}_{r_i}(E_i)$$

which in turn is given by the factorization of the center of L,

$$K = \prod_{i=1}^{t} K_i$$

into a product of fields which is determined by the factorization of

$$\chi_A = \prod_{i=1}^{t} \chi_{A_i}^{r_i}$$

into distinct $\mathbb{Q}$-irreducible factors. For every simple abelian variety A_i in the decomposition we have that the endomorphism algebra E_i is uniquely determined up to isomorphism by its invariants.

Theorem 3.3.8 *Let A be a simple g-dimensional abelian variety over $\mathbb{F}_q$ and let χ denote the characteristic polynomial of the Frobenius endomorphism, π of A. Let $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be the endomorphism algebra of A and consider the $\mathbb{Q}$-subalgebra, $K = \mathbb{Q}[\pi]$ of L, generated by π.*

(a) χ is the r^{th}-power of a $\mathbb{Q}$-irreducible polynomial and L is a central division algebra of dimension r^2 over the field K.

(b) For any prime P of K we have

$$\mathrm{inv}_P(L) = \begin{cases} \frac{1}{2} & \text{if } P \text{ is real,} \\ 0 & \text{if } P \text{ lies over } \ell \neq p \text{ and} \\ \frac{\mathrm{ord}_P(\pi)}{\mathrm{ord}_p(q)}[K : \mathbb{Q}_p] & \text{if } P \text{ lies over } p \end{cases}$$

and r is the period of L in $\mathrm{Br}(K)$*. In particular r, which is the least common denominator if all the* $\mathrm{inv}_P(L)$*'s, is determined from π.*

(c) $2g = [L : K]^{\frac{1}{2}}[K : \mathbb{Q}]$.

Proof Since π commutes with all the $\mathbb{F}_q$ endomorphisms of A, we know it is a central element of L. Since the L is a division algebra (so it has no zero divisors), K is a field. By Theorem 3.3.6, $L_\ell \cong \mathrm{End}(\mathrm{V}_\ell(A))$ and since $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is generated topologically by the Frobenius endomorphism with respect to the field $\mathbb{F}_q$, we have that $\mathrm{End}(\mathrm{V}_\ell(A))$ is the centralizer of π in $\mathrm{End}(\mathrm{V}_\ell(A))$. So in L_ℓ we know by the double centralizer theorem that $\mathrm{centre}(L_\ell) = \mathrm{centre}(\mathrm{centre}(\pi)) = \mathrm{centre}(\mathrm{centre}(K_\ell)) = K_\ell$ so K is the center of L. We must have that $\chi = g^r$ for some monic polynomial g with integer coefficients and some integer r, otherwise K wouldn't be a field. First, L does not split over the real primes of K if there are any. If P is a prime of K lying above $\ell \neq p$, we consider $\mathrm{V}_\ell(A)$. It is a free module of rank r over K_ℓ. Therefore L_ℓ is the algebra of $r \times r$ matrices with entries in K_ℓ, so L has invariant 0 at such P. This also shows that $[L : \mathbb{Q}] = r^2[K : \mathbb{Q}]$ and it is clear that $2g = \deg(\chi) = r[K : \mathbb{Q}]$. To complete this we should look at the case where P lies over p. The main problem is that the concept of the Tate module is not defined for p. Tate proved that for abelian varieties A and B over $\mathbb{F}_q$, the map $\mathbb{Z}_p \otimes \mathrm{Hom}_{\mathbb{F}_q}(A, B) \to \mathrm{Hom}(\mathrm{T}_p(A), \mathrm{T}_p(B))$ is bijective. Proofs of this result and of the formula giving the invariant of $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ at primes lying over p appear in [39]. It is modeled after the proofs for $\ell \neq p$, slightly complicated by the fact that one is dealing with modules over a non-commutative ring. □

Given an arbitrary g-dimensional abelian variety A over $\mathbb{F}_q$, we have K as the center of the semisimple algebra L since K_ℓ is the center of L_ℓ. Hence K is itself semisimple.
Furthermore we always have $2g \leq \dim_{\mathbb{Q}}(L) \leq (2g)^2$.

A is said to admit sufficiently many complex multiplications (is of CM type) if and only if its endomorphism algebra L contains a commutative semisimple algebra, K over $\mathbb{Q}$, of dimension $2g$. Equivalently write

$$A \sim \prod_{i=1}^{t} A_i^{r_i}$$

up to $\mathbb{F}_q$-isogeny as a direct product of simple abelian varieties. Then A is said to be of CM type if and only if $E_i = \mathrm{End}_{\mathbb{F}_q}(\mathrm{A_i}) \otimes \mathbb{Q}$ contains an algebraic number field K_i of degree $2\dim(A_i)$ over $\mathbb{Q}$ for all A_i. Immediately from the definition we see that every abelian variety over a finite field $\mathbb{F}_q$ is of CM type.

Theorem 3.3.9 *Let A be an abelian variety of dimension g over $\mathbb{F}_q$ and let χ denote the characteristic polynomial of π. Set $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ and let $K = \mathbb{Q}[\pi]$ be the $\mathbb{Q}$-subalgebra of L generated by π.*

(a) A is $\mathbb{F}_q$-isogenous to a power of a $\mathbb{F}_q$-simple abelian variety if and only if χ is the power of a $\mathbb{Q}$-irreducible polynomial. In which case L is a central simple algebra over K which splits at all finite primes of K not dividing p, but does not split at any real prime of K.

(b) The following are equivalent

(i) $\dim_{\mathbb{Q}}(L) = 2g$.

(ii) χ *has no multiple roots.*

(iii) $L = K$.

(iv) L *is commutative.*

(c) The following are equivalent

(i) $\dim_{\mathbb{Q}}(L) = (2g)^2$.

(ii) χ *is a power of a linear polynomial.*

(iii) $K = \mathbb{Q}$.

(iv) $L \cong \mathbb{M}_g(D)$ *where* D *is the definite quaternion algebra over* $\mathbb{Q}$ *which is ramified exactly at* p *and* ∞.

Proof See [36] Theorem 2. □

Example We give an example in each case of Theorem 3.3.9. For case (a), consider an abelian variety over $\mathbb{F}_{5^2}$ having characteristic polynomial

$$\chi = x^4 - 12x^3 + 86x^2 - 300x + 625 = (x^2 - 6x + 25)^2.$$

Then $L = \mathbb{M}_2(K)$ is a central simple algebra over $K = \mathbb{Q}(3 + 4\sqrt{-1})$.
For (b) we let

$$\chi = x^4 - 4x^3 - 498x^2 - 1372x + 117649$$

be the characterisitic polynomial for an abelian variety over $\mathbb{F}_{7^3}$. Then $L = K$ where K is the number field obtain by adjoining a root of χ to $\mathbb{Q}$.
Finally for (c), consider an abelian variety over $\mathbb{F}_{101^2}$ with characteristic polynomial

$$\chi = x^2 + 202x + 10201 = (x + 101)^2.$$

Then L is the rational quaternion algebra ramified at exactly 101 and ∞. □

3.4 Complex multiplication

The theory of complex multiplication goes back to Hilbert's Twelfth Problem where he asks for those functions that play for an arbitrary algebraic number field the role that the exponential function plays for the field of rational numbers and the elliptic modular functions play for an imaginary quadratic number field. The classical result, referred to by Hilbert, can be stated as follows: for any quadratic imaginary field K, the maximal abelian extension of K is obtained by adjoining to it the moduli of polarized 1-dimensional abelian varieties and their torsion points with complex multiplication by K.

As Weil observed, in dimension greater than 1, the moduli of polarized abelian varieties of CM type and their torsion points generate abelian extensions, not of the field of complex multiplication, but of another field associated with it. The latter is now called the reflex field.

By a complex multiplication field (CM-field) we will mean a totally imaginary quadratic extension of a totally real algebraic number field. An algebraic number field K is a CM field if and only if complex conjugacy, denoted by $\epsilon_{\mathbb{C}}$, induces a non-trivial automorphism of K and $\sigma\epsilon_{\mathbb{C}} = \epsilon_{\mathbb{C}}\sigma$ for every isomorphism $\sigma : K \to K$.

In the decomposition of the endomorphism algebra L in the previous section, $E_i = \mathrm{End}_{\mathbb{F}_q}(A_i)$ is a division algebra over $\mathbb{Q}$ admitting a positive involution and a division algebra admitting a positive involution might contain a maximal commutative subfield K_i which is not a CM field. A priori, the maximal commutative subalgebra K in L might not be a product of CM fields, however if A contains a polarization we can always find one a maximal $CMfield$ which is invariant under the Rosati involution induced by the polarization. So we will always assume K is a product of CM fields.

Let K be a CM field of degree $2g$ over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. Let $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_g\}$ be g embeddings of K into $\mathbb{C}$ such that no two of them are complex conjugate. We call (K, Φ) a CM type of K. There exist 2^g different CM types or 2^{g-1} if φ_1 is fixed. We will call an element $\alpha \in K$ totally imaginary if $\epsilon_{\mathbb{C}}(\alpha) = -\alpha$. A totally imaginary α of K is positive (respectively non-negative, negative, non-positive) with respect to a CM type if $\frac{1}{i}\varphi(\alpha)$ is positive (respectively non-negative, negative, non-positive) for all φ in the CM type.

Every CM type of K has a reflex type $(K^*, \{\delta_1, \ldots, \delta_g\})$ where K^* is obtained by adjoining to K all sums of the form $\sum_{i=1}^{g} \varphi_i(a)$ with $a \in K$.

Let A be a g-dimensional abelian variety A over $\mathbb{C}$. It is well know that $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for some lattice Λ in $\mathbb{C}^g$. Further we know that there exists a non-degenerate Riemann form on the lattice inducing a polarization on Λ and if this polarization is principal then the lattice can be given in the form $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ where $\Omega \in \mathbb{H}_g = \{z \in \mathbb{M}_g(\mathbb{C}) |\ z^t = z,\ \mathrm{Im}(z) \text{ positive definite}\}$ represents $A(\mathbb{C})$. A is said to admit sufficiently many complex multiplications (is of CM type) if and only if its endomorphism algebra $L = \mathrm{End}_{\mathbb{C}}(A) \otimes \mathbb{Q}$ contains a commutative semisimple algebra K over $\mathbb{Q}$ of dimension $2g$. Equivalently write

$$A \sim \prod_{i=1}^{t} A_i^{n_i}$$

up to $\mathbb{F}_q$-isogeny as a direct product of simple abelian varieties. Then A is said to admit complex multiplications if and only if $\mathrm{End}_{\mathbb{C}}(A_i) \otimes \mathbb{Q}$ is CM field K_i of degree $2\dim(A_i)$ over $\mathbb{Q}$ for all A_i.

Suppose A is a g-dimensional complex abelian variety of CM type. If $g \geq 2$, then for every CM type (K, Φ), and ideal, I, in K we have $\Lambda = \{(\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_g(\alpha))^t |\ \alpha \in I\}$ as a lattice in $\mathbb{C}^g$ and the corresponding abelian variety, say A, is said to be of CM-type (K, Φ). This means there exists a basis $\{\Omega_1, \ldots, \Omega_g\}$ for the invariant 1-forms on A such that that is $\alpha\Omega_i = \varphi_i(\alpha)\Omega_i$ for all $\alpha \in K$ and the complex conjugates $\{\epsilon_{\mathbb{C}}(\varphi_1), \ldots, \epsilon_{\mathbb{C}}(\varphi_g)\}$ are the other half of the embeddings. For the injection $\iota : K \to \mathrm{End}_{\mathbb{C}}(A) \otimes \mathbb{Q}$ we have that the representation of $\iota(K)$ in the space of invariant 1-forms on A is equivalent to $\varphi_1 \oplus \varphi_2 \oplus \ldots \oplus \varphi_g$. Conversely every CM type of K arises from some abelian variety of CM-type over $\mathbb{C}$ unique up to isogeny.

Suppose $\mathrm{Gal}(K/\mathbb{Q}) = \{\varphi_1, \varphi_2, \ldots, \varphi_g, \epsilon_{\mathbb{C}}(\varphi_1), \ldots, \epsilon_{\mathbb{C}}(\varphi_g)\}$. Then A is simple if and only if the only $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ for which $\{\sigma(\varphi_1), \sigma(\varphi_2), \ldots, \sigma(\varphi_g)\} = \{\varphi_1, \varphi_2, \ldots, \varphi_g\}$ is the identity map. We call the CM type primitive if its corresponding abelian variety is simple. A reflex CM type is primitive and a primitive CM type is its own double reflex. In the simplest case where K is an abelian extension of $\mathbb{Q}$ and the CM type $(K, \{\varphi_1, \varphi_2, \ldots, \varphi_g\})$ is primitive then the reflex CM type is $(K, \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_g^{-1}\})$.

In $g \geq 2$ it is important to fix a polarization of A and hence a projective embedding. A polarized abelian variety of CM type has a field of moduli which is an unramified abelian extension of the reflex field as we have mentioned before. If $g = 1$, then $K = K^*$ and $K(\mathrm{j}(A))$, the Hilbert class field of K (maximal unramified abelian extension of K), is the field of moduli.

Using the concept of a CM type one can now give a complete classification of the isogeny classes of abelian varieties over finite fields.

3.4.1 Weil numbers

We shall say that an algebraic integer π is a Weil q-number if we have $\sigma(\pi)\epsilon_{\mathbb{C}}(\sigma(\pi)) = q = p^n$ with n a positive integer and any conjugate $\sigma(\pi)$ of π, where $\epsilon_{\mathbb{C}}$ denotes the complex conjugacy of $\mathbb{C}$. The integer n is called the order of π.

Let π and α be Weil q-numbers. We shall say that π is equivalent to α and write $\pi \equiv \alpha$ if π^r is conjugate to α^s for some positive integers r and s. For a Weil q-number we denote by $[\pi]_{\mathbb{C}}$ the conjugacy class of π and by $[\pi]_{\equiv}$ its equivalence class.

Proposition 3.4.1 *Let π be a Weil q-number and let n be its order. If π is real, then $\pi = \pm\sqrt{q}$. If π is imaginary then $\mathbb{Q}[\pi]$ is a* CM*-field.*

Proof The first assertion is clear. The second follows from the definitions of a Weil q-number and the conditions for a number field to be a CM-field. □

Note that the Weil q-numbers can all be constructed in the following easy fashion. Let π be a Weil q-number and define $\alpha = \pi + q\pi^{-1}$. Let $\varphi : \mathbb{Q}(\pi) \to \mathbb{C}$ be a complex embedding. We have

$$\epsilon_{\mathbb{C}}(\varphi(\alpha)) = \epsilon_{\mathbb{C}}(\varphi(\pi)) + q\epsilon_{\mathbb{C}}(\varphi(\pi))^{-1} = q\varphi(\pi)^{-1} + \varphi(\pi) = \varphi(\alpha).$$

So α is a totally real algebraic integer. We also note that

$$|\varphi(\alpha)| \leq |\varphi(\pi)| + q|\varphi(\pi)|^{-1} = 2q^{\frac{1}{2}}.$$

Conversely given such a number α, the roots of the equation $x^2 - \alpha x + q = 0$ are Weil q-numbers.

We state some results of Honda and Tate on the classification up to isogeny of abelian varieties over finite fields. In particular we will give a complete classification of isogeny classes of abelian varieties over finite fields in terms of their Frobenius endomorphisms.

Theorem 3.3.5 (c) implies that if π_A is conjugate to π_B (hence their characteristic polynomials are the same), then B is isogenous to A, so the map that sends a simple abelian variety A over $\mathbb{F}_q$ to its Frobenius endomorphism π_A ($A \mapsto \pi_A$) is injective.

A theorem of Weil says that if A is an abelian variety of CM type over $\mathbb{C}$ then A is defined over a number field. The rough idea is that given some CM type one can construct a corresponding abelian variety A over $\mathbb{C}$. This has a model over some number field K and (after enlarging this field if necessary) A has good reduction at all primes of K. We can produce suitable CM type for any given Weil q-number π in such a way that the Frobenius endomorphism of the reduction of A over $\mathbb{F}_q$ is conjugate to π. In other words every $\mathbb{F}_q$-simple abelian variety A over $\mathbb{F}_q$ corresponds to a conjugacy class of Weil q-numbers with order n where $q = p^n$ by considering the Frobenius endomorphism of A. More precisely

Theorem 3.4.2 *For every $n \geq 1$ We have a bijective map*

$$\begin{array}{rccl} \varphi: & \{[A]_{\sim \mathbb{F}_q} |\ A \text{ is a simple abelian variety over } \mathbb{F}_q\} & \to & \{[\pi]_{\mathbb{C}} |\ \pi \text{ is a Weil } q-\text{number}\} \\ & [A]_{\sim \mathbb{F}_q} & \mapsto & [\pi_A]_{\mathbb{C}} \end{array}$$

Proof By the definition of equivalent Weil q-numbers we have a map

$$\begin{array}{rccl} \lambda: & \{[A]_{\sim \overline{\mathbb{F}}_p} |\ A \text{ is a simple abelian variety over } \overline{\mathbb{F}}_p\} & \to & \{[\pi]_{\equiv} |\ \pi \text{ is a Weil } q-\text{number}\} \\ & [A]_{\sim \overline{\mathbb{F}}_p} & \mapsto & [\pi_A]_{\equiv} \end{array}$$

By Theorem 3.3.5 the map φ is injective. Moreover the surjectivity of φ follows from that of λ by the standard method of descending the field of definition. See [14] for a well written proof. □

This is well known as the Honda-Tate theorem and provides us with a classification of the simple objects in the category of abelian varieties up to $\mathbb{F}_q$-isogeny.

3.4.2 Weil polynomials

Let π be a Weil q-number. To every g-dimensional abelian variety A over $\mathbb{F}_q$ we associate the characteristic polynomial $\chi \in \mathbb{Z}[x]$ of its Frobenius endomorphism (acting on the ℓ-adic Tate modules of A). We call a polynomial a Weil q-polynomial if it is the characteristic polynomial of an abelian variety defined over $\mathbb{F}_q$. Weil proved that all of the roots of a Weil q-polynomial are Weil numbers, and showed that every Weil q-number is a root of some Weil q-polynomial. Furthermore, Theorem 3.3.5 states that two abelian varieties over $\mathbb{F}_q$ are isogenous if and only if their associated Weil q-polynomials are equal.

If A is a simple abelian variety over $\mathbb{F}_q$ then χ is a power of an irreducible polynomial, and in fact the Honda-Tate theorem (Theorem 3.4.2) says the map that sends A to the set of roots (in $\overline{\mathbb{Q}}$) of χ induces a bijection between the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the set of Galois conjugacy classes of Weil q-numbers in $\mathbb{Q}$. Thus the Honda-Tate theorem also provides us with a simple number-theoretic criterion for determining whether a polynomial, all of whose roots are Weil q-numbers, is a Weil

q-polynomial.

3.5 Endomorphism rings

Let A be an arbitary g-dimensional abelian variety A over $\mathbb{F}_q$ and let $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be its endomorphism algebra. L is a semisimple $\mathbb{Q}$-algebra. We know $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(A)$ is a finitely generated torsion-free $\mathbb{Z}$-module of finite rank, so we can consider it as a $\mathbb{Z}$-submodule of L. It is a full $\mathbb{Z}$-lattice in L and so by definition $\mathcal{O}$ is a $\mathbb{Z}$-order in L. In the previous section we gave a complete classification of abelian varieties up to isogeny. The rest of this section we can ride the crest of this wave to results on the precise endomorphism rings of abelian varieties over finite fields.

3.5.1 Base field extension

We note that in passing from $\mathbb{F}_q$ to an extension of degree d replaces π by π^d. If $\mathbb{Q}[\pi] = \mathbb{Q}[\pi^d]$ then L is unchanged and it follows that the endomorphism ring is unchanged. To see this suppose $\varphi \in L$ is an endomorphism of A defined over the extension. Then for some $m \in \mathbb{Z}$ we have $m\varphi$ in $\mathrm{End}_{\mathbb{F}_q}(A)$ since $\mathrm{End}_{\mathbb{F}_q}(A)$ is a $\mathbb{Z}$-lattice in L. But $m\varphi$ vanishes on the subgroup $A[m]$ so there is an $\alpha \in \mathrm{End}_{\mathbb{F}_q}(A)$ defined over $\mathbb{F}_q$ with $\alpha m = m\varphi$ and thus $\varphi = \alpha$. If $\mathbb{Q}[\pi] \neq \mathbb{Q}[\pi^d]$, however, L can change and A may acquire more endomorphisms. If not we will say $\mathrm{End}_{\mathbb{F}_q}(A)$ is stable under base field extension.

Lemma 3.5.1 *Let α be an algebraic number with minimal polynomial $f \in \mathbb{Q}[x]$ and suppose that d is a positive integer such that the field $E = \mathbb{Q}(\alpha^d)$ is a proper subfield of $K = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\alpha^r)$ for all $0 < r < d$. Then either $f \in \mathbb{Q}[x^d]$ or there is a primitive d^{th} root of unity ζ_d in K such that $K = E(\zeta_d)$.*

Proof Let ζ_d be a primitive d^{th} root of unity in an algebraic closure of K and let $F = E(\zeta_d) \cap K$. Note that $E \subseteq F$. Since $E(\zeta_d)$ is a Galois extension of E it is also a Galois extension of f, and it follows that $E(\zeta_d)$ and K are linearly disjoint over F, so that $m = [K(\zeta_d) : E(\zeta_d)] = [K : F]$. Since $K(\zeta_d) = \mathbb{Q}(\alpha, \zeta_d)$ is a Krummer extension of $E(\zeta_d) = \mathbb{Q}(\alpha^d, \zeta_d)$, we see that α^m lies $E(\zeta_d)$ and hence also in F. Suppose $m > 1$. Then $\mathbb{Q}(\alpha^m)$ is a subfield of the proper subfield F of K, the lemma's hypothesis shows we have $m = d$. If we let h be the minimal polynomial of α^d over $\mathbb{Q}$, then $f(x) = h(x^d)$. Suppose $m = 1$. Then $K(\zeta_d) = E(\zeta_d)$ so K/E is a subextension of the abelian extension $K(\zeta_d)/E$ and is therefore Galois. Let $G = \mathrm{Gal}(K/E)$ be it's Galois group and suppose σ is an element in G different from the identity element. Let $\xi = \alpha^{-1}\sigma(\alpha)$ so that ξ lies in the multiplicative group generated by ζ_d. Suppose r is a positive integer less that d. Then the hypothesis of the lemma shows that $K = \mathbb{Q}(\alpha^r)$ and so we must have $\alpha^r \neq \sigma(\alpha^r) = \xi^r \alpha^r$. Thus ξ must in fact be a primitive d^{th} root of unity, which shows that $\zeta_d \in K$. It follows that $K = K(\zeta_d)$ and this last field is $E(\zeta_d)$ because $m = 1$. □

Theorem 3.5.2 *Let A be an simple abelian variety over $\mathbb{F}_q$ and identify the Frobenius endomorphism of A with a Weil q-number π. Set $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ to be the endomorphism algebra of A and let $K = \mathbb{Q}(\pi)$ be the subfield of L generated by π. Let D be the set of integers $d \in \mathbb{Z}$ such that $d > 1$ and either one of the following holds true.*

(a) The field $E = \mathbb{Q}(\pi^d)$ is a proper subfield of K and there is a primitive d^{th} root of unity, ζ_d, in K such that $K = E(\zeta_d)$.

(b) The minimal polynomial for π over $\mathbb{Q}$ lies in $\mathbb{Z}[x^d]$.

Then $K = \mathbb{Q}(\pi^d)$ for all integers $d > 0$ if and only if $D = \emptyset$.

Proof If d is an integer D, then clearly $\mathbb{Q}(\pi^d)$ is a proper subfield of K. On the other hand if there exists some $d > 0$ such that $\mathbb{Q}(\pi^d) \neq K$ then there exists a smallest such d and by Lemma 3.5.1 this d lies in D. □

3.5.2 Action on torsion elements

A module, M, over a unital ring R is called faithful if for all distinct elements a, b of R, there exists $\lambda \in M$ such that $a\lambda \neq b\lambda$. In other words, the multiplications by distinct elements a and b define two different endomorphisms of M.

This condition is equivalent to requiring that whenever $a \in R$, $a \neq 0$, that $a\lambda \neq 0$ for some $\lambda \in M$, for example $\lambda M \neq 0$, so that the annihilator of M is reduced to $\{0\}$. This shows, in particular, that any torsion-free module is faithful. More generally, any ring $\mathcal{O}$ containing R as a subring is faithful as a module over R, since 1 is annihilated only by 0.

Proposition 3.5.3 *Let A be an abelian variety over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(A)$. For any separable $\varphi \in \mathcal{O}$, we have $A[\varphi]$ is a faithful $\mathcal{O}/\mathcal{O}\varphi$ module.*

Proof Clearly, $A[\varphi]$ is an $\mathcal{O}/\mathcal{O}\varphi$-module. We have to show that $A[\varphi]$ is a faithful $\mathcal{O}/\mathcal{O}\varphi$-module, that is, any $\alpha \in \mathcal{O}$ with $\alpha A[\varphi] = 0$ belongs to $\mathcal{O}\varphi$. Suppose α is such that $\alpha A[\varphi] = 0$. Since φ is separable, this implies that $\alpha = \gamma\varphi$ for some endomorphism γ of A by Proposition 3.2.1 applied with $A = B = C$. This implies that $\alpha \in \mathcal{O}\varphi$, which proves the claim. □

We know that for a positive integer n coprime to p and $\varphi \in \mathcal{O}$, an isogeny such that $A[n] \subseteq \ker(\varphi)$ (for example φ acts as zero on the n-torsion), then there exists some endomorphism α such that $\alpha = \varphi n = n\varphi$ implying that α is divisible by n in $\mathcal{O}$.

Note that $A(\mathbb{F}_{q^k}) = A[\pi^k - 1]$ for $k \geq 1$. Immediately from this we see that all the n-torsion is defined over $\mathbb{F}_{q^k}$ if and only if $\frac{1}{n}(\pi^k - 1) \in \mathcal{O}$.

Suppose we are given some other $\mathbb{Z}$-order, Λ, in the endomorphism algebra of L. If Λ is generated by elements of the form $\frac{1}{m}(\pi^k - 1)$ for some collection of pairs (k, m) then by simply by checking the field of definition of the m-torsion we can determine if Λ is contained in $\mathcal{O}$. Note however that it is not true in general that, knowing the field of definition of the n-torsion for all n, is enough to detemine the endomorphism ring. The endomorphism ring may differ because the action of the Frobenius endomorphism on the torsion subgroups is different.

3.5.3 Representatives

Let A be an abelian variety over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(A)$ and let L be its endomorphism algebra. Take any $B \in [A]_{\sim\mathbb{F}_q}$. The endomorphism ring of B is an $\mathbb{Z}$-order in a semisimple $\mathbb{Q}$-algebra isomorphic to L. In order to be able to compare $\mathcal{O}$ with the endomorphism ring of B we will need a representation of $\mathrm{End}_{\mathbb{F}_q}(B)$ as a $\mathbb{Z}$-order in L. We must be careful on the exact $\mathbb{Z}$-order in L since we are interrested in properties which depend heavily on the isomorphism class of A but behave badly up to isogeny.

For any isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ of degree m we have an isogeny $\hat{\varphi} = m\varphi^{-1} \in \mathrm{Hom}_{\mathbb{F}_q}(B, A)$. Note that $\hat{\varphi}\mathrm{End}_{\mathbb{F}_q}(B)\varphi \subseteq \mathrm{End}_{\mathbb{F}_q}(A)$ and $\varphi\mathrm{End}_{\mathbb{F}_q}(A)\hat{\varphi} \subseteq \mathrm{End}_{\mathbb{F}_q}(B)$. The map

$$\begin{array}{rcl} \mathrm{End}_{\mathbb{F}_q}(A) & \to & \mathrm{End}_{\mathbb{F}_q}(B) \\ \alpha & \mapsto & \varphi\alpha\hat{\varphi} \end{array}$$

is a $\mathbb{Z}$-module homomorphism but unfortunately in general it is not a ring homomorphism. To correct the deficiency we define a ring monomorphism

$$\begin{array}{rcl} \iota_\varphi : \mathrm{End}_{\mathbb{F}_q}(B) & \to & L \\ \alpha & \mapsto & \hat{\varphi}\alpha\varphi = m(\varphi^{-1}\alpha\varphi \otimes 1)m^{-1} \end{array}$$

and consider the image $R = \iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$ of $\mathrm{End}_{\mathbb{F}_q}(B)$ in L. The $\mathbb{Z}$-order, $\iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$ is called a representative for B in L. If $\iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B)) \cong \mathrm{End}_{\mathbb{F}_q}(A)$ then φ is called an isometry. We say A is isometric to B if there exists an isometry and write $A \equiv_{\mathbb{F}_q} B$. Isometry is an equivalence relation and the equivalence class of A, denoted $[A]_{\equiv\mathbb{F}_q}$ will simply be refered to as the endomorphism class of A.

The $\mathbb{Z}$-order, $\iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$, is in fact just the pull-back of $\mathrm{End}_{\mathbb{F}_q}(B)$ under isomorphism of rings induced by φ. The explicit isomorphism between the two algebras is given by

$$\begin{array}{rcl} \iota_B : L & \to & \mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Q} \\ \lambda \otimes \dfrac{1}{d} & \mapsto & \varphi\lambda\hat{\varphi} \otimes \dfrac{1}{dm} \end{array}$$

with inverse map

$$\begin{array}{rcl} \iota_B^{-1} : \mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Q} & \to & L \\ \lambda \otimes \dfrac{1}{d} & \mapsto & \hat{\varphi}\lambda\varphi \otimes \dfrac{1}{dm} = m(\varphi^{-1}\lambda\varphi \otimes \dfrac{1}{d})m^{-1}. \end{array}$$

Note that $\iota_\varphi(\pi_B) = \pi_A \otimes 1$. This shows that that the Frobenius endomorphism of A is preserved and thus contained in every possible representative.

Let $\iota_B(\alpha)$ be an isogeny in $\mathrm{End}_{\mathbb{F}_q}(B)$ for some invertible α in L. Then we get a new map,

$$\hat{\iota}_B : \lambda \mapsto \iota_B(\alpha)\, \iota_B(\lambda)\, \iota_B(\alpha^{-1}) = \iota_B(\alpha\lambda\alpha^{-1})$$

induced by α. This shows that ι_B is preceded by a conjugation in L. Furthermore every $\hat{\iota}_B$ arises from some isogeny in this way.

For each isogeny, $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$, and a rational prime, $\ell \neq p$, φ induces a homomorphism $\varphi_\ell : \mathrm{T}_\ell(A) \to \mathrm{T}_\ell(B)$ and an isomorphism $\varphi_\ell : \mathrm{V}_\ell(A) \to \mathrm{V}_\ell(B)$. These are seemingly two natural ways for L to act on $\mathrm{V}_\ell(B)$. We can compose ι_B with the natural action of $\mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Q}$, or we can identify $\mathrm{V}_\ell(B)$ with $\mathrm{V}_\ell(A)$ via φ_ℓ and take the action of $\mathrm{V}_\ell(A)$ given by the identity map of L. But as it should be these are these are the same. The first takes α to $(\varphi\alpha\hat{\varphi} \otimes m^{-1})_\ell$ and the second takes α to $\varphi_\ell\alpha_\ell\hat{\varphi}_\ell \otimes m^{-1}$ since $m_\ell = m$. So functoriality gives $m\varphi_\ell \otimes m^{-1} = \varphi_\ell^{-1}$ on $\mathrm{V}_\ell(B)$. So $\mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Z}_\ell$ consists of all those elements of $\mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Q}_\ell$, taking $\mathrm{T}_\ell(B)$ back to itself. So

$$\{\alpha \mid \iota_B(\alpha) \in \mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Z}_\ell\} = \{\alpha \mid \alpha(\varphi_\ell^{-1}(\mathrm{T}_\ell(B)) \subseteq \varphi_\ell^{-1}(\mathrm{T}_\ell(B))\}.$$

This is quite a computational criterion. $\varphi_\ell^{-1}(\mathrm{T}_\ell(B))$ is a lattice in $\mathrm{V}_\ell(A)$ whose quotient by $\mathrm{T}_\ell(A)$ is the ℓ-primary part of $\ker(\varphi)$. Similar results hold at p.

Example With $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ as above, let $\iota_B(\alpha) \in \mathrm{End}_{\mathbb{F}_q}(B)$ be an isogeny. Let $R = \iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$ and let $S = \hat{\iota}_\varphi(\mathrm{End}_{\mathbb{F}_q}(B)))$. Then $S = \alpha^{-1}R\alpha$. To see this apply the above construction to it. $\hat{\iota}_B \in \mathrm{End}_{\mathbb{F}_q}(B) \otimes \mathbb{Z}_\ell$ if and only if $\iota_B(\lambda)_\ell$ takes $\iota_B(\alpha)_\ell^{-1}(\mathrm{T}_\ell(B))$ to itself, if and only if $\iota_B(\alpha\lambda\alpha^{-1})_\ell$ takes $\mathrm{T}_\ell(B)$ to itself, if and only if $\iota_B(\alpha\lambda\alpha^{-1}) \in \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Z}_\ell$. Up to change of variance. The same holds for p. Now $\mathrm{End}_{\mathbb{F}_q}(B)$ is determined by it's localizations, so $\hat{\iota}_B(\lambda) \in \mathrm{End}_{\mathbb{F}_q}(B)$ if and only if $\iota_B(\alpha\lambda\alpha^{-1}) \in \mathrm{End}_{\mathbb{F}_q}(B)$, if and only if $\alpha\lambda\alpha^{-1} \in R$, if and only if $\lambda \in \alpha^{-1}R\alpha$. □

The above example shows how the propositions will be used. Given a representative for some B in the isogeny class of A, they give us the localizations of R and like any lattice in L, R is determined by it's localizations. To avoid misconceptions, it should be pointed out that the isomorphism type of $\mathrm{End}_{\mathbb{F}_q}(B)$ is not determined by it's localizations.

Example Consider case (c) in Theorem 3.3.9. Suppose the characteristic polynomial of the abelian variety A is a square of a linear polynomial. We will see later that in this case the representatives are exactly the maximal $\mathbb{Z}$-orders in the definite quaternion algebra over $\mathbb{Q}$ ramified at exactly p and ∞. For $\ell \neq p$, $L_\ell \cong \mathbb{M}_2(\mathbb{Q}_\ell)$. If $R = \iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$, then R_ℓ is a maximal $\mathbb{Z}_\ell$-order in $\mathbb{M}_2(\mathbb{Q}_\ell)$ and all such are isomorphic. L_p is a division algebra, and so it has a unique maximal $\mathbb{Z}_p$ order. But we know that for most p the quaternion algebra will have non-isomorphic maximal $\mathbb{Z}$ orders. □

To summarize, each $B \in [A]_{\sim\mathbb{F}_q}$, the $\mathbb{Z}$-order, R in L, which occur as an representative for B is determined up to conjugacy, which is the same thing as isomorphism preserving the Frobenius endomorphism.

Proposition 3.5.4 *Let $B \in [A]_{\sim\mathbb{F}_q}$ be such that there exists a ring isomorphism*

$$\lambda : \mathrm{End}_{\mathbb{F}_q}(A) \to \mathrm{End}_{\mathbb{F}_q}(B)$$

mapping the Frobenius endomorphism of A to the Frobenius endomorphism of B. Then $B \in [A]_{\equiv\mathbb{F}_q}$.

Proof From the arguments above we know that A and B are isogenous. We choose a C in the isogeny class and consider $R = \iota_A^{-1}(\mathrm{End}_{\mathbb{F}_q}(A))$ and $S = \iota_B^{-1}(\mathrm{End}_{\mathbb{F}_q}(B))$ as $\mathbb{Z}$-orders in $L = \mathrm{End}_{\mathbb{F}_q}(C) \otimes \mathbb{Q}$. Let $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ be an isogeny. We have an $\alpha \in S$ with $\alpha R \alpha^{-1} = S$. Then $\iota_B(\alpha)$ is an isogeny giving us a new $\hat{\iota}_B$ for which $\hat{\iota}_B^{-1}(\mathrm{End}_{\mathbb{F}_q}(B)) = R$. Hence $\gamma = \iota_B(\alpha)\varphi$ has the desired property. □

Any attempt to describe isomorphism classes of representatives in L is two-fold. Find the $\mathbb{Z}$-orders R in L such that R represents some $A \in [C]_{\sim \mathbb{F}_q}$ and given such an R, find all possible other abelian varieties in the isogeny class such that R represents them.

Lemma 3.5.5 *Let R be an arbitrary $\mathbb{Z}$-order in L. If R is representing some B in $[A]_{\sim \mathbb{F}_q}$ then π_A and $q\pi_A^{-1}$ is in R.*

Proof By hypothesis R represents B, so there exists an isogeny $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ such that $\iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B)) = R$. Clearly π_A is in R as $\iota_\varphi(\pi_B) = \pi_A$. Suppose that $q = p^n$ and recall that the Frobenius automorphism π over $\mathbb{Z}/p\mathbb{Z}$ takes B to its conjugate variety $B^{(p)}$. Doing this n times brings us back to B and $\pi^n = \pi_B$. Now $\ker(\pi) \subseteq A[p]$ and there is a functorial map $p\pi^{-1} : B^{(p)} \to B$ with $\pi p \pi^{-1} = p\pi^{-1}\pi = p$. So $(p\pi^{-1})^n$ is an endomorphism of B with $(\pi)^n(p\pi^{-1})^n = p^n = q$ so $\iota_\varphi((p\pi^{-1})^n) = q\pi^{-1}$. □

Note that the converse is not necessarily true. An $\mathbb{Z}$-order in L might contain these elements and not be a representative. We'll see an example of this later on.

3.5.4 Kernel Ideals

Here we make a connection between kernels living as finite subgroups inside an abelian variety and the ideals in it's representatives. For any isogeny in $\mathrm{Hom}_{\mathbb{F}_q}(A, B)$, we fix a variety C which is in the isogeny class of A and B, take $L = \mathrm{End}_{\mathbb{F}_q}(C) \otimes \mathbb{Q}$ as it's endomorphism algebra and consider $\mathbb{Z}$-orders in L which occur as representatives for A and B.

Let A be a g-dimensional abelian variety with representative R in L.

For any left ideal, M of R, for M to be a $\mathbb{Z}$-lattice in L is equivalent to M containing an isogeny. Indeed, if M is a $\mathbb{Z}$-lattice in L then it contains $n \otimes 1$ for large n and if M contains an isogeny, φ, then it contains $\deg(\varphi)\alpha$ for all α in R.

If M satisfies any of these equivalent conditions, we will call M an integral left R-ideal. For such a M we define

$$\mathrm{G}_{\ker}(M) = \bigcap_{\alpha \in M} \ker(\alpha)$$

as the intersection of the kernels of all elements of M and we define the kernel ideal of M as $\mathrm{I}_{\ker}(M) = \{\alpha \in R \mid \alpha(\mathrm{G}_{\ker}(M)) = 0\}$.

$M \subseteq \mathrm{I}_{\ker}(M)$ and we will call M a kernel ideal if $M = \mathrm{I}_{\ker}(M)$. An integral left R-ideal M need not be a kernel ideal and the property of being a kernel ideal depends on A not just on the ring R.

Clearly $\mathrm{G}_{\ker}(M)$ is a finite subgroup of A and so we've constructed an isogenous abelian variety $A/\mathrm{G}_{\ker}(M)$ in $[A]_{\sim_{\mathbb{F}_q}}$. This quotient will be refered to in short as the abelian variety associated to M. We want to show that this construction only depends on the R-module structure of M.

Proposition 3.5.6 *Let G and H be two finite subgroups of A. Then $A/G \cong A/H$ if and only if for some isogeny $\alpha \in R$ and some non-zero $n \in \mathbb{Z}$, $\alpha^{-1}G = n^{-1}H$.*

Proof See [39] Proposition 3.6. □

Proposition 3.5.7 *Let M be an integral left R-ideal and let $B = A/\mathrm{G}_{\ker}(M)$ be the associated isogenous abelian variety.*

(a) Let N be another integral left R-ideal. If M and N are isomorphic as left R-modules, then $B \cong_{\mathbb{F}_q} A/\mathrm{G}_{\ker}(N)$.

(b) Let $\varphi : A \to B$ be the canonical map.

(i) $\mathrm{O}_{\mathrm{right}}(M) \subseteq \iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$ and equality holds if $M = \mathrm{I}_{\ker}(M)$.

(ii) For any integral left $\iota_\varphi(\mathrm{End}_{\mathbb{F}_q}(B))$-ideal, N let $\lambda : B \to B/\mathrm{G}_{\ker}(N)$ denote the canonical map. Then for the integral left R-ideal MN and the associated abelian variety $A/\mathrm{G}_{\ker}(MN)$ we have the canonical map as $\lambda\varphi : A \to A/\mathrm{G}_{\ker}(MN)$.

(c) Suppose $M = \mathrm{I}_{\ker}(M)$ and let N be another integral left R-ideal such that $N = \mathrm{I}_{\ker}(N)$. Then M and N are isomorphic as left R-modules if and only if $B \cong_{\mathbb{F}_q} A/\mathrm{G}_{\ker}(N)$ if and only if $M = N\alpha$ for some invertible α in L.

Proof See [39] Proposition 3.9 and Theorem 3.11. □

Pectora roborant cultus recti

Since L is semisimple, it is a direct sum of simple algebras and the maximal $\mathbb{Z}$-order is necessarily just a direct sum of maximal $\mathbb{Z}$-orders in the components. In particular, projections on components are in $\mathcal{O}_L$, so every integral left ideal I is a direct sum of left ideals, one in each component. Now if M is an integral ideal in a maximal $\mathbb{Z}$-order, $\mathcal{O}$, in a simple algebra of dimension m^2 over it's center, the ordinary norm $\mathrm{norm}(M) = \#\mathcal{O}/M$ is an m^{th} power and we will call the m^{th} root the reduced norm of M. This is multiplicative under proper multiplication. Finally we let $\overline{\mathrm{n}}\mathrm{orm}(I)$ be the product of the reduced norms of the components.

Proposition 3.5.8 *Let M be an integral left R-ideal.*

(a) Suppose $M = \mathrm{I}_{\ker}(M)$. Then $M\alpha = \mathrm{I}_{\ker}(M\alpha)$ for every isogeny $\alpha \in R$.

(b) Suppose R is a maximal $\mathbb{Z}$-order in L. Then R is a representative for some isogenous variety in $[A]_{\sim_{\mathbb{F}_q}}$ and $A/\mathrm{G}_{\ker}(M)$ has a maximal representative. Moreover $M = \mathrm{I}_{\ker}(M)$ and $\mathrm{rank}_{\mathbb{Z}}(\mathrm{G}_{\ker}(M)) = \overline{\mathrm{n}}\mathrm{orm}(M)$.

Proof Take $\varphi \in R$ and suppose that for all v, $M\alpha v = 0$ implies $\varphi v = 0$. Then in particular $\alpha v = 0$ implies $\varphi v = 0$ and so $\varphi \mathrm{G}_{\ker}(M\alpha) = 0$ which implies $\varphi \in R\alpha$. Let $\varphi = \beta\alpha$, thus for

all v, $M\alpha v = 0$ implies $\beta\alpha v = 0$. Now being an isogeny, α is surjective, so for all γ, $M\gamma = 0$ implies $\beta\gamma = 0$. As $M = \mathrm{I}_{\ker}(M)$, $\beta \in M$ and so $\varphi = \beta\alpha \in M\alpha$. Now assume R is a maximal order in L and let Λ be a representative for some $B \in [A]_{\sim\mathbb{F}_q}$. As Λ is a lattice in L, we have $m\Lambda \subseteq R$ for some integer m. Let $M = \Lambda n R$. M is a left ideal in Λ and $R \subseteq \mathrm{O}_{\mathrm{right}}(M)$ Hence $R \subseteq \iota_\lambda(\mathrm{End}_{\mathbb{F}_q}(B/\mathrm{G}_{\ker}(M))$ where λ is the projection map $\lambda : B \to B/\mathrm{G}_{\ker}(M)$. As R is maximal it must be equal to Λ and thus R is a representative. Since R is maximal we know that $\mathrm{O}_{\mathrm{right}}(M)$ is also maximal and it follows that $\iota_\lambda(\mathrm{End}_{\mathbb{F}_q}(B/\mathrm{G}_{\ker}(M))$ is a maximal $\mathbb{Z}$-order in L. For the last statement of (b) see [39] Theorem 3.15. □

Note that even in the simplest cases (that of dimension 1) not every variety isogenous to A need to be of the form $A/\mathrm{G}_{\ker}(M)$. Theorem 3.5.8(b) shows that if A has a non-maximal representative then there exists an isogenous variety B with maximal representative such that B is not of the form $A/\mathrm{G}_{\ker}(M)$.

If we restrict to maximal representatives, the last part in Theorem 3.5.8 tells us that we have an action of the Brandt groupoid of L on the isomorphism classes of abelian varieties in $[A]_{\equiv\mathbb{F}_q}$, but this action will not in general be transitive, even if L is commutative. The next theorem tells us it is closely related to questions of separability.

Theorem 3.5.9 *Suppose A is simple over $\mathbb{F}_q$ and identify the Frobenius endomorphism π_A with a Weil q-number π. Assume further that L is commutative.*

(a) Assume R is the maximal $\mathbb{Z}$-order in L which is a representative for some B in $[A]_{\sim\mathbb{F}_q}$. The ideal class group of R acts freely on $\{[C]_{\cong\mathbb{F}_q} |\ C \in [B]_{\equiv\mathbb{F}_q}\}$. For a place P of L lying above p. Let $g_P = \gcd(\mathrm{rcd}(L_P/\mathbb{Q}_p), \mathrm{ord}_p(q))$ and define a set N_P of ordered tuples

$$N_P = \{(n_1, \ldots, n_{g_P}) \mid 0 \le n_1 \le \ldots, n_{g_P} \le \mathrm{ram}(L_P/\mathbb{Q}_p) \text{ and } \sum_{i=1}^{g_P} n_i = \frac{g_P \cdot \mathrm{ord}_P(\pi)}{\mathrm{ord}_p(q)}\}.$$

Then the number of orbits is equal to $\prod_P \#(N_P)$ where P ranges over all the places of L lying above p. Furthermore two abelian varieties are in the same orbit if and only if there is a separable isogeny between them.

(b) Let L^+ be the totally real subfield of index 2 in L. Suppose p splits completely in L^+ and that $\mathcal{O}_{L^+} \subseteq R \subseteq \mathcal{O}_L$ with $\mathcal{O}_L$ and $\mathcal{O}_{L^+}$ the maximal $\mathbb{Z}$-order in L and L^+ respectively.

(i) R_p is maximal.

(ii) The class group of R operates freely on the isomorphism classes $\{[C]_{\cong\mathbb{F}_q} |\ C \in [B]_{\equiv\mathbb{F}_q}\}$. There are 2^s orbits where s is the number of prime factors of p in L^+ staying prime in L.

(iii) Two classes are in the same orbit if and only if there is a separable isogeny between them.

In this case the $\mathbb{Z}$-orders R in L which are representatives for some $B \in [A]_{\sim\mathbb{F}_q}$ are exactly those containing π_A and $\mathcal{O}_{L^+}$.

Proof For the first part we construct a representation of L_p on $\mathrm{V}_p(A)$ and compute the lattices involved. We already know that every ideal is a kernel ideal and Theorem 3.5.7 (c) shows that the class group acts and every orbit is a principal homogeneous space. Note that in every ideal class there is an ideal prime to p. Theorem 3.5.8 (b) then shows that the corresponding isogeny has degree prime to p and hence is separable. Thus two curves in the same orbit are connected by separable isogenies.
For case (b) we have that any rank 1 R-module, M with $\mathrm{O}_{\mathrm{right}}(M) = R$, is invertible so it makes sense to talk about the class group. Also every integral ideal I has it's localization at $\ell \neq p$ determined, and every lattice away from p can be obtained from an integral ideal in R. The idea is then to look more closely at the invariant lattices at p and deduce that R_p is the maximal order. This is done in [39] Theorem 5.3 and the rest then follows from (a) □

We remark that $\mathbb{Z}$-lattices M, such that $\mathrm{O}_{\mathrm{right}}(M) = R$ need not be projective R-modules, for example there might exists a $\mathbb{Z}$-lattice M, and distinct integral ideals $I \subset J$, such that $IM = JM$. This shows that for an appropriately chosen A, not all integral ideals are kernel ideals, and hence the property of being a kernel ideal depends on the variety chosen.

Inside the isogeny class and the class of varieties with representative R, there is a naturally defined subset: The varieties with $\mathrm{T}_p(A)$ and all $\mathrm{T}_\ell(A)$ for $\ell \neq p$ are free. From these and only these we can get others as $A/\mathrm{G}_{\mathrm{ker}}(M)$. They form a principal homogeneous space over the class group of R.

Proposition 3.5.10 *Suppose that all abelian varieties are simple and defined over the prime field $\mathbb{F}_p$. Let L be the endomorphism algebra of A. Then there are two cases.*

(a) $K = \mathbb{Q}(\pi)$ contains no real prime and the following holds true.

(i) L is communative.

(ii) All $\mathbb{Z}$-orders in L containing $q^{-1}\pi$ and π are representatives for some B in $[A]_{\sim_{\mathbb{F}_p}}$ and for each such representative, R, there is a is a bijection

$$\{[C]_{\cong_{\mathbb{F}_q}} \mid C \in [B]_{\equiv_{\mathbb{F}_p}}\} \leftrightarrow \{[M]_{\cong} \mid M \text{ is a } \mathbb{Z}-\text{lattice in } L \text{ with } \mathrm{O}_{\mathrm{right}}(M) = R\}.$$

(b) $K = \mathbb{Q}(\pi)$ contains a real prime and

$$\mathrm{h}(L) = \#\{[B]_{\cong_{\mathbb{F}_p}} \mid B \text{ has a maximal representative in } L\}.$$

Furthermore if $p \not\equiv 1 \bmod 4$, then there are no other representatives in L, whilst there are more otherwise correponding to $\mathbb{Z}$-orders in L of index 8 and 16.

Proof Since we are working over the prime field, in the case where there are no real primes, $\mathrm{inv}_P(L) \in \mathbb{Z}$ and so $L = K$ is always commutative. In this case we can always get any $\mathbb{Z}$-order containing π at $\ell \neq p$. But here $[K : \mathbb{Q}] = 2g = \dim_{\mathbb{Q}_p}(\mathrm{V}_\ell(A))$. Thus $\mathrm{V}_p(A)$ is free of rank 1 over K_p, so at p we can choose any lattice invariant under π and $q\pi^{-1}$. Suppose now a representative R is given. For all but finitely many ℓ, R_ℓ will be maximal and so $\mathrm{T}_\ell(A)$ will be free of rank 1 over it. At the other ℓ we can select a lattice free of rank 1 over R_ℓ. Then by an isogeny we can get an A with $\mathrm{T}_p(A)$ and all $\mathrm{T}_\ell(A)$ free of rank 1. For such an

A clearly every ideal of R is a kernel ideal, and the associated varieties with representative R are those ideals whose order is precisely R. Once we note that every lattice with order R is isomorphic to an ideal of R, Theorem 3.5.8 (b) completes the proof of part (a). Suppose now there is a real prime. This is the case where $K = \mathbb{Q}(\sqrt{p})$ and L is the quaternion algebra over K ramified at the two real primes. Since $\sqrt{p}$ and $-\sqrt{p}$ are conjugate, there is only one isogeny class. The endomorphism ring must contain $\mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{p}]$ which is the maximal $\mathbb{Z}$-order in K if $p \not\equiv 1 \bmod 4$ but has index two otherwise.
For $p \not\equiv 1 \bmod 4$, we look more carefully over $\mathbb{Q}_2$. Suppose $\ell \neq 2$, $\ell \neq p$ and $p \equiv 1 \bmod 4$. There are two cases. Suppose ℓ stays prime or ramifies in K. Then K_ℓ is a field and $L_\ell = \mathbb{M}_2(K_\ell)$ acts on a 2-dimensional K_ℓ-space. The endomorphism ring contains $\sqrt{p}$ and so the whole maximal order of K_ℓ, so the lattices we want are K_ℓ-lattices. The $\mathbb{Z}_\ell$-orders in L_ℓ preserving these lattices are the maximal ones and all lattices are conjugate. If ℓ splits in K, then $K_\ell = \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$ and $L_\ell = \mathbb{M}_2(\mathbb{Q}_\ell) \oplus \mathbb{M}_2(\mathbb{Q}_\ell)$. Since we know the maximal order in $\mathbb{Q}_\ell$, we get a maximal order in each $\mathbb{M}_2(\mathbb{Q}_\ell)$ and the product will give us a maximal order in L_ℓ and again we can pass from any lattice to another. At p we have K_p is a field. $\mathrm{V}_p(A)$ is a 2 dimensional K_p space, $L_p = \mathbb{M}_2(K_p)$ and the argument is the same as for K_ℓ. Suppose first $p \equiv 5 \bmod 8$. Then 2 stays prime in K and $L_2 = \mathbb{M}_2(K_2)$. Let $\lambda = \frac{1}{2}(1+\sqrt{p})$, so that $\{1, \sqrt{p}\}$ forms a $\mathbb{Z}_2$-basis for the maximal order in K_2. Let Λ be any lattice in $\mathrm{V}_2(A)$ with basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. We can choose α_1 and α_2 linearly independant over K_2 and write α_3 and α_4 as integral combinations over K_2. Subtracting scalar multiples of α_1 and α_2 we can make α_3 and α_4 into $\mathbb{Z}_2$-linear combinations of $\lambda\alpha_1$ and $\lambda\alpha_2$. Changing by unimodular $\mathbb{Z}_2$-matrices we may assume $\alpha_3 = b\lambda\alpha_1$ and $\alpha_4 = c\lambda\alpha_2$ with b dividing c. For this to be preserved by $\mathbb{Z}[\pi]_2 = \mathbb{Z}_2 + 2\lambda\mathbb{Z}_2$, we need b dividing 2 and c dividing 2. Thus the possible lattices are $\{\alpha_1, \lambda\alpha_1, \alpha_2, \lambda\alpha_2\}$, $\{\alpha_1, \lambda\alpha_1, \alpha_2, 2\lambda\alpha_2\}$ and $\{\alpha_1, 2\lambda\alpha_1, \alpha_2, 2\lambda\alpha_2\}$. Writing the elements of L_2 in terms of the basis $\{\alpha_1, \alpha_2\}$, we find the first one gives us a maximal order, the second an order of index 8 and the third an order of index 16.
Finally consider $p \equiv 1 \bmod 8$. $K_2 = \mathbb{Q}_2 \oplus \mathbb{Q}_2$ and $L_2 = \mathbb{M}_2(\mathbb{Q}_2) \oplus \mathbb{M}_2(\mathbb{Q}_2)$. If Λ is any $\mathbb{Z}_2$ lattice in $\mathbb{Q}_2^2 \times \mathbb{Q}_2^2$, we can choose a basis of four elements so that the first two lies in the first summand. Conjugating by an element of L_2 to change basis in each summand, we may assume the basis is of the form $\{(1,0,0,0), (0,1,0,0), (a,b,1,0), (c,d,0,1)\}$. This must be preserved by $(\sqrt{p}, -\sqrt{p})$ in $\mathbb{Q}_2 \oplus \mathbb{Q}_2$ or equivalently by $(2\sqrt{p}, 0)$ which means that $2a, 2b, 2c, 2d \in \mathbb{Z}_2$. Since we can change a, b, c, d by elements of $\mathbb{Z}_2$ and can permute the basis elements in each summand. If we calculate all the lattices, we get 1 maximal order and the rest corresponding to orders of index 8 and 16. □

3.6 Ordinary abelian varieties

An abelian variety A over $\mathbb{F}_q$ is ordinary if the rank of its group of p-torsion points over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ is equal to the dimension of A. Ordinary abelian varieties have commutative endomorphism rings but as we will se later the converse is not nessacarily true.

In this section we fix an ordinary g-dimensional abelian variety A over $\mathbb{F}_q$, associate its Frobenius endomorphism with a Weil q-number π and let $L = \mathrm{End}(A) \otimes \mathbb{Q}$ be its endomorphism algebra. It follows from Theorem 3.3.9 that $L = \mathbb{Q}[\pi]$ is a commutative semisimple $\mathbb{Q}$-algebra with $[L : \mathbb{Q}] = 2g$. Furthermore since L is commutative and separable as $\mathbb{Q}$-algebra we know that there exists a unique $\mathbb{Z}$-order in L namely the integral closure of $\mathbb{Z}$

in L which we will denote by $\mathcal{O}_L$.

For an ordinary abelian variety we always have that all endomorphisms are defined over $\mathbb{F}_q$ and so A is always stable under base field extension. Since $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ we will simply write $\mathrm{End}(A)$.

3.6.1 Weil correspondences

A Weil polynomial is ordinary if it is the characteristic polynomial of Frobenius of an ordinary abelian variety and a Weil number is ordinary if its minimal polynomial is an ordinary Weil polynomial. For example, a monic polynomial over $\mathbb{Z}$ is an ordinary Weil q-polynomial if and only if it is of even degree $2g$, all of its roots are Weil numbers, and its middle coefficient (that is, the coefficient of x^g) is coprime to q (not divisible by p). Furthermore, an ordinary abelian variety A over $\mathbb{F}_q$ is simple if and only if its Weil polynomial χ is irreducible.

The Honda-Tate theorem (Theorem 3.4.2) simplifies considerably if one considers only the ordinary case.

Theorem 3.6.1 *The map*

$$\begin{array}{rccc} \varphi: & \{[A]_{\sim_{\mathbb{F}_q}} \mid A \text{ is an abelian variety over } \mathbb{F}_q\} & \to & \{\chi \mid \chi \text{ is a Weil } q-\text{polynomial}\} \\ & [A]_{\sim_{\mathbb{F}_q}} & \mapsto & \chi \end{array}$$

induces a bijection between the the set of isogeny classes of ordinary abelian varieties over $\mathbb{F}_q$ and the set of ordinary Weil q-polynomials under which isogeny classes of simple ordinary abelian varieties correspond to irreducible ordinary Weil q-polynomials.

Proof This theorem follows easily from the standard Honda-Tate theorem (Theorem 3.4.2) and from the fact that for simple ordinary abelian varieties A, the polynomial χ is irreducible. □

Proposition 3.6.2 *Let A be a simple ordinary g-dimensional abelian variety over $\mathbb{F}_q$. We identify the Frobenius endomorphism with a Weil q-number π and let $L = \mathrm{End}(A) \otimes \mathbb{Q}$ be the endomorphism algebra of A. Then χ is a $\mathbb{Q}$-irreducible polynomial and $L = \mathbb{Q}(\pi)$ is isomorphic to the number field defined by χ. In fact L is a totally imaginary quadratic extension of a totally real number field L^+.*

Proof In the notation of Theorem 3.3.8, $r = 1$ if and only χ is irreducible, if and only if $\mathrm{End}(A)$ is commutative. Further $\mathrm{End}(A)$ is commutative if and only if there are no real primes and for all primes P of L lying over p, $\mathrm{ord}_p(q)$ divides $[L_P : \mathbb{Q}_p]$. So L is totally imaginary with $2g = [L : \mathbb{Q}]$. Consider $\alpha = \pi + q\pi^{-1}$. Under every embedding $\pi\epsilon_{\mathbb{C}}(\pi) = q$ and $|\pi| = q^{\frac{1}{2}}$ and it follows that $\alpha = \pi + \epsilon_{\mathbb{C}}(\pi)$ is totally real. Thus $L^+ = \mathbb{Q}(\alpha)$ is totally real and L is quadratic over it. Earlier remarks show that π satisfies the equation $\pi^2 - \alpha\pi + q = 0$. The fact that the solution of this equation is totally imaginary means that under every embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{R}$, $|\alpha| \leq 2q^{\frac{1}{2}}$. Conversely if α is any totally real algebraic integer satisfying this condition then the solution of $\pi^2 - \alpha\pi + q = 0$ will be a Weil q-number such that L is quadratic over $L^+ = \mathbb{Q}(\alpha)$. □

Finally it is useful to note that ordinary Weil q-polynomials have a special form.

Proposition 3.6.3 *Suppose that $\chi = x^{2g} + a_{2g-1}x^{2g-1} + \ldots + a_1 x + a_0$ is an ordinary Weil q-polynomial. Then $x^{2g}\chi(\frac{q}{x}) = q^g\chi(x)$, we have $a_0 = q^g$ and $a_i = q^{g-i}a_{2g-i}$ for all $i = 1, 2, \ldots, g$.*

Proof If χ had a real root then it would have a $\mathbb{Q}$-irreducible factor of the form $x \pm q^{\frac{1}{2}}$ or $x^2 - q$, depending on whether or not $q^{\frac{1}{2}}$ is an integer and no ordinary Weil q-polynomial can have such a factor. Thus χ factors over $\mathbb{R}$ as a product of polynomials of the form $x^2 - tx + q$, so we have $a_0 = q^g$. Since the complex roots of χ all have magnitude $q^{\frac{1}{2}}$ it follows that $x^{2g}\chi(\frac{q}{x}) = a_0\chi(x) = q^g\chi(x)$. The statement of the symmetry of the coefficients of χ follows immediately from this equality. □

3.6.2 Endomorphism rings

For $B \in [A]_{\sim\mathbb{F}_q}$ and isogenies $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ and $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ of degree m and n respectively, the induced injections into L yields the same embedding. For all $\alpha \in \mathrm{End}(B)$

$$\begin{aligned}
\iota_\lambda(\alpha) &= n\lambda^{-1}\alpha\lambda \otimes n^{-1} \\
&= n\lambda^{-1}(\varphi m\varphi^{-1})\alpha(\varphi m\varphi^{-1})\lambda \otimes n^{-1}m^{-2} \\
&= (n\lambda^{-1}\varphi)m\varphi^{-1}\alpha\varphi m(\varphi^{-1}\lambda) \otimes n^{-1}m^{-2} \\
&= m\varphi^{-1}\alpha\varphi(n\lambda^{-1}\varphi)(m\varphi^{-1}\lambda) \otimes n^{-1}m^{-2} \\
&= m\varphi^{-1}\alpha\varphi \otimes m^{-1} = \iota_\varphi(\alpha).
\end{aligned}$$

where the second last step relies on the commutativity of $\mathrm{End}(B)$. So the embedding is independant of choice of isogeny and B has only one $\mathbb{Z}$-order $\iota(\mathrm{End}(B))$ representing it.

For simple ordinary abelian varieties all conceivable $\mathbb{Z}$-orders actually occur as representatives for abelian varieties $B \in [A]_{\sim\mathbb{F}_q}$.

Theorem 3.6.4 *Let A be a simple ordinary abelian variety over $\mathbb{F}_q$ with endomorphism algebra $L = \mathrm{End}(A) \otimes \mathbb{Q}$.*

(a) $\{B \in [A]_{\sim\mathbb{F}_q} \mid \iota(\mathrm{End}(B)) = \mathcal{O}_L\}$ forms a principal homogeneous space for the ideal class group of $\mathcal{O}_L$.

(b) The $\mathbb{Z}$-orders R in L which are representatives for some $B \in [A]_{\sim\mathbb{F}_q}$ are exactly those $\mathbb{Z}$-orders in L containing π and $q\pi^{-1}$

Proof See [39] Theorem 7.4. □

In part Theorem 3.6.4 (a) we can be less restrictive. The result still holds if A is not ordinary as long as $\mathrm{End}(A)$ is commutative and stable under base field extension, however, the example after the proof of Theorem 7.4 in [39] shows how (b) fails if A is not ordinary even if $\mathrm{End}(A)$ is commutative and stable under base field extention.

One very nice property of ordinary abelian varieties we should mention is that they have canonical liftings to characteristic zero.

3.6.3 The ring associated to an isogeny class

Let A be an ordinary abelian variety over $\mathbb{F}_q$ and suppose A factors up to isogeny as

$$A \sim_{\mathbb{F}_q} \prod_{i=1}^{t} A_i^{n_i}.$$

We identify the Frobenius endomorphism of A with a Weil q-number π and consider the subring $R = \mathbb{Z}[\pi, q\pi^{-1}]$ of $\mathrm{End}(A)$. We have seen that every representative of an element in the isogeny class of A contains this $\mathbb{Z}$-algebra and if A is a simple ordinary abelian variety then every $\mathbb{Z}$-order in L containing R is a representative for some element in $[A]_{\sim \mathbb{F}_q}$. So it is important to us to be able to calculate the discriminant of R. In this section we will give formulas for the discriminant in terms of the coefficients of the characteristic polynomial χ_A.

The quotient ring $K = R \otimes \mathbb{Q}$ of R is a product of CM-fields

$$K = \prod_{i=1}^{t} K_i$$

and clearly R is a $\mathbb{Z}$-order in K. Consider the subset

$$K^+ = \prod_{i=1}^{t} K_i^+$$

of K where K_i^+ denotes the maximal real subfield if K_i. Let $R^+ = R \cap K^+$. The $\mathbb{Z}$-order R^+ is totally real, that is, every ring homomorphism from R^+ to $\mathbb{C}$ maps R^+ into $\mathbb{R}$.

Lemma 3.6.5 *The elements π and $q\pi^{-1}$ generate the unit ideal in R, $R^+ = \mathbb{Z}[\pi + q\pi^{-1}]$ and R is a free R^+-module of rank 2 generated by 1 and π.*

Proof Let χ be the Weil q-polynomial corresponding to the isogeny class $[A]_{\sim \mathbb{F}_q}$ via Theorem 3.6.1. Then χ is the characteristic polynomial of π so $\chi(\pi) = 0$. We may interpret this equality as an identity in $K = R \otimes \mathbb{Q}$ and by dividing the equality by π^g and using relations among the coefficients of χ given in Proposition 3.6.3 we see that the middle coefficient a_g of χ can be written as a $\mathbb{Z}$-linear combination of powers of π and $q\pi^{-1}$ Thus a_g is an element of the ideal of R generated by π and $q\pi^{-1}$ and since this ideal also contains $q = \pi q \pi^{-1}$, it contains 1 as well, because a_g is coprime to q. In other words, π and $q\pi^{-1}$ generate the unit ideal. The rest follows from the facts that $R = R^+[\pi]$ with π is quadratic over R^+ and for every minimal prime P of R the image of π in R/P is quadratic over the image of R^+. $\square$

We define the radical of χ_A as the product of all $\mathbb{Q}$-irreducible factors of χ_A, each taken once and denote it by $\mathrm{Rad}(\chi_A)$. The polynomial $\mathrm{Rad}(\chi_A)$ is an ordinary Weil q-polynomial. Let $2n$ be its degree and write $\mathrm{Rad}(\chi_A) = x^{2n} + b_{2n-1}x^{2n-1} + \ldots + b_1 x + b_0$.

Proposition 3.6.6 *With notation as above we have*

$$\mathrm{disc}(R) = (-1)^n \mathrm{disc}(R^+)^2 \mathrm{norm}(\pi - q\pi^{-1})$$

where

$$\mathrm{norm}(\pi - q\pi^{-1}) = q^{-n}((\sum_{i=0}^{n} b_{2i}q^i)^2 - q(\sum_{i=0}^{n-1} b_{2i+1}q^i)^2) \text{ with } b_{2n} = 1.$$

Furthermore if n is even, say $n = 2m$ then

$$\mathrm{norm}(\pi - q\pi^{-1}) = (b_n + 2\sum_{i=0}^{m-1} b_{2n-2i}q^{m-i})^2 - q(2\sum_{i=0}^{m-1} b_{2n-(2i+1)}q^{m-(i+1)})^2.$$

Proof The proof of this proposition are mainly computational and we will only give brief outlines. It is not hard to show that the ring isomorphism, $\mathbb{Z}[x,y] \to R,\ x \mapsto \pi,\ y \mapsto q\pi^{-1}$, induces an isomorphism $R \cong \mathbb{Z}[x,y]/\langle \varphi_1, \varphi_2 \rangle$ where $\varphi_1 = xy - q$ and $\varphi_2 = (x^n + y^n) + b_{2n-1}(x^{n-1} + y^{n-1}) + \ldots + b_{n+1}(x+y) + b_n$. Now consider the ring $\mathbb{Z}[x,y]/\langle \omega \rangle$ with

$$\omega = \omega_n + b_{2n-1}\omega_{n-1} + \ldots b_{n+1}\omega_1 + b_n$$

$$\omega_i = 2q^{\frac{i}{2}} t_i(\tfrac{1}{2}xq^{\frac{1}{2}}) \text{ and}$$

$$t_i(x) = \cos(i\cos^{-1}(x)) \text{ the Chebyshev polynomial.}$$

By noting that $t_i(x)$ have integer coefficients, that $t_i(\pi, q\pi^{-1}) = (\pi)^i + (q\pi^{-1})^i$ and that $\varphi_2(\pi, q\pi^{-1}) = 0$, it easily follows that ω is the minimal polynomial of $\pi + q\pi^{-1}$. In particular $R^+ = \mathbb{Z}[\pi + q\pi^{-1}] \cong \mathbb{Z}[x,y]/\langle \omega \rangle$ and $\mathrm{disc}(R^+) = \mathrm{disc}(\omega)$. The idea is now that the ring R can be built up in two steps from $\mathbb{Z}$. First adjoin a root of ω to $\mathbb{Z}$ to obtain R^+ and then adjoin a root of $x^2 + (\pi + q\pi^{-1})x + q$ to R^+ to obtain R. One can show that as $\mathbb{Z}$-order we have the dual of R^+ as $\hat{\epsilon}(R^+) = (\omega'(\pi + q\pi^{-1}))^{-1}R^+$. Similarly we have the dual of R as R^+-module as $\hat{\epsilon}(R) = (\pi - q\pi^{-1})^{-1}R$. Thus the dual of R as $\mathbb{Z}$-module is $\hat{\epsilon}(R) = ((\pi - q\pi^{-1})\omega'(\pi + q\pi^{-1}))^{-1}R$. The absolute value of the discriminant of a $\mathbb{Z}$-algebra is the index in its dual, so $|\mathrm{disc}(R)| = |\mathrm{disc}(R^+)|^2 |\mathrm{norm}(\pi - q\pi^{-1})|$. If we keep track of the signs of the expressions in the last equality we get the first statement of the proposition. Let χ be the minimal polynomial for π^2, so that $\mathrm{norm}(a - \pi^2) = \chi(a)$ for all $a \in \mathbb{Q}$. Since $\dim_{\mathbb{Q}}(K)$ is even we have $\mathrm{norm}(\pi^2 - q) = \mathrm{norm}(q - \pi^2)$, so we find that

$$\mathrm{norm}(\pi - q\pi^{-1}) = \frac{\mathrm{norm}(\pi^2 - q)}{\mathrm{norm}(\pi)} = \frac{\chi(q)}{q^n}.$$

If we write χ in terms of the coefficients of the minimal polynomial of π, we find that this last equality is the second equality in the statement of the proposition. When n is even, the third statement follows from Proposition 3.6.3 and the second equality. □

3.7 Supersingular abelian varieties

Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$ of characteristic p with q elements. Let χ be the characteristic polynomial of the Frobenius endomorphism π of A relative to $\mathbb{F}_q$. An abelian variety A over $\mathbb{F}_q$ is supersingular if each complex root of χ

can be written as $\zeta_m\sqrt{q}$, the product of some root of unity ζ_m and the positive square root $\sqrt{q}$.

3.7.1 Supersingular Weil numbers

Let $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}}$ for any positive integer m. The primitive m^{th} roots of unity are the ζ_m^r with positive integers r that are coprime to m. Throughout this section Φ be denote the Euler Φ-function. An algebraic number $\pi \in \mathbb{C}$ is called a supersingular Weil q-number if it is of the form $\zeta_m\sqrt{q}$ for some primitive m^{th} root of unity ζ_m.

Let $\pi = \zeta_m\sqrt{q}$ be an supersingular Weil q-number. Suppose $K = \mathbb{Q}(\pi)$, $F = \mathbb{Q}(\pi^2)$ and let $\mathcal{O}_K$, $\mathcal{O}_F$ be the ring of integers of K, F respectively.

For the rest of this section fix $t = \frac{m}{\gcd(2,m)}$ and $\tau = \begin{cases} -1 & \text{if } -1 \text{ is not a square mod } p. \\ 1 & \text{if } -1 \text{ is a square mod } p. \end{cases}$
Obviously $F = \mathbb{Q}(\zeta_t)$ and $[K : F] = 1$ or 2.

Lemma 3.7.1 *Suppose q is a non-square and let $d = \operatorname{disc}(\mathbb{Q}(\sqrt{p}))$. Then $K = F$ if and only if*

(a) d divides m and

(b) d does not divide t if 4 divides m.

In this case 2 divides $\operatorname{rcd}(P/p)$ for any prime P of $\mathcal{O}_K$ lying over p.

Proof We note $K = \mathbb{Q}(\zeta_t, \sqrt{p\zeta_t}) = F(\sqrt{p\zeta_t})$. Thus $K = F$ if and only if $\sqrt{\zeta_t p} \in F$, and if and only if $F(\sqrt{p}) = F(\sqrt{\zeta_t})$. That is, $\mathbb{Q}(\zeta_t, \sqrt{p}) = \mathbb{Q}(\zeta_m)$. This is equivalent to $\sqrt{p} \in \mathbb{Q}(\zeta_m)$ and $\sqrt{p} \notin \mathbb{Q}(\zeta_t)$ if 4 divides m which is equivalent to saying $\sqrt{p} \in \mathbb{Q}(\zeta_m)$ if and only if $\operatorname{disc}(\mathbb{Q}(\sqrt{p}))$ divides m. To show the second assertion it is enough to prove it for just one prime P over p since all primes lying over p are conjugate as K is equal to the cyclotomic field $\mathbb{Q}(\zeta_t)$. We claim $p \cdot \gcd(2, p)$ divides t. In fact, if $p = 2$ then (a) implies 8 divides m, but

$$\operatorname{disc}(\mathbb{Q}(\sqrt{p})) = \begin{cases} p & \text{if } p \equiv 1 \bmod 4, \\ 4p & \text{if } p \not\equiv 1 \bmod 4, \end{cases}$$

and so our claim follows. If $p \neq 2$ then (a) implies $p \cdot \gcd(2, p) = p$ divides m. But since $p \neq 2$, we have that $p \cdot \gcd(2, p)$ divides t. But if $p \neq 2$ and p divides m then $\mathbb{Q}(\sqrt{\tau p}) \subseteq \mathbb{Q}(\zeta_m)$. Thus $\mathbb{Q}(\zeta_t)$ contains a quadratic field $\mathbb{Q}(\sqrt{\tau p})$ over $\mathbb{Q}$ where p is totally ramified. Hence 2 divides $\operatorname{rcd}(P/p)$. □

Proposition 3.7.2 *Suppose A is a g-dimensional simple supersingular abelian variety over $\mathbb{F}_q$ and identify the Frobenius endomorphism with a Weil q-number $\pi = \zeta_s\sqrt{q}$. Let $L = \operatorname{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be the endomorphism algebra. Then the characteristic polynomial χ is a power of a $\mathbb{Q}$-irreducible polynomial.*

(a) Let D be the set of all supersingular Weil q-numbers $\zeta_m\sqrt{q}$ for some primitive m^{th} root of unity ζ_m such that, if m factors as $m = p^k n$, then either $m \in \{1, 2\}$ or q is

a square, $p \cdot \gcd(2,p)$ does not divide m and p is of odd order in the group $(\mathbb{Z}/n\mathbb{Z})^*$. We have the following two cases.

(i) When $\pi \in D$ then $[K:F]=2$ and L is a quaternion algebra over K.

(ii) When $\pi \notin D$ then L is commutative and equal to K.

(b) Suppose A is of odd dimension $g>2$, then $L=K$ and L must be commutative.

Proof Let P be any place of K (including both finite and infinite primes). Let e_P be the denominator of the Hasse invariant $\mathrm{inv}_P(L)$ of L at P. We have

$$\mathrm{inv}_P(L) = \frac{\mathrm{ord}_P(\pi)[K_P:\mathbb{Q}_p]}{\mathrm{ord}_P(q)} = \frac{[K_P:\mathbb{Q}_p]}{2} = \frac{\mathrm{ram}(P/p)\cdot \mathrm{rcd}(P/p)}{2}$$

for all primes P lying over p, so $e_P = 1$ or 2. Now $e_P = 1$ for all complex P and also for all finite primes P not lying over p, while $e_P = 2$ for all real P. Suppose χ is the e^{th}-power of a $\mathbb{Q}$-irreducible polynomial, then $e = \mathrm{lcm}_P(e_P) = 1$ or 2 and so it remains to show that $e_P = 2$ for some P if and only if $\pi \in D$. That $e = 1$ or 2 is equivalent to having real primes P and so $e_P = 2$. Below we consider two cases: Suppose q is not a square. We claim that $e_P = 1$ for all finite primes P over p. Now $[K:F] = 1$ or 2. The former implies 2 divides $\mathrm{ram}(P/p)$. Consider the latter case, if $\sqrt{p} \in K$, then 2 divides $\mathrm{ram}(P/p)$ and so $e_P = 1$. Otherwise, we would have quadratic extensions $F \subset K \subset \mathbb{Q}(\zeta_m, \sqrt{p})$. But if p was unramified in $K = E$, then it would be unramified in $\mathbb{Q}(\zeta_m, \sqrt{p})/\mathbb{Q}(\zeta_m)$, which is absurd, so we must conclude that p is (totally) ramified in K/F and hence 2 divides $\mathrm{ram}(P/p)$ and so $e_P = 1$. Suppose q is a square, so that $K = \mathbb{Q}(\zeta_m)$. Then for any finite prime P over p, we have that $\mathrm{rcd}(P/p)$ equals the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ and $\mathrm{ram}(P/p) = \Phi(\frac{1}{n}m)$. Thus $e_P = 2$ if and only if the product $\mathrm{ram}(P/p)\cdot\mathrm{rcd}(P/p)$ is odd, i.e. if and only if $p\cdot\gcd(2,p)$ does not divide m and the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$ is odd. This finishes the proof of (a). Recall that $2g = e[K:\mathbb{Q}]$ and so to prove (b) it suffices to show 2 divides $[K:F][\mathbb{Q}(\zeta_t):\mathbb{Q}]$. Either $[K:F] = 1$ or 2, in the former case $[\mathbb{Q}(\zeta_t):\mathbb{Q}] = \Phi(t) > 1$ and so is even. □

We next determine all minimal polynomials of supersingular Weil q-numbers.

Let $\tau_1(a) = 1$,

$$\tau_2(a) = \begin{cases} 0 & \text{if 2 divides } a, \\ (-1)^{\frac{1}{8}(a^2-1)} & \text{if 2 does not divide } a, \end{cases}$$

and for an integer a and an odd integer b define

$$\tau_b(a) = \begin{cases} 0 & \text{if } b \text{ divides } a. \\ 1 & \text{if } b \text{ is a square modulo } a. \\ -1 & \text{if } b \text{ is not a square modulo } a. \end{cases}$$

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ for some the primitive m^{th} root of unity, ζ_m, consists of all the σ_i defined by $\sigma_i(\zeta_m) = \zeta_m^i$ with i coprime to m and $1 \le i \le m$. We claim that $\sqrt{p} \in \mathbb{Q}(\zeta_m)$ implies $\sigma_i(\sqrt{p}) = \tau_i(p)\sqrt{p}$. Since they are both multiplicative, it suffices to show that $\sigma_\ell(\sqrt{p}) = \tau_\ell(p)\sqrt{p}$ for each prime ℓ dividing i. If ℓ is odd, then

$$\sigma_\ell(\sqrt{p}) \equiv (\sqrt{p})^\ell = p^{\frac{1}{2}(\ell-1)}\sqrt{p} \bmod \ell$$

and thus $\sigma_\ell(\sqrt{p}) = \tau_\ell(p)\sqrt{p}$. Suppose $\ell = 2$. Since m is odd, our hypothesis implies that

$$\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_m).$$

Denote by $\overline{\sigma}_2$ the image of σ_2 in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, then $\sigma_2(\sqrt{p}) = \overline{\sigma}_2(\sqrt{p}) = \sqrt{p}$ or $-\sqrt{p}$. It equals the former if and only if $\overline{\sigma}_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p}))$, that is, if and only if 2 is a square in $(\mathbb{Z}/p\mathbb{Z})^*$. Thus $\sigma_2(\sqrt{p}) = \tau_2(p)\sqrt{p}$.

Proposition 3.7.3 *Let χ be the minimal polynomial a given supersingular Weil $q-$number, π and let $K = \mathbb{Q}(\pi)$, $E = \mathbb{Q}(\pi^2)$ and $F = \mathbb{Q}(\sqrt{p})$. Define χ_m be the m^{th} cyclotomic polynomial and let $[\pi]$ denote the conjugacy class of π.*

(a) If q is square, then $[\pi] = [\zeta_m\sqrt{q}]$ for some m and $\chi = q^{\frac{1}{2}\Phi(m)}\chi_m(\frac{1}{\sqrt{q}}x)$.

(b) If q is nonsquare, then $[\pi] = [\zeta_m^r\sqrt{q}]$ for some primitive m^{th} root of unity ζ_m^r such that $m \not\equiv 2 \bmod 4$

$$\text{and } \begin{cases} \chi = q^{\frac{t}{m}\Phi(m)}\chi_t(\frac{1}{q}x^2) \text{ if } K \neq E. \\ \chi = \prod_{i\in\mathbb{Z}} (x \mp \tau_i(q)\zeta_m^r\sqrt{q}),\ 1 \leq i \leq t,\ \gcd(i,t) = 1 \text{ if } K = E. \end{cases}$$

Proof Part (a) is straightforward. We shall show part (b). Write $\pi = \zeta_m^r\sqrt{q}$ for some primitive m^{th} root of unity ζ_m^r. If 2 divides m, then since $\frac{1}{2}m$ is odd we have that

$$\pi = -\zeta_{\frac{1}{2}m}^{\frac{1}{4}r(m+2)}\sqrt{q} \text{ and } \pi \in [\zeta_{\frac{1}{2}m}^k\sqrt{q}] \text{ for some primitive } \tfrac{1}{2}m^{\text{th}} \text{ root of unity, } \zeta_{\frac{1}{2}m}^k.$$

Thus we may assume $m \not\equiv 2 \bmod 4$ for the rest of the proof. Now $[K : E] = 1$ or 2. Let $\mathrm{disc}_E(K)$ denote the discriminant of the number field extension K/E. It can shown that $K = E$ if and and only $\mathrm{disc}_{\mathbb{Q}}(F)$ divides m and $2\mathrm{disc}_{\mathbb{Q}}(F)$ does not divide m. Suppose $[K : E] = 2$. It is not hard to see that π is a root of χ and χ is in fact its minimal polynomial since χ has degree $2\frac{t}{m}\Phi(m)$. So we have

$$[K : \mathbb{Q}] = \frac{[K : \mathbb{Q}(\zeta_t)][\mathbb{Q}(\zeta_m) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_t)]}$$

with $[K : \mathbb{Q}] = 2\frac{t}{m}\Phi(m)$. Suppose $[K : E] = 1$. Then $\sqrt{p} \in \mathbb{Q}(\zeta_m)$ and so by the argument preceding the proposition we have $\sigma_i(\pi) = \sigma_i(\zeta_m^r\sqrt{q}) = \tau_i(q)\zeta_m^{ir}\sqrt{q}$ for all $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_t)/\mathbb{Q})$. So we have

$$\chi = \textstyle\prod_{i\in I} (x \mp \tau_r(q)\zeta_m^{ri}\sqrt{q})$$

as the minimal polynomial of π since π is of degree $\Phi(t)$. □

3.7.2 Additional structure

With the example in section 2.1.4 and the comments which follows thereafter in mind we let L be a finite field extension over a number field, K, with ring of integers R. In preparation for the upcoming material, we state below a few lemmas from algebraic number theory.

Lemma 3.7.4 *Suppose $\Lambda = R[\alpha]$ and $\omega \in R[x]$ is the minimal polynomial of α. Let P be any non-zero prime ideal of R. There is a bijective correspondence between the set of prime ideals S of Λ over P and the set of monic irreducible factors $\overline{\upsilon}$ of*

$$\overline{\omega} = \omega \bmod P \in (R/P)[x].$$

If S corresponds to $\overline{\upsilon}$ in this bijection, then $S = (P, \upsilon(\alpha))$ in Λ. Also $\mathrm{rcd}(S/P) = \dim_{R/P}(\Lambda/S) = \deg(\overline{\upsilon})$ and $\mathrm{ram}(S/P)$ equals the multiplicity of $\overline{\upsilon}$ as a factor of $\overline{\omega}$.

Proof See [24] Chapter I, Proposition 25 on p.27. □

Lemma 3.7.5 *Let the notation be as in the previous lemma. Let υ be monic. The prime ideal $S = (P, \upsilon(\alpha))$ of Λ is not invertible if and only if $\overline{\upsilon}^2$ divides $\overline{\omega}$ and all coefficients of the remainder of ω upon division by υ are in P^2. The R_P-order Λ_P is non-maximal if and only if there is a monic irreducible factor $\overline{\upsilon}$ of $\overline{\omega}$ such that $\overline{\upsilon}^2$ divides $\overline{\omega}$, and all coefficients of the remainder of ω upon division by υ are in P^2.*

Proof Consider the surjective map $\tau : R[x] \to R[\alpha] = \Lambda$, write $M = \tau^{-1}(S) = P[x] + \upsilon R[x]$ and so $\tau^{-1}(S^2) = M^2 + \omega R[x]$. Hence

$$S/S^2 = M/(M^2 + \omega R[x]) \cong (M/M^2)/N$$

where N is the submodule generated by the image of ω. Recall from the previous lemma that $d = \deg(\overline{\upsilon}) = \dim_{R/P}(\Lambda/S)$. For $h \in R[x]$, we write h in base g and obtain $h = r_2\upsilon^2 + r_1\upsilon + r_0$ for some $r_2, r_1, r_0 \in R[x]$ with $\deg(r_0), \deg(r_1) < d$. Then $h \in M$ if and only if $r_0 \in P[x]$, while $h \in M^2$ if and only if $r_1 \in P[x]$ and $r_0 \in P^2[x]$. Therefore we find $\dim_{\Lambda/S}(M/M^2) = 1 + \dim_{R/P}(P/P^2) = 2$ and $\dim_{\Lambda/S}(N) = 0$ if $\omega \in M^2$ and is 1 otherwise. Thus, by the isomorphism above, we have $\dim_{\Lambda/S}(S/S^2) = \dim_{\Lambda/S}(M/M^2) - \dim_{\Lambda/S}(N) = 2 - \dim_{\Lambda/S}(N)$, which is 1 when $\omega \notin M^2$ and is 2 when $\omega \in M^2$. We conclude that S is not invertible if and only if $\omega \in M^2$, which is equivalent to $\overline{\upsilon}^2$ dividing $\overline{\omega}$ and all coefficients of the remainder of ω upon division by υ are in P^2.
The R_P-order Λ_P is a product of Λ_S for those finitely many primes S in Λ lying over P. Thus Λ_P is maximal if and only if each Λ_S is a discrete valuation ring, for example, its only prime S over P is invertible. The second assertion then follows from the first and the bijective correspondence in the previous lemma. □

Corollary 3.7.6 *Let the notation be as in Lemma 3.7.4. If υ is linear, say, $\upsilon = x - \lambda$ with $\lambda \in R$, then S is not invertible if and only if $\omega(\lambda) \equiv 0$ mod P^2 and $\omega'(\lambda) \equiv 0$ mod P, where ω' denotes the derivative of ω.*

Proof The condition that $\overline{\upsilon}^2$ divides $\overline{\omega}$ is equivalent to that of $\omega(\lambda) \equiv 0 \bmod P$ and $\omega'(\lambda) \equiv 0 \bmod P$. The condition that all coefficients of the remainder of ω upon division by υ are in P^2 is equivalent to $\omega(\lambda) \equiv 0 \bmod P^2$. □

For a elementary supersingular abelian variety over $\mathbb{F}_q$ with associated Frobenius element, π, we will show that the ring $\mathbb{Z}[\pi] = \mathbb{Z}[\zeta_m\sqrt{q}]$ is locally almost a discrete valuation ring at every prime and is in fact a Bass order.

Lemma 3.7.7 *Let $K = \mathbb{Q}[\pi]$ and $F = \mathbb{Q}[\pi^2]$ be the $\mathbb{Q}$-subalgebras of $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ with maximal $\mathbb{Z}$-orders $\mathcal{O}_F$ and $\mathcal{O}_K$ respectively. Set $R = \mathbb{Z}[\pi]$ to be the $\mathbb{Z}$-subalgebra of $\mathcal{O}_K$ generated by π. Define D to be the set of supersingular Weil $q-$numbers, $\zeta_m\sqrt{q}$, with q not a square and which satisfy the following conditions:*

$$p \neq 2,\ p \text{ does not divide } m \text{ and } \begin{cases} \text{if } p \equiv 3 \bmod 4, \text{ then } 4 \text{ divides } m. \\ \text{if } p \equiv 1 \bmod 4, \text{ then } 4 \text{ does not divide } m. \end{cases}$$

Let ℓ be rational prime different from p.

(a) If $(\ell, \pi) \notin \{2\} \times D$, then $R_\ell = (\mathcal{O}_K)_\ell$.

(b) If $(\ell, \pi) \in \{2\} \times D$ then $R_2 \subset (\mathcal{O}_K)_2$. Let P be any prime in $\mathcal{O}_F$ lying over 2, then

(i) K is a quadratic extension over F

$$\text{where } \begin{cases} P \text{ is split if } p \equiv \pm 1 \bmod 8 \text{ and} \\ P \text{ is inert if } p \equiv \pm 3 \bmod 8. \end{cases}$$

(ii) R_P is a Bass order over $(\mathcal{O}_F)_P$ such that $(\mathcal{O}_K)_P$ is the only $(\mathcal{O}_F)_P$-order in K_P that properly contains R_P. Moreover, $(\mathcal{O}_K)_P/R_P \cong (\mathcal{O}_F)_P/P$ as $(\mathcal{O}_F)_P$-orders in K_P.

Proof If q is a square, then $\pi \notin D$ and $R_\ell = \mathbb{Z}[\zeta_m]_\ell = (\mathcal{O}_K)_\ell$, so for the rest of the proof, we assume q is not a square. We consider the following two cases.
We set $\tau = -1$ if -1 is not a square mod p or otherwise we let $\tau = 1$. Case 1. Suppose $\ell \neq 2$ or p divides m. We claim $R_\ell = (\mathcal{O}_K)_\ell$. Since $\ell \neq p$, we note that $\mathbb{Z}[\pi^2]_\ell = \mathbb{Z}[\zeta_t]_\ell = (\mathcal{O}_F)_\ell$. Suppose $\ell \neq 2$, obviously $\mathbb{Z}[\pi^2]_\ell = (\mathcal{O}_F)_\ell \subseteq R_\ell \subseteq (\mathcal{O}_K)_\ell$. If $K = F$ then $(\mathcal{O}_K)_\ell = (\mathcal{O}_F)_\ell$ and so $R_\ell = (\mathcal{O}_K)_\ell$. If $K \neq F$ then $[\mathcal{O}_K : R]_\ell^2$ divides $\mathrm{disc}(R)$ but since $R \cong \mathcal{O}_F[x]/\langle x^2 - q\zeta_t \rangle$, we have $\mathrm{disc}(R) = \mathcal{O}_F \cdot \mathrm{disc}(x^2 - q\zeta_t^r) = 4q\mathcal{O}_F$. So $(\mathrm{disc}(R))_\ell = (\mathcal{O}_F)_\ell$ since $4q$ is coprime to ℓ. Therefore $[\mathcal{O}_K : R]_\ell$ is the unit ideal and so $R_\ell = (\mathcal{O}_K)_\ell$.
Now let $\ell = 2$ and suppose p divides m. If $p \neq 2$ and p divides m then $\mathbb{Q}(\sqrt{\tau p}) \in \mathbb{Q}(\zeta_m)$, thus $\sqrt{\tau p} \in \mathbb{Z}[\zeta_t]_2 = \mathbb{Z}[\pi^2]_2 \subseteq R_2$. Moreover, the norm of $\sqrt{\tau p}$ over $\mathbb{Q}$ is $\pm p$ which is coprime to 2 so $\sqrt{\tau p}$ is a unit in R_2. Therefore, $R_2 = \mathbb{Z}[\pi\sqrt{\tau p}]_2 = \mathbb{Z}[\zeta_m^r\sqrt{\tau}]_2$. This proves our claim.
Case 2. Suppose $\ell = 2$ and that p does not divide m. Write $m = 2^k s$. It is easy to verify that $K = \mathbb{Q}(\zeta_s, \alpha)$ where $\alpha = \zeta_{2^k}^\mu\sqrt{p}$ for some 2^k-th primitive root of unity $\zeta_{2^k}^\mu$. We note that $\mathbb{Q}(\zeta_s)$ and $\mathbb{Q}(\alpha)$ are linearly disjoint and that the minimal polynomial of α over $\mathbb{Q}(\zeta_s)$ is

$$h = \begin{cases} x^{2^{k-1}} + p^{2^{k-2}} & \text{if } k \geq 2, \text{ and} \\ x^2 - p & \text{if } k < 2. \end{cases}$$

Let S be any prime ideal in the ring of integers of $\mathbb{Q}(\zeta_s)$ lying over 2. We show $R_S = \mathbb{Z}[\zeta_s, \alpha]_S$. The inclusion $R_S \subseteq \mathbb{Z}[\zeta_s, \alpha]_S$ is trivial. Conversely, since $\pi^{2^k} = \zeta_s^{2^k} q^{2^{k-1}}$ and $\alpha = \pi\zeta_s^{-\mu}$, we have $\zeta_s, \alpha \in R_S$. Thus $\mathbb{Z}[\zeta_s, \alpha]_S \subseteq R_S$. That is, $R_S = \mathbb{Z}[\zeta_s, \alpha]_S$. Hence, $R_S = (\mathbb{Z}[\zeta_s]_S)[\alpha]$.
If $k \geq 2$, then $h \equiv (x-1)^{2^{k-1}} \bmod S$. Note that $\mathbb{Z}[\zeta_s]_S$ is a discrete valuation ring, so we have by Corollary 3.7.6 that R_S is not maximal if and only if $h(1) = 1 + q^{2^{k-2}} \equiv 0 \bmod S^2$, that is, $k = 2$ and $p \equiv 3 \bmod 4$. Similarly, if $k < 2$ then $h \equiv (x-1)^2 \bmod S$ and so R_S

is not maximal if and only if $p \equiv 1 \bmod 4$. Note $R_2 = \prod_{S|2} R_S$. By Lemma 3.7.5 and the above argument, R_2 is not maximal if and only if $\pi \in D$.
In the case $\pi \in D$, we have $F = \mathbb{Q}(\zeta_s)$ and $K = F(\sqrt{\tau p})$ is quadratic over F. The decomposition of P in this quadratic extension K over F corresponds to that of 2 in $\mathbb{Q}(\sqrt{\tau p})$ over $\mathbb{Q}$, which is as in our assertion. Since R_P is a quadratic order over the complete discrete valuation ring $(\mathcal{O}_F)_P$, it is a Bass order (by the example in section 2.1.4). As $(\mathcal{O}_F)_P$-orders, we have $R_P \subset (\mathcal{O}_K)_P \cong (\mathcal{O}_F)_P^2$. There is an injection $R_P/(\mathcal{O}_F)_P \to (\mathcal{O}_K)_P/(\mathcal{O}_F)_P \cong (\mathcal{O}_F)_P$, under which $R_P/(\mathcal{O}_F)_P \cong P^m(\mathcal{O}_F)_P$ for some positive integer m. In other words, $R_P = (\mathcal{O}_F)_P + P^m(\mathcal{O}_K)_P$ and so $(\mathcal{O}_K)_P/R_P \cong (\mathcal{O}_F)_P/P^m$. But

$$\operatorname{disc}(R_P) = (\mathcal{O}_F)_P \cdot \operatorname{disc}(x^2 - \tau p) = 4(\mathcal{O}_F)_P$$

and hence $[(\mathcal{O}_K)_P : R_P]^2 = [(\mathcal{O}_F)_P : P^m]^2 = 2^{2m}(\mathcal{O}_F)_P$ which divides $4(\mathcal{O}_F)_P$. Thus $m = 1$, that is, $(\mathcal{O}_K)_P/R_P \cong (\mathcal{O}_F)_P/P$ as $(\mathcal{O}_F)_P$-modules. Hence $(\mathcal{O}_K)_P$ is the only $(\mathcal{O}_F)_P$-order in K_P that properly contains R_P. □

Chapter 4

Hyperelliptic curves over finite fields

We now get to the most interesting part of this thesis. In this chapter we will look at examples of abelian varieties which arise as Jacobians of hyperelliptic curves and look at the algebras which contain their endomorphism rings. We work out concrete examples to illustrate the theory studied in the previous two chapters. In the most simplest case, where the Jacobian has dimension 1, we develop practical methods to determine the isomorphism class of the endomorphism ring.

4.1 The Jacobian

Let C be a genus g hyperelliptic curve defined over the finite field $\mathbb{F}_q$. We will assume that $\mathbb{F}_q$ has characteristic p different from 2. In this case the affine part of C is defined by the equation

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

with f monic and of degree $2g+1$ and for simplicity we shall say that C is the curve defined by $y^2 = f(x)$. The unique point at infinity on C is denoted by P_∞.

We denote the Jacobian of C by $\mathrm{J}_C(\mathbb{F}_q)$. This is a projective group variety defined over $\mathbb{F}_q$. The canonical injection

$$\begin{aligned} \iota : \ C(\mathbb{F}_q) &\to \mathrm{J}_C(\mathbb{F}_q) \\ P &\mapsto [P - P_\infty] \end{aligned}$$

associates to $P \in C(\mathbb{F}_q)$ the divisor class of $P - P_\infty$ and it is also defined over $\mathbb{F}_q$. For details on the arithmetic of hyperelliptic curves see [22].

Two hyperelliptic curves are said to be isomorphic over a field $\mathbb{F}_q$ if they are isomorphic as projective varieties over $\mathbb{F}_q$. Briefly two projective varieties A and B are isomorphic over $\mathbb{F}_q$ if there exist morphisms $\varphi : \ A \to B$ and $\psi : B \to A$ defined over $\mathbb{F}_q$ such that $\psi\varphi$ and $\varphi\psi$ are identity maps on A and B respectively.

The relation of isomorphism is an equivalence relation on the set of hyperelliptic curves of genus g. If C_1 and C_2 are isomorphic over $\mathbb{F}_q$ then their $\mathbb{F}_q$-Jacobians $\mathrm{J}_{C_1}(\mathbb{F}_q)$ and

$\mathrm{J}_{C_2}(\mathbb{F}_q)$ are also isomorphic as abelian groups. Note however that if $\mathrm{J}_{C_1}(\mathbb{F}_q) \cong \mathrm{J}_{C_2}(\mathbb{F}_q)$ as abelian groups, then this does not imply that C_1 and C_2 are isomorphic as projective varieties.

Example Consider the following curves over $\mathbb{F}_3$.

$$\begin{aligned} C_1 : y^2 &= x^5 + x^3 + x^2 - x - 1 \\ C_2 : y^2 &= x^5 - x^3 + x^2 - x - 1 \end{aligned}$$

The two curves, C_1 and C_2, are not geometrically isomorphic but have isomorphic Jacobians. For a proof of this see [16]. □

We will call a curve ordinary (respectively supersingular) if the Jacobian is ordinary (respectively supersingular) as an abelian variety.

4.1.1 Mumford's representation

If K is an algebraic extension field of $\mathbb{F}_q$, we may distinguish the rational points on curves defined over $\mathbb{F}_q$ and K by $y^2 = f(x)$, by denoting them $C(\mathbb{F}_q)$ and $C(K)$. The injection ι extends to the injection

$$\iota : \ C(K) \to \mathrm{J}_C(K)$$

and the group law on $\mathrm{J}_C(K)$ extends that of $\mathrm{J}_C(\mathbb{F}_q)$. In particular, let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$ and let τ be the hyperelliptic involution on $C(\overline{\mathbb{F}}_q)$. As a consequence of the Riemann Roch theorem, any element in $\mathrm{J}_C(\overline{\mathbb{F}}_q)$ can be uniquely represented by a divisor of the form

$$D = \sum_{j=1}^{r} \iota(P_j)$$

with the following properties

(a) all P_j are points on the affine part of $C(\overline{\mathbb{F}}_q)$,

(b) $P_j \neq \tau(P_k)$ for all $j \neq k$ and

(c) r is at most g.

The integer r is called the weight of the divisor D. Note that since the points P_j are not at infinity, we may take $P_j = [\,\alpha_j, \beta_j, 1\,]$ with respect to the standard embedding in $\mathbb{P}^2$. Then the Mumford representation of D is defined by

$$D = [\,u(x), v(x)\,] = [\,x^r + u_{r-1}x^{r-1} + \ldots + u_0,\ v_{r-1}x^{r-1} + \ldots + v_0\,],$$

where

$$u(x) = \prod_{j=1}^{r}(x - \alpha_j) \ \text{ and } \ v(\alpha_i) = \beta_j$$

holds with suitable multiplicities, so that $u(x)$ divides $v(x)^2 - f(x)$. Since $\mathbb{F}_q$ is perfect, the divisor D is defined over a field K containing $\mathbb{F}_q$ if and only if the polynomials $u(x)$

and $v(x)$ have coefficients in K. For $j = 0, \ldots, r-1$ we will denote by $u_j(D)$ (respectively $v_j(D)$) the coefficient u_j (respectively v_j) in this representation.

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and $P = [\,\alpha, \beta, \,] \in C$, $\sigma(P) = [\,\sigma(\alpha), \sigma(\beta)\,]$ is in C. So σ induces a map on C. This map is extended linearly to $\mathrm{J}_C(\mathbb{F}_q)$ acting pointwise. Crucially this implies that it acts on each coefficient of $u(x)$ and $v(x)$, the polynomials in Mumford's notation, when a divisor is defined over $\mathbb{F}_q$ or might permute its points but leave the divisor as a whole invariant. We may therefore define $A(\mathbb{F}_q) = \mathrm{J}_C(\mathbb{F}_q)$ as the subgroup of $A(\overline{\mathbb{F}}_q) = \mathrm{J}_C(\overline{\mathbb{F}}_q)$ fixed by $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. We know $A(\mathbb{F}_q)$ is finite and in fact $(\sqrt{q}-1)^{2g} \leq \#A(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g}$.

4.1.2 Elliptic curves

The goal of this section is to point out a very special case where everything can be computed explicitly, namely for elliptic curve. In this case the curve is isomorphic to its Jacobian. We will assume all elliptic curves, C over $\mathbb{F}_q$, are given in Weierstrass form

$$C : y^2 = x^3 + ax + b$$

with a and b in $\mathbb{F}_q$. In this case the j-invariant can easily be computed from the formula

$$\mathrm{j}(C) = \frac{6912a^3}{4a^3 + 27b^2}.$$

If two elliptic curves have the same j-invariant then they are isomorphic over $\overline{\mathbb{F}}_q$ ([32] Propositions 3.1.4(b) and 3.3.1.(b)). Furthermore if two elliptic curves over $\mathbb{F}_q$ have the same number of points over $\mathbb{F}_q$ and they are not supersingular then we may explicitly find an isomorphism over $\mathbb{F}_q$. This gives us a way to determine the isomorphism class of an elliptic curve over $\mathbb{F}_q$, which we denote as $[C]_{\cong \mathbb{F}_q}$.

Pectora roborant cultus recti

4.2 Modular equations

Consider a hyperelliptic curve C of genus g, let $A = \mathrm{J}_C(\mathbb{F}_q)$ be its Jacobian, and ℓ a prime. The quotient of the Jacobian by a subgroup of order ℓ is an abelian variety ℓ-isogenous to A, but if the genus is greater than one, it is in general not the Jacobian of a curve. General abelian varieties are more intricate to handle than Jacobians of curves, for which invariants can easily be computed, so we will rather study directly the ℓ-torsion subgroup of the Jacobian. In this section we define the ℓ^{th} modular equations of a genus g hyperelliptic curve defined over a field $\mathbb{F}_q$ using the structure of the ℓ-torsion subgroup. More precisely the equations are univariate polynomials whose roots are in one to one correspondence with the cyclic subgroups of the ℓ-torsion subgroup of A. The definitions avoid the use of modular forms, so they are valid over any perfect field.

Let ℓ be a prime different form the characteristic of K. It can be shown (see [33]) that the number of ℓ-torsion divisors in $A(\overline{\mathbb{F}}_q)$ of non-zero weight is $\ell^{2g} - 1$. For the rest of this section we will assume that every such ℓ-torsion divisor has weight exactly g. This is closely related to the Manin-Mumford conjecture which states that the Jacobian of a curve over $\mathbb{C}$ contains only finitely many torsion elements of weight 1. More generally, Lang's conjecture,

which is now known to be true (See [13] p.435), implies that the Jacobian of a given curve over $\mathbb{C}$ contains only finitely many torsion elements of non-maximal weight, as soon as the Jacobian is simple. As a consequence, for a given curve with simple Jacobian, the number of primes ℓ for which our assumption does not hold is finite. We remark that the assumption holds for all curves of genus 1 since the only divisor whose weight is not maximal is zero.

For a prime ℓ we will denote by $A[\ell]$ the subgroup of the ℓ-torsion elements in $A(\overline{\mathbb{F}}_q)$. Let D be an ℓ-torsion divisor. Each of the sets

$$\langle D\rangle = \{-\frac{1}{2}(\ell-1)D, \ldots, 0, \ldots, \frac{1}{2}(\ell-1)D\}$$

form a cyclic subgroup of cardinality ℓ in $A[\ell]$. Our objective is to separate these subgroups, using only algebraic constructions. To this effect we choose a function $\delta_\ell(D)$ with values in $\overline{\mathbb{F}}_q$, which takes a constant value on each of the subgroups $\langle D\rangle$ The modular equations we construct may then be thought of as a minimal polynomial for δ_ℓ. More precisely we define δ_ℓ as the function

$$\delta_\ell(D) = \sum_{i=1}^{\frac{1}{2}(\ell-1)} u_{g-1}(iD).$$

Our assumption that all ℓ-torsion divisors have weight g implies that the function δ_ℓ is well-defined for all non-zero ℓ-torsion divisors D. Note that iD and $-iD$ have the same ${u_{g-1}}^{\text{th}}$-coordinate, so even though we restrict the number of summands to $\frac{1}{2}(\ell-1)$, δ_ℓ depends only on the subgroup generated by D as required.

We next define the polynomial χ_ℓ in $\overline{\mathbb{F}}_q[t]$, whose roots are the values taken by δ_ℓ on the non-zero ℓ-torsion divisors:

$$\chi_\ell(t) = \prod_{D\in A[\ell]\setminus\{0\}} (t - \delta_\ell(D)).$$

The polynomial χ_ℓ is a $(\ell-1)^{\text{th}}$ power in $\overline{\mathbb{F}}_q[t]$ and is actually a polynomial in $\mathbb{F}_q[t]$. Indeed, $A[\ell]\setminus\{0\}$ can be written as the disjoint union of the $\frac{\ell^{2g}-1}{\ell-1}$ sets $\langle D\rangle\setminus\{0\}$, and the function $\delta_\ell(D)$ takes a constant value on each part of this partition. This proves the first part. Let σ be in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. If D is any divisor, $\sigma(u_{g-1}(D)) = u_{g-1}(\sigma(D))$. Also, σ commutes with the group law, whence $\sigma(iD) = i\sigma(D)$, so σ induces a permutation among the non-zero ℓ-torsion divisors. If D is such a divisor, then $\sigma(\delta_\ell(D)) = \delta_\ell(\sigma(D))$ obviously holds. Since σ permutes the ℓ-torsion divisors, this equality shows that χ_ℓ is left invariant by σ, so χ_ℓ is in $\mathbb{F}_q[t]$.

Since $\mathbb{F}_q$ is a perfect field, and χ_ℓ is a $(\ell-1)^{\text{th}}$ power in $\overline{\mathbb{F}}_q[t]$, there exists a polynomial Ξ_ℓ with coefficients in $\mathbb{F}_q$ such that $\chi_\ell = (\Xi_\ell)^{\ell-1}$. We will call the unique monic polynomial Ξ_ℓ the ℓ^{th} modular equation of C. It has degree $\frac{\ell^{2g}-1}{\ell-1}$ and we will denote it by $\Xi_\ell(C)$ to emphasize the dependance on the curve C.

Our choice of the function δ_ℓ was arbitrary. The interesting case is when Ξ_ℓ is square-free, which happens when δ_ℓ takes distinct values on the distinct cyclic subgroups of $A[\ell]$. Unfortunately it is not be the case for all curves. An alternative choice for δ_ℓ might solve the problem. Instead of considering the sum of the u_{g-1}-coordinates of half the divisors in

the subgroup, we choose some integer k and form the sum of the k^{th} power of any linear combination of all the coordinates $[\,u(x), v(x)\,]$. Then, we might have to extend the summation in the definition of δ_ℓ to all elements in the subgroup $\langle D \rangle$ since not all coordinates are negation-invariant. The subsequent results follow in a similar manner for such alternative constructions.

Computing Ξ_ℓ is a two-stage process. First compute a representation of the ℓ-torsion divisors, then compute the modular equation using this information. In genus 1, the ℓ-torsion divisors are the roots of the elliptic division polynomials and the modular equations come from characteristic polynomial computations modulo these division polynomials.

In genus 2, the torsion divisors can be characterized using Cantor's division polynomials (See [5]) and the computation of Ξ_ℓ is analogous to the elliptic case.

In the general case, as in the genus 2 case, the Mumford-Cantor coordinates of the ℓ-torsion divisors are algebraic over $\mathbb{F}_q$ but in general the multiplication by ℓ-map can not be represented by a single rational function in Mumford-Cantor's coordinates. In [1] Adleman and Huang propose an algorithm that computes a representation of these numbers and once the ℓ-torsion divisors are known, we can compute the modular equation in the same way as in the genus 2 case.

4.2.1 Division polynomials and their analogues

In this section we relate specific polynomials to the torsion groups of the Jacobian of a hyperelliptic curve over a finite field.

Let $C : y^2 = x^3 + ax + b$ be a hyperelliptic curve of genus 1 and let $A = \mathrm{J}_{\mathbb{F}_q}(C)$ be its Jacobian variety. For P be a point on A and n a positive integer, the coordinate of nP are rational functions of P,

$$nP = \left[\frac{\upsilon_n(P)}{\varphi_n(P)^2}, \frac{\omega_n(P)}{\varphi_n(P)^3} \right]$$

where υ_n, ω_n and φ_n are multivariate relatively prime polynomials in $\mathbb{F}_q[x, y]$. We call them the n^{th} division polynomials on A. The first few polynomials are given by $\varphi_0(P) = 0$, $\varphi_1(P) = 1$, $\varphi_2(P) = 2y$, $\varphi_3(P) = 3x^4$ and $\varphi_4(P) = 4y(x^6 + ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$. They satify the following recursive formulas.

$$\varphi_n(P)^2\varphi_{m+1}(P)\varphi_{m-1}(P) - \varphi_m(P)^2\varphi_{n+1}(P)\varphi_{n-1}(P) = \varphi_{m+n}(P)\varphi_{m-n}(P) \text{ for } m > n > 0.$$

$$\varphi_{2k}(P) = \frac{1}{2y}\varphi_k(P)(\varphi_{k+2}(P)\varphi_{k-1}(P)^2 - \varphi_{k-2}(P)\varphi_{k+2}(P)^2) \text{ for } k > 2.$$

$$\varphi_{2k+1}(P) = \varphi_{k+2}(P)\varphi_k(P)^3 - \varphi_{k+1}(P)^3\varphi_{k-1}(P) \text{ for } k \geq 2.$$

One can show that the polynomials $\upsilon_n(P)$, $\omega_n(P)^2$, and also $\varphi_n(P)$ if n is odd, are polynomials in x only. From these univariate polynomials we define

$$\tilde{u}_0(P) = -\frac{\varphi_{n-1}(u_0(P))\varphi_{n+1}(u_0(P))}{\varphi_n(u_0(P))^2} \text{ and}$$

$$\tilde{v}_0(P) = \frac{\varphi_{n+2}(u_0(P))\varphi_{n-1}(u_0(P))^2 - \varphi_{n-2}(u_0(P))\varphi_{n+1}(u_0(P))^2}{4v_0(P)\,\varphi_n(u_0(P))^3}.$$

such that

$$nP = [\, x + \tilde{u}_0(P), \tilde{v}_0(P)\,].$$

Now let C be a hyperelliptic curve of genus $g \geq 2$ over $\mathbb{F}_q$ and let $A = \mathrm{J}_{\mathbb{F}_q}(C)$ be its Jacobian. Cantor gives an efficient algorithm using calculations in imaginary quadratic function fields to do group operations with unique representatives of any equivalence class, D in $A(\mathbb{F}_q)$. He defines division polynomials of hyperelliptic curves generalizing the genus one case and gives an efficient recursion to build them.

For the genus 2 case he provides a sequence of univariate polynomials d_0, d_1, d_2 and e_0, e_1, e_2 of degrees $2n^2-1$, $2n^2-2$, $2n^2-3$ and $3n^2-2$, $3n^2-2$, $3n^2-3$ respectively. From these univariate polynomials we define

$$\tilde{u}_i(D) = \frac{d_{2-i}(-u_0(D))}{d_0(-u_0(D))} \quad \text{for } i = 0, 1.$$

$$\tilde{v}_i(D) = \frac{v_0(D)e_{2-i}(-u_0(D))}{e_0(-u_0(D))} \quad \text{for } i = 0, 1.$$

such that

$$nD = \left[\, x^2 + \tilde{u}_1(D)x + \tilde{u}_0(D), \tilde{v}_1(D)x + \tilde{v}_0(D)\,\right].$$

D is a n-torsion divisor if and only if $d_1(-u_0(D)) = d_0(-u_0(D)) = 0$. Hence all n-torsion divisors have weight exactly 2 if and only if d_0 and d_1 are coprime polynomials.

For a weight 2 divisor $D = P_1 + P_2 - 2\infty$ with $P_1 = [\, u_0(P_1), v_0(P_1)\,]$ and $P_2 = [\, u_0(P_2), v_0(P_2)\,]$. The condition $nD = 0$ can be restated as $n(P_1 - \infty) = -n(P_2 - \infty)$ where $n(P_1 - \infty)$ and $-n(P_2 - \infty)$ are rational functions in $\mathbb{F}_q[\, u_0(P_1), u_0(P_2), v_0(P_1), v_0(P_2)\,]$. Assume that all n-torsion divisors on A have weight exactly 2 then $n(P_1 - \infty) = -n(P_2 - \infty)$ implies

$$\frac{d_1(u_0(P_1))}{d_0(u_0(P_1))} = \frac{d_1(u_0(P_2))}{d_0(u_0(P_2))},\ \frac{d_2(u_0(P_1))}{d_0(u_0(P_1))} = \frac{d_2(u_0(P_2))}{d_0(u_0(P_2))},\ \frac{v_0(P_1)e_1(u_0(P_1))}{e_0(u_0(P_1))} = -\frac{v_0(P_2)e_1(u_0(P_2))}{e_0(u_0(P_2))}$$

$$\text{and} \quad \frac{v_0(P_1)e_2(u_0(P_1))}{e_0(u_0(P_1))} = -\frac{v_0(P_2)e_2(u_0(P_2))}{e_0(u_0(P_2))}.$$

Further we add the equations $v_0(P_1)^2 = f(u_0(P_1))$ and $v_0(P_1)^2 = f(u_0(P_1))$ to specify that P_1 and P_2 are indeed points on the curve. The inequality $u_0(P_1) \neq u_0(P_2)$ is necessary to discard the obvious solutions $P_1 = -P_2$, but may also eliminate points P_1 such that $n(P_1 - \infty)$ is of 2-torsion and the inequality $d_0(u_0(P_1))e_0(u_0(P_1)) \neq 0$ is equivalent to the assumption that $n(P_1 - \infty)$ has weight 2.

Due to symmetry in (P_1, P_2) for a general curve, the system of equations has $2(n^{2g} - 1)$ solutions, but this number may be less if $n(P_1 - \infty)$ is of 2-torsion or has weight 1, for some n-torsion divisors of the form $D = P_1 + P_2 - 2\infty$. Letting $\mathrm{I}_n \subseteq \mathbb{F}_q[\, u_0(P_1), u_0(P_2), v_0(P_1), v_0(P_2)\,]$ be the ideal defining the solutions of the above system, we thus have to check that I_n has the maximal number of solutions. To this effect we can use a standard effective elimination algorithm such as Grobner bases.

For hyperelliptic curves for genus $g > 2$ we represent the Mumford-Cantor coordinates of the ℓ-torsion divisors for ℓ a prime using the following objects

(a) A function q in $\mathbb{F}_q[\, u_0, \ldots, u_{g-1}, v_0, \ldots, v_{g-1}\,]$ such that q takes $\ell^{2g} - 1$ distinct values on divisors in $A[\ell]\backslash\{0\}$.

(b) The square-free polynomial

$$\tilde{q} = \prod_{D \in A[\ell]\backslash\{0\}} (s - q(D)) \in \mathbb{F}_q[s].$$

(c) The interpolating polynomials $\tilde{u}_0, \ldots, \tilde{u}_{g-1}, \tilde{v}_0, \ldots, \tilde{v}_{g-1}$ in $\mathbb{F}_q[s]$ of degree less than $\ell^{2g} - 1$ such that for all ℓ-torsion divisors D, $\tilde{u}_i$ (respectively $\tilde{v}_i$) takes the value $u_i(D)$ (respectively $v_i(D)$) when evaluated at $q(D)$.

4.2.2 Computing $\Xi_\ell(C)$

In the previous section we gave an overview on how to compute the ℓ-torsion divisors on the Jacobian of a hyperelliptic curve C of arbitrary genus over $\mathbb{F}_q$. We next show how to derive the ℓ^{th} modular equation for C. Suppose C is a hyperelliptic curve of genus 1. Given an odd prime ℓ, the coordinate representing the position of a point along a line perpendicular to the y-axis of the ℓ-torsion points $P = [u_0, v_0]$ are the roots of φ_ℓ. For $i = 1, \ldots, \frac{1}{2}(\ell - 1)$, the denominator in the rational function

$$\frac{v_i(P)}{\varphi_i(P)^2}$$

is coprime to φ_ℓ and the image of this rational function modulo φ_ℓ is a polynomial δ_i in $\mathbb{F}_q[t]$ which gives the abscissa of iP in terms of the abscissa of P, for P of ℓ-torsion. We have

$$\delta_\ell(P) = \sum_{i=1}^{\frac{1}{2}(\ell-1)} \delta_i(u_0(P)).$$

The polynomial χ_ℓ is thus the characterisitic polynomial of

$$\sum_{i=1}^{\frac{1}{2}(\ell-1)} \delta_i \mod \varphi_\ell$$

and the modular equation Ξ_ℓ is the $(\ell - 1)^{\text{th}}$ root of χ_ℓ.

In genus 2 we assume that, with notation of the previous section with $P_1 = (u_0(P_1), v_0(P_1))$, $P_2 = (u_0(P_2), v_0(P_2))$ and $D = P_1 + P_2 - 2\infty$ a weight 2 divisor, that we are in the favorable case of an ideal I_ℓ having $2(\ell^{2g} - 1)$ solutions and that we can compute efficiently modulo I_ℓ. The function δ_ℓ becomes

$$\delta_\ell(D) = \sum_{i=1}^{\frac{1}{2}(\ell-1)} u_1(iD).$$

Roughly speaking we want to compute the δ_ℓ modulo I_ℓ. To this effect for $i = 1, \ldots, \frac{1}{2}(\ell-1)$ we let δ_i be the polynomial in $\mathbb{F}_q[\, u_0(P_1), u_0(P_2), v_0(P_1)v_0(P_2)\,]$ which takes the value $u_1(iD)$ when evaluated on a ℓ-torsion divisor D. To obtain δ_i we compute Mumford-Cantor coordinates of $i(P_1 - \infty) + i(P_2 - \infty)$ with all computations done modulo I_ℓ These computations can be done using Cantor's division polynomials and Cantor's addition algorithm (see [4]). As such they involve divisions modulo I_ℓ which is possible in general but may fail in unlucky cases. If we assume that divisions can be done then χ_ℓ is defined to be the characteristic polynomial of

$$\sum_{i=1}^{\frac{1}{2}(\ell-1)} \delta_i \mod \mathrm{I}_\ell,$$

so it can be computed using linear algebra in the quotient

$$\mathbb{F}_q[\, u_0(P_1), u_0(P_2), v_0(P_1), v_0(P_2)\,]/\mathrm{I}_\ell.$$

Knowing χ_ℓ, we then deduce the modular equation Ξ_ℓ using the squarefree factorization of χ_ℓ. If we write

$$\chi_\ell = p_1^{m_1} \cdots p_k^{m_k}$$

with all p_i pairwise coprime squarefree polynomials in $\mathbb{F}_q[t]$, then all the m_i are multiples of $\ell - 1$ and

$$\Xi_\ell = p_1^{n_1} \cdots p_k^{n_k}$$

with $n_i = (\ell - 1)m_i$ for all i.

Finally we turn to the general case. Let C be a hyperelliptic curve of genus $g > 2$ and suppose we know the objects representing the Mumford-Cantor's coordinates of the ℓ-torsion divisors D. The computation of χ_ℓ follows the same inspiration as in the previous paragraph. Recall that the function $\delta_\ell(D)$ is defined as

$$\delta_\ell(D) = \sum_{i=1}^{\frac{1}{2}(\ell-1)} u_{g-1}(iD).$$

For simplicity assume that the polynomial $\tilde{q}$ is irreducible, so $K = \mathbb{F}_q[s]/\langle\, \tilde{q}\,\rangle$ is a field, and let $\tilde{s}$ be the image of s in K. Since K is a field we can apply Cantor's algorithm to compute multiplication by i in $K[x]$ on the divisor

$$D(\tilde{s}) = [\, x^g + \tilde{u}_{g-1}(\tilde{s})x^{g-1} + \ldots + \tilde{u}_0(\tilde{s}), \tilde{v}_{g-1}(\tilde{s})x^{g-1} + \ldots + \tilde{v}_0(\tilde{s})\,]$$

for any i. Let $\delta_i \in K$ be the u_{g-1}^{th} coordinate of $iD(\tilde{s})$. If we consider δ_i in $\mathbb{F}_q[s]$, then $u_{g-1}(iD) = \delta_i(q(D))$ holds for all ℓ-torsion divisors D. This implies that

$$\delta_\ell(D) = \sum_{i=1}^{\frac{1}{2}(\ell-1)} \delta_i(q(D))$$

also holds for all ℓ-torsion divisors D. Thus the polynomial χ_ℓ is the characteristic polynomial of

$$\sum_{i=1}^{\frac{1}{2}(\ell-1)} \delta_i \mod \tilde{q}.$$

Generally the polynomial $\tilde{q}$ is squarefree but not irreducible and so K is not a field, but a product of fields $K = \prod_{j=1}^{c} K_j$. This might make it impossible to apply the multiplication by i-algorithm on the divisor $D(\tilde{s})$, since this algorithm requires divisions in K. A first solution to obtain χ_ℓ consists in factoring $\tilde{q}$, applying the process described above in each field K_j to obtain the polynomial χ_j and the product of all χ_j is χ_ℓ.

Of course we want to avoid factorization. A better solution is thus using dynamic evaluation techniques. This involves computing the iterates of $D(\tilde{s})$ as if K were a field. The divisions in K are performed using extended gcd computations. When a division occurs where the dividend is not invertible in K, we have found a new factor of $\tilde{q}$. We then pursue the computations modulo each factor and finally multiplying all the results as above. Here the factorization of $\tilde{q}$ is not required.

4.2.3 Factorization patterns

Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$. Let ℓ be a prime such that $\gcd(\ell, q) = 1$ and assume that all ℓ-torsion divisors on the Jacobian, A, have weight exactly g. The polynomial Ξ_ℓ can be factored over $\mathbb{F}_q$. Let π denote the q^{th} power raising action of $\overline{\mathbb{F}}_q$ extended to C and to A. The ℓ-torsion subgroup $A[\ell]$ can be viewed as a $\mathbb{F}_\ell$-vector space of dimension $2g$ on which π acts as an endomorphism.

Lemma 4.2.1 *Assume that Ξ_ℓ is squarefree and let D and E be non-zero torsion divisors. Then $\delta_\ell(D) = \delta_\ell(E)$ if and only if $E \in \langle D \rangle$.*

Proof The only if part follows from the definition of δ_ℓ. For the converse, since Ξ_ℓ is squarefree, the number of values taken by δ_ℓ is maximal, therefore two distinct subgroups cannot give the same value. □

We define the modified order of a polynomial χ with coefficients in $\mathbb{F}_q$ as $\overline{\text{o}}\text{rd}(\chi) = \min(N)$ where N is the set $N = \{k \in \mathbb{N}^* | \deg(x^k \mod \chi(x)) = 0\}$.

Lemma 4.2.2 *Let D be a non-zero ℓ-torsion divisor of $A[\ell]$. Consider the $\mathbb{F}_\ell$-vector space $V(D)$ spanned by the galoisian conjugates $\{\pi^n(D) \mid n \in \mathbb{N}\}$. Let χ be the characteristic polynomial of π restricted to $V(D)$. If Ξ_ℓ is squarefree, then $\delta_\ell(D)$ is defined over an extension of $\mathbb{F}_q$ of degree $\overline{\text{o}}\text{rd}(\chi)$.*

Proof Let k be the smallest integer such that $\pi^k(D) \in \langle D \rangle$. Since π fixes $\mathbb{F}_q$, we check $\pi(\delta_\ell(D)) = \delta_\ell(\pi(D))$, and so for all $i \geq 0$ we have $\pi^i(\delta_\ell(D)) = \delta_\ell(\pi^i(D))$. By the definition of k for $i < k$, $\pi^i(D)$ is not in $\langle D \rangle$, so $\delta_\ell(\pi^i(D)) \neq \delta_\ell(D)$ by Lemma 4.2.1. For example $\pi^i(\delta_\ell(D)) \neq \delta_\ell(D)$. Since $\delta_\ell(\pi^k(D)) \neq \delta_\ell(D)$, we have proven that k is the degree of the extension of $\mathbb{F}_q$ where $\delta_\ell(D)$ is defined. □

We now consider the characteristic polynomial of χ of π restricted to the space $V(D)$ generated by the conjugates of D. By the definition of $V(D)$, χ is the minimal polynomial of π restricted to $V(D)$. Let λ be the element of $\mathbb{F}_\ell^*$ such that $\pi^k(D) = \lambda D$. The endomorphism $\pi^k - \lambda \cdot 1$ is trivial on D and on all its conjugates, therefore it is trivial on the whole of $V(D)$. Hence we have $x^k = \lambda \equiv 0 \bmod \chi(x)$. Conversely, let m and a be such that $x^m - a \equiv 0 \bmod \chi(x)$, then π^m is equal to $a \cdot 1$ on $V(D)$ and in particular on D. Therefore m must be an integer larger than or equal to k. It follows that k is minimal among the integers satisfying this property.

Theorem 4.2.3 *Assume Ξ_ℓ is squarefree. Then the endomorphism π of the $\mathbb{F}_\ell$-vector space $A[\ell]$ determines the factorization pattern of Ξ_ℓ over $\mathbb{F}_q$.*

Proof Let M be the matrix of the action of π on a basis B of $A[\ell]$. For all D in $A[\ell]$ expressed as a vector according to the same basis, finding $V(D)$ and the associated polynomial $\chi(x)$ is a matter of elementary linear algebra. The extension where the root of Ξ_ℓ associated to D is defined follows easily. Hence knowing the matrix M gives all the extensions where the roots of Ξ_ℓ are defined, which gives the factorization pattern, because the field of definition is finite. □

In genus 1, the modular equations Ξ_ℓ we've constructed here have the same factorization patterns as the the ones constructed for elliptic curves via modular forms and we state them here for completeness.

We will make use of the notation

$$\underbrace{(n_1)^{a_1}}_{b_1} \cdots \underbrace{(n_k)^{a_k}}_{b_k}$$

for a squarefree polynomial having a_i irreducible factors of degree n_i for $i = 1, \ldots, k$ where $b_i = n_i a_i$.

Let A be an elliptic curve over $\mathbb{F}_q$ and let ℓ be coprime to q. Let $x^2 - cx + q$ be the charactersitic polynomial of the frobenius endomorphism of A. Assume that the modular polynomial Ξ_ℓ is squarefree, then the set of degrees of its irreducible factors is one of the following, where $r \geq 1$.

(a) $(1)(\ell)$ or $(1)^{\ell+1}$ if $c^2 - 4q \equiv 0 \bmod \ell$,

(b) $(1)^2(r)^{\frac{1}{r}(\ell-1)}$ if $c^2 - 4q$ is a non-zero square modulo ℓ and

(c) $(r)^{\frac{1}{r}(\ell+1)}$ if $c^2 - 4q$ is a not a square modulo ℓ.

The first case corresponds to a frobenius endomorphism having a double eigenvalue. According to the presence of one or two blocks in the Jordan decomposition we get one or the other subcase. The second case is the case where there are two distinct eigenvalues and the third case is the non-diagonalizable case.

Example In the following table we illustrate the factorization patterns of a few elliptic curves defined over $\mathbb{F}_{22147}$.

Elliptic curves over $\mathbb{F}_{22147}$		
ℓ	j	Ξ_ℓ
2	6907	$(1)^3$
	12313	$(1)^3$
	21946	$(1)^3$
	17609	$(1)(2)$
	14728	$(1)(2)$
	15062	$(1)^3$
	11531	$(1)(2)$
	17964	$(1)^3$
	120	$(1)^3$
	7169	$(1)(2)$
	14003	$(1)(2)$
	17672	$(1)^3$
3	6907	$(1)(2)$

□

Example Here we work out the factorization patterns of the 3rd modular equation of hyperelliptic curves of genus 2 defined by

$$C \ : \ y^2 = x^5 + 5x^3 + x$$

over $\mathbb{F}_p$. For these curves, it is known that all 3-torsion divisors have weight exactly 2.

Hyperelliptic curves of genus 2 over $\mathbb{F}_p$		
p	χ	Ξ_3
73	$(x^2 + 2x + 73)^2$	$(1)^{40}$
79	$(x^2 - 4x + 79)(x^2 + 4x + 79)$	$(1)^2(2)(3)^2(6)^5$
89	$(x^2 + 89)^2$	$(1)^8(2)^{16}$
131	$(x^2 - 20x + 131)(x^2 + 20x + 131)$	$(4)^{10}$
139	$(x^2 - 12x + 139)(x^2 + 12x + 139)$	$(1)^4(2)^{18}$
157	$(x^2 - 2x + 157)^2$	$(1)^4(3)^{12}$
4111	$(x^2 - 60 * x + 4111) * (x^2 + 60 * x + 4111)$	$(2)^{20}$

□

4.3 Isogenies

In the elliptic case, isogenies can be made explicit. In the first section we briefly review this method which is entirely credited to Velu. For the background on isogenies of elliptic curves we refer the reader to [32] Section 3.4.

4.3.1 Explicit formulas

[32] Corollary 2.2.12 tells us that every isogeny, $\rho \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ of elliptic curves factors as

$$\varphi : \ A \xrightarrow{\pi} A^\sigma \xrightarrow{\delta} B$$

with π the q^{th} power frobenius isogeny and δ a separable isogeny such that $\deg(\delta) = q$ whilst [32] Proposition 3.4.12 assures us that for every subgroup, H of A, there exists a unique separable isogeny $\rho \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ such that $H = \mathrm{G}_{\ker}(\rho)$. It is well known that an isogeny $\rho \in \mathrm{Hom}_{\mathbb{F}_q}(A, B)$ of elliptic curves over $\mathbb{F}_q$ can be expressed as a rational map

$$\rho(x, y) = \left[\frac{\upsilon(x, y)}{\varphi(x, y)^2}, \frac{\omega(x, y)}{\varphi(x, y)^3} \right]$$

where υ, ω and φ are univariate polynomials over $\mathbb{F}_q$. Another way to say this is that the polynomials must satisfy the relation

$$\omega^2 = \upsilon^3 + a_2\upsilon\varphi^4 + b_2\varphi^6.$$

The points $P \in A(\overline{\mathbb{F}}_q)$ which are roots of the polynomial $\varphi(x, y)$ are exactly the points in the kernel of the isogeny. If an isogeny ρ is defined over $\mathbb{F}_q$, then its kernel $H = \mathrm{G}_{\ker}(\rho)$ is also defined over $\mathbb{F}_q$. For example $\forall\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, we have $[\,\sigma(u_0), \sigma(v_0)\,] \in H$. Since we assume that all elliptic curves are in Weierstrass form, we have that $P \in H$ if and only if $[\,u_0(P), -v_0(P)\,] \in H$ from which it follows that the kernel of the isogeny ρ is determined by the polynomial

$$\varphi(x) = \prod_{P \in M} (x - u_0(P)) \in \mathbb{F}_q[x].$$

When we say we construct an isogeny we will mean that we explicitly compute the polynomials υ, ω and φ. Velu showed how φ determines the isogeny and Elkies developed methods to calculate $\varphi(x)$ given only the j-invariants of the curves A and B. We will briefly review the ideas of Elkies and Velu.

The following explicit formulas come directly from Velu's paper [37]. We simplified them a little (to the case where p is not 2 or 3). We reproduce them here for convenience of the reader.

Let $C : y^2 = x^3 + ax^2 + bx + c$ be an elliptc curve over $\mathbb{F}_q$. Suppose there is a cyclic subgroup M of order ℓ given by a polynomial $\varphi(x)$, by which we mean

$$M = \{P \in A(\overline{\mathbb{F}}_q) \mid v_0(P) = \pm\sqrt{u_0(P)^3 + au_0(P)^2 + bu_0(P) + c} \ \text{ and } \ \varphi(u_0(P)) = 0\} \cup \{\infty\}.$$

We list the roots of $\varphi(x)$ in two sets: the set

$$F_1 = \{\lambda \in \overline{\mathbb{F}}_q \mid \varphi(\lambda) = 0 \ \text{ and } \ \lambda^3 + a\lambda^2 + b\lambda + c = 0\}$$

will for example have the 2-torsion point $[\,\lambda, 0\,]$, and the set F_2 will be the set consisting of the rest of the roots of $\varphi(x)$. Hence $\#M = 1 + \#(F_1 \cup F_2)$ and $\deg(\varphi) = \#F_1 + \#F_2$. For each $\lambda \in F_1 \cup F_2$, let P_λ be one of the (one or two) corresponding points on $A(\overline{\mathbb{F}}_q)$. Define

$$\begin{aligned} f_1 &= 3\lambda^2 + 2a\lambda + b \\ f_2 &= -2v_0(P_\lambda) \\ f_3 &= f_1 \ \text{ if } \ \lambda \in F_1 \ \text{ or } \ 2f_1 \ \text{ if } \lambda \in F_2 \\ f_4 &= (f_2)^2 \end{aligned}$$

and consider the set $F = \{(f_1, f_2, f_3, f_4)_\lambda \mid \lambda \in F_1 \cup F_2\}$ of tuples. By letting

$$\begin{aligned}
\tilde{u}_0(P) &= u_0(P) + \sum_{(f_1,f_2,f_3,f_4)_\lambda \in F} \left(\frac{f_3}{(u_0(P) - \lambda)} + \frac{f_4}{(u_0(P) - \lambda)^2} \right) \\
\tilde{v}_0(P) &= v_0(P) - \sum_{(f_1,f_2,f_3,f_4)_\lambda \in F} \left(\frac{f_4\, 2v_0(P)}{(u_0(P) - \lambda)^3} + \frac{f_3(v_0(P) - v_0(P_\lambda))}{(u_0(P) - \lambda)^2} - \frac{f_1 f_2}{(u_0(P) - \lambda)^2} \right)
\end{aligned}$$

we get that the isogeny with kernel G is given by $P \mapsto [\,\tilde{u}_0(P), \tilde{v}_0(P)\,]$. Furthermore by letting

$$\begin{aligned}
t &= \sum_{(f_1,f_2,f_3,f_4)_\lambda \in F} (f_3) \text{ and} \\
w &= \sum_{(f_1,f_2,f_3,f_4)_\lambda \in F} (f_4 + \lambda f_3),
\end{aligned}$$

we get that the image of the isogeny is given by the curve with equation $y^2 = x^3 + ax^2 + (b - 5t)x + (c - 4at - 7w)$.

Velu's formula makes the isogeny with kernel M explicit. Given the kernel of the isogeny in terms of $\varphi(x)$, Velu's formulas provide us with equations for the image elliptic curve and the polynomials $\upsilon(x, y)$ and $\omega(x, y)$.

We need a method to calculate the polynomial $\varphi(x)$ associated to an ℓ-isogeny between two elliptic curves. Such a method has been developed by Elkies in the context of algorithms for counting points on elliptic curves.

The basic idea is to use relations (which are found by working over $\mathbb{C}$) between classical modular forms and functions. By using only the two j-invariants of the the curves one may obtain all the data necessary to construct the polynomial $\varphi(x)$. There are several references for these formulas. (For example see [9]).

4.3.2 Modular curves

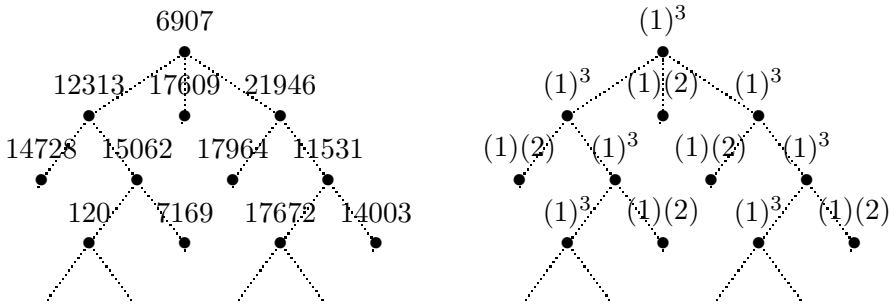
The modular curves $X_0(\ell)$ are a geometric tool which is of great value when studying isogenies of elliptic curves. The classical modular equations $\Phi_\ell(x, y) \in \mathbb{Z}[x, y]$ for $X_0(\ell)$ as a plane algebraic curve is given by the relation $\Phi_\ell(\mathrm{j}(\tau), \mathrm{j}(\ell\tau)) = 0$ between the classical modular functions $\mathrm{j}(\tau)$ and $\mathrm{j}(\ell\tau)$ on $X_0(\ell)$. The most important fact for the current application is that, if C is a given elliptic curve, then the elliptic curves which are ℓ-isogenous to C are precisely those curves (up to isomorphism) whose j-invariant is a root of $\Phi_\ell(\mathrm{j}(C), y) = 0$. The factorization patterns of these modular equations are well know and are among the most useful theoretical results for relating the j-invariants of ℓ-isogenous elliptic curves. For practical computation, its degree and coefficients are much too large.

Example With notation as above, the roots of $\Phi_\ell(\mathrm{j}(C), y)$ mod p are the j-invariants of curves ℓ-isogenous to the elliptic curve C defined over $\mathbb{F}_p$. So by solving repeatedly for a root we can construct a chain of ℓ-isogenies. The following graph illustrates the thought

for 2-isogenies starting with the elliptic curve

$$C : y^2 = x^3 + 17236x + 9822 \quad \text{over} \quad \mathbb{F}_{22147}$$

with j-invariant $\mathrm{j}(C) = 6907$. The factorization patterns of the modular equations for these curves obtained in this way are given in the example of section 4.2.



The connection between the ℓ-isogenies and the factorization pattern of the modular equation is clear. □

4.3.3 Isogeny classes

Most of the results in this section are from Deuring's classical paper which has been a model for the whole theory. We briefly discuss the structure of the Weil q-numbers and the isogeny classes they represent.

There is a bijection between the isogeny classes of elliptic curves, A over $\mathbb{F}_q$ and the rational integers α such that under all embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ we have $|\alpha| \leq 2\sqrt{q}$ and α satisfies one of the following conditions:

(a) $\gcd(\alpha, p) = 1$. Here the corresponding isogeny class consists of ordinary elliptic curves.

(b) $\mathrm{ord}_p(q)$ is even and $\alpha = \pm 2\sqrt{q}$. Here α corresponds to an isogeny class of supersingular elliptic curves A with $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$.

(c)
$$\mathrm{ord}_p(q) \text{ is even with } \begin{cases} p \not\equiv 1 \bmod 3 \text{ and } \alpha = \pm\sqrt{q}. \\ p \not\equiv 1 \bmod 4 \text{ and } \alpha = 0. \end{cases}$$
$$\mathrm{ord}_p(q) \text{ is odd with } \begin{cases} p = 2 \text{ and } \alpha = \pm p^{\frac{1}{2}}(a+1). \\ p = 3 \text{ and } \alpha = \pm p^{\frac{1}{2}}(a+1). \\ \alpha = 0. \end{cases}$$
In all theses cases α corresponds to an isogeny class of supersingular elliptic curves A with $\mathrm{End}_{\mathbb{F}_q}(A) \neq \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$.

The characteristic polynomial of an elliptic curve provides us with the necessary information to determine the endomorphism algebra as summarized below.

Let A be an elliptic curve over $\mathbb{F}_q$ with characteristic polynomial χ. We identify the frobenius endomorphism with a Weil q-number π and let $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be the endomorphism algebra of A. Then either one of the following two cases occur.

(a) $\chi = x^2 - \alpha x + q$ and $L = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{\alpha^2 - 4q})$ is commutative. Moreover

p ramifies in L if $\begin{cases} \alpha = 0 \text{ and } \mathrm{ord}_p(q) \text{ is odd.} \\ \alpha = 0,\ \mathrm{ord}_p(q) \text{ is even and } p = 2. \\ \alpha = \pm\sqrt{q},\ \mathrm{ord}_p(q) \text{ is even and } p = 3. \\ \alpha = \pm p^{\frac{1}{2}(a+1)},\ \mathrm{ord}_p(q) \text{ is odd and } p = 2 \text{ or } p = 3. \end{cases}$

p stays prime in L if $\begin{cases} \alpha = 0,\ \mathrm{ord}_p(q) \text{ is even and } p \equiv 3 \bmod 4. \\ \alpha = \pm\sqrt{q},\ \mathrm{ord}_p(q) \text{ is even and } p \equiv 2 \bmod 3. \end{cases}$

p splits in all other cases.

(b) $\chi = (x - \lambda)^2$ and $[L : \mathbb{Q}(\pi)] = 2$ with L the unique quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞.

So for elliptic curves, $\mathrm{End}_{\mathbb{F}_q}(A)$ is either a $\mathbb{Z}$-order in an imaginary quadratic number field or a $\mathbb{Z}$-order in a quaternion algebra over $\mathbb{Q}$. The latter occurs if and only if A is a supersingular elliptic curve with all endomorphisms defined over $\mathbb{F}_q$.

4.4 Endomorphism rings

We studied endomorphism rings of abelian varieties and by using our knowledge of isogeny classes and Weil q-numbers of abelian varieties, once the characteristic polynomial is known, we can construct the endomorphism algebra. We looked at the possible representatives for elements in a specific isogeny class and the ideals they contain. In this chapter we look at applications of the theory to Jacobians of hyperelliptic curves. We will show that in very restrictive cases we can gather enough information to determine the exact endomorphism ring of the Jacobian. In the elliptic case where the Jacobian variety is ordinary we will give practical methods for doing so and show how something similar can be done in higher genus. We will try to keep the theory as general as possible.

4.4.1 The ordinary case

Let A is an elliptic curve over $\mathbb{F}_q$. For elliptic curves, $\mathrm{End}_{\mathbb{F}_q}(A)$ is either a $\mathbb{Z}$-order in an imaginary quadratic number field or an $\mathbb{Z}$-order in a quaternion algebra over $\mathbb{Q}$. The latter occurs if and only if A is a supersingular elliptic curve with all endomorphisms defined over $\mathbb{F}_q$.

Let $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be the endomorphism algebra associated to the isogeny class of A. As usual we identify the frobenius endomorphism with a Weil q-number π.

We consider all the $\mathbb{Z}$-orders R in L which are representatives for curves $B \in [A]_{\sim \mathbb{F}_q}$. In the setting of Lemma 3.5.5 (a) we have either π is rational and $q\pi^{-1} = \pi$ or $q\pi^{-1}$ is conjugate to π in a quadratic number field and so lies in the same orders as π. Suppose A is an ordinary elliptic curve then the representatives are all those R containing π. Alternatively suppose A is a supersingular elliptic curve such that $\mathrm{End}_{\overline{\mathbb{F}}_q}(A) = \mathrm{End}_{\mathbb{F}_q}(A)$, then the representatives are all the maximal $\mathbb{Z}$-orders in L. If $\mathrm{End}_{\overline{\mathbb{F}}_q}(A) \neq \mathrm{End}_{\mathbb{F}_q}(A)$ then the representatives are those R which contain π and are maximal at p.

Theorem 4.4.1 *Suppose L is commutative and let R be a $\mathbb{Z}$-order in L which is a representative for some B in the isogeny class of A.*

(a) For all integral left R-ideals M we have $\mathrm{I}_{\mathrm{ker}}(M) = M$.

(b) $\{[B]_{\cong \mathbb{F}_q} \mid B \in [A]_{\equiv \mathbb{F}_q}\}$ forms a principal homogenous space over the ideal class group of R.

Proof We first show that every ideal is a kernel ideal. We must show that an integral R-ideal M is determined by the sets

$$\cap\{\varphi^{-1}(\mathrm{T}_\ell(A)) \mid \varphi \in M\} \quad \text{and} \quad \sum\{\varphi(\mathrm{T}_p(A)) \mid \varphi \in M\} = M\mathrm{T}_p(A).$$

At p the order R is maximal so $\mathrm{T}_p(A)$ is the sum of free modules and $M\mathrm{T}_p(A)$ and $M\mathrm{T}_p(A)$ determines the localization of M at p. Let $\hat{\epsilon}(\mathrm{V}_\ell(A))$ be the dual $\mathbb{Q}_\ell$-space of $\mathrm{V}_\ell(A)$ and let $\hat{\epsilon}(\mathrm{T}_\ell(A))$ be the dual lattice of $\mathrm{T}_\ell(A)$. Then the dual of $\varphi^{-1}(\mathrm{T}_\ell(A/\mathrm{G}_{\mathrm{ker}}(M)))$ is simply $M\hat{\epsilon}(\mathrm{T}_\ell(A))$. Now R is an order in a quadratic number field, and $\hat{\epsilon}(\mathrm{T}_\ell(A))$ like $\mathrm{T}_\ell(A)$ is a rank one module over R_ℓ. It is therefore invertible, for example free. Hence $M\hat{\epsilon}(\mathrm{T}_\ell(A))$ does determine the localization of M at ℓ. The integral left R-ideals with $\mathrm{O}_{\mathrm{right}}(M) = R$ are all invertible and conversely for all invertible integral left R-ideals we have $\mathrm{O}_{\mathrm{right}}(M) = R$. These ideals modulo scalar multiplication form the ideal class class group of R. Theorem 3.5.7 (b)(i),(ii) and (c) show that the ideal class group operates freely on the isomorphism classes of curves with representative R. We must show that there is only one orbit. Let H be a finite subgroup of A with $\mathrm{End}_{\mathbb{F}_q}(A/H) = R$ then we clain $H = \mathrm{G}_{\mathrm{ker}}(M)$ for some ideal M. At $\ell \neq p$, H corresponds to a lattice, including $\mathrm{T}_\ell(A)$ or to a sublattice of $\hat{\epsilon}(\mathrm{T}_\ell(A))$. Since $\hat{\epsilon}(\mathrm{T}_\ell(A))$ is free of rank 1, this is given by $M_\ell\hat{\epsilon}(\mathrm{T}_\ell(A))$ for some local ideal M_ℓ. At p we know R_p is maximal and the fact that we get all lattices from ideals is a special case of Theorem 3.5.9 (b). As H is finite, $M_\ell = R_\ell$ for all but finitely many ℓ. Hence there is a lattice M whose localizations are the M_ℓ, it is an ideal because it is one locally, and clearly then $H = \mathrm{G}_{\mathrm{ker}}(M)$. □

Elliptic curves over $\mathbb{C}$ are exactly the principally polarized abelian varieties of dimension 1. They are isomorphic to complex tori $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ and $\tau \in \mathbb{C}$ has strictly positive imaginary part.

Suppose A is of CM-type when viewed as an abelian variety of dimension 1. This is equivalent to $\mathrm{End}_{\mathbb{C}}(A) \neq \mathbb{Z}$ and that L is isomorphic to the CM field $K = \mathbb{Q}(\pi)$. In this case, $\mathrm{End}_{\mathbb{C}}(A) = \{\alpha \in \mathbb{C} \mid \alpha, \alpha\tau \in \Lambda\}$ and so $\alpha = m + n\tau \in \mathrm{End}_{\mathbb{C}}(A)$. The condition $\alpha\tau \in \Lambda$ implies τ satisfies some equation $a\tau^2 + b\tau + c = 0$ (for example τ lies in a quadratic imaginary field K). We may choose a, b, c to be integers such that $\gcd(a, b, c) = 1$. In this case the

field K is equal to $\mathbb{Q}(\sqrt{b^2-4ac})$ and $\mathrm{End}_{\mathbb{C}}(A)$ is a $\mathbb{Z}$-order in K with discriminant b^2-4ac ([25] Theorem 8.1).

Let $\mathcal{O} = \mathrm{End}_{\mathbb{C}}(A)$. The lattice Λ is a projective $\mathcal{O}$-module and A is isomorphic to an elliptic curve $\mathbb{C}/\Gamma$ if and only if Γ is in the same ideal class as Λ in the ideal class group of $\mathcal{O}$, denoted $\mathrm{H}(\mathcal{O})$. These elliptic curves are defined over the ring class field of $\mathcal{O}$. It follows that the number of isomorphism classes of elliptic curves over $\mathbb{C}$ having endomorphism ring, $\mathcal{O}$, is equal to the class number $\mathrm{h}(\mathcal{O})$ of the order $\mathcal{O}$.

Let M be an $\mathcal{O}$-ideal, then the identity map from $\mathbb{C}$ to itself induces the map $\mathbb{C}/M \to \mathbb{C}/MN^{-1}$ which has kernel $MN^{-1}/M \cong \mathcal{O}/N$. This is an isogeny of degree $\mathrm{norm}(N)$ and all isogenies arise in this way.

For each representative, $\mathcal{O}$, the theory of complex multiplication combined with Deuring's theory about lifting endomorphisms from characteristic p to characteristic 0, shows that the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with endomorphism ring isomorphic to $\mathcal{O}$ is equal to $\mathrm{h}(\mathcal{O})$, the number of equivalence classes of projective $\mathcal{O}$-modules modulo principal ones. Furthermore the action of of isogenies is the same as composition of ideal classes. Indeed, elliptic curves over $\mathbb{F}_q$ can be lifted to elliptic curves over $\mathbb{C}$ with the same endomorphism ring $\mathcal{O}$ and can thus be interpreted as $\mathbb{C}/M$ where M is a projective $\mathcal{O}$-module. Also given some other projective $\mathcal{O}$-module N, one has the isogeny $\mathbb{C}/M \to \mathbb{C}/MN^{-1}$ with kernel $MN^{-1}/M \cong \mathcal{O}/N$.

Over $\mathbb{C}$, the correspondence between the endomorphism class of an elliptic curve up to isomorphism and the ideal class group $\mathrm{H}(\mathcal{O})$ of its endomorphism ring is canonical, however the reduction of these curves over $\mathbb{F}_q$ depends on a totally split prime P, lying above p, in the ring class field. The only method known to the author to efficiently compute the correspondence between $\mathrm{H}(\mathcal{O})$ and the set of j-invariants of curves over $\mathbb{F}_q$ is to compute the j-invariant for each ideal class $[M] \in \mathrm{H}(\mathcal{O})$ up to some amount of precision, then to compute the Hilbert class polynomial and therefore the ring class field of $\mathcal{O}$, to find to prime P above p, and then to reduce these values modulo P. The class polynomial is given by

$$h(x) = \prod_{\tau_i} (x - \mathrm{j}(\tau_i)),$$

where τ_i is a particular algebraic integer associated to each ideal class in $\mathrm{H}(\mathcal{O})$. Let A be an ordinary elliptic curve over $\mathbb{F}_q$ and let π be the corresponding Weil q-number associated to the frobenius endomorphism of A. We will follow the ideas in [23] and describe methods to determine the isomorphism type of the endomorphism ring of A.

Since A is ordinary we know that $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ and it follows from Theorem 3.6.2 that $L = \mathrm{End}(A) \otimes \mathbb{Q}$ is a field. Moreover L is isomorphic to its center $K = \mathbb{Q}(\pi)$ which is an imaginary quadratic extension of $\mathbb{Q}$ and contains $\mathrm{End}(A)$ as a $\mathbb{Z}$-order in a natural way. Let $\mathcal{O}_K$ be the maximal $\mathbb{Z}$-order in K and set $d = \mathrm{disc}(\mathcal{O}_K)$.
We have $K = \mathbb{Q}(\sqrt{m})$ for some negative integer m which is assumed to have no square factors and satisfies

$$m = \begin{cases} \frac{1}{4}d & \text{if } d \not\equiv 0 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

The maximal $\mathbb{Z}$-order in K is given by

$$\mathcal{O}_K = \mathbb{Z}[\,\tfrac{1}{2}(d+\sqrt{d})\,]$$

and it is a well know fact that for every $\mathbb{Z}$-order, $\mathcal{O}$ in K, we have an unique integer c such that

$$\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K = \mathbb{Z}[\,\tfrac{1}{2}c(d+\sqrt{d})\,]$$

and $\mathrm{disc}(\mathcal{O}) = c^2 d$ illustrating the fact that $\mathbb{Z}$-orders in imaginary quadratic number fields are uniquely determined by their discriminants.

Since A is ordinary with $\#A(\mathbb{F}_q) = q + 1 - t$ we have $K = \mathbb{Q}(\sqrt{m})$ with $m = t^2 - 4q$. Furthermore for the $\mathbb{Z}$-algebra, $\mathbb{Z}[\pi]$ generated by π we have

$$\mathbb{Z}[\pi] = \mathbb{Z}[\pi, q\pi^{-1}] = \mathbb{Z}[\,\tfrac{1}{2}(m+\sqrt{m})\,]$$

and thus $\mathrm{disc}(\mathbb{Z}[\pi]) = c^2 d$ where $c = [\mathcal{O}_K : \mathbb{Z}[\pi]]$ is the largest integer such that $d = \frac{m}{c^2}$. Since elliptic curves are simple abelian varieties, by Theorem 3.6.4, we know that the representatives for isogeneous curves are exactly those $\mathbb{Z}$-orders containing $\mathbb{Z}[\pi]$.

For any B in $[A]_{\sim_{\mathbb{F}_q}}$ we consider the representatives $\iota(\mathrm{End}(A))$ and $\iota(\mathrm{End}(B))$ as $\mathbb{Z}$-orders in the endomorphism algebra of an abelian variety isogenous to A and B, which is isomorphic to the field K. We see that there are finitely many possibilities for such representatives corresponding to the divisors of c.

We have seen that the isogeny class of an ordinary elliptic curve contains $\mathrm{h}(\mathcal{O})$ elliptic curves with endomorphism ring isomorphic to $\mathcal{O}$ for each of the orders $\mathcal{O}$ satisfying $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. Imaginary quadratic number fields K are well-understood and the structure and size of their ideal class group can be computed efficiently. In particular the class group of K is generated by the primes p which split of ramify in K.

The class number of a $\mathbb{Z}$-order is closely related to the class number of the maximal $\mathbb{Z}$-order, $\mathcal{O}_K$. We can express the class number of a $\mathbb{Z}$-order $\mathcal{O}$ as

$$\mathrm{h}(\mathcal{O}) = \frac{\mathrm{h}(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]}[\mathcal{O}_K : \mathbb{Z}[\pi]] \prod_{\ell}(1 - \frac{\omega}{\ell})$$

where ℓ ranges over all primes dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ and

$$\omega = \begin{cases} 0 & \text{if } \ell \text{ divides } d \ (p \text{ is ramified in } K) \\ -1 & \text{if } d \text{ is not a square mod } \ell \ (p \text{ is inert in } K) \\ 1 & \text{if } d \text{ is a square mod } \ell \ (p \text{ is split in } K) \end{cases}$$

with $d = \mathrm{disc}(K)$ (See [25] Theorem 8.7). In particular we see that the class number grows as the index $[\mathcal{O}_K : \mathcal{O}]$ grows and at each prime ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$, the probability that $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathbb{Z}[\pi] \otimes \mathbb{Z}_\ell$ is at least $\frac{1}{3}(\ell - 1)$ times as great as $\mathcal{O} \otimes \mathbb{Z}_\ell$ being larger. Thus one expects the endomorphism ring of an ordinary elliptic curve to contain $\mathbb{Z}[\pi]$ with small index.

The following result tells us exactly when the representatives of isogenous ordinary elliptic

curves coincide.

Theorem 4.4.2 *Let A and B be isogenous ordinary elliptic curves over $\mathbb{F}_q$ and let $\varphi : A \to B$ be an isogeny over $\mathbb{F}_q$.*

(a) There exist relatively prime integers a and b such that $\mathbb{Z} + a\iota(\mathrm{End}(A)) = \mathbb{Z} + b\iota(\mathrm{End}(B))$ and $\deg(\varphi)$ divides ab.

(b) Suppose $\iota(\mathrm{End}(A)) \subseteq \iota(\mathrm{End}(B))$ (respectively $\iota(\mathrm{End}(B)) \subseteq \iota(\mathrm{End}(A))$) and $\ell \neq p$ is a rational prime dividing the index $[\iota(\mathrm{End}(B)) : \iota(\mathrm{End}(A))]$ (respectively $[\,\iota(\mathrm{End}(A)) : \iota(\mathrm{End}(B))\,]$), then ℓ divides $\deg(\varphi)$.

(c) The following are equivalent

(i) $\iota(\mathrm{End}(A)) \cong \iota(\mathrm{End}(B))$ as $\mathbb{Z}$-orders in K.

(ii) The integral left $\iota(\mathrm{End}(A))$-ideal, $\mathrm{I}_{\ker}(\varphi) = \{\alpha \in \iota(\mathrm{End}(A)) \mid \alpha(\mathrm{G}_{\ker}(\varphi)) = 0\}$, is projective and $\mathrm{norm}(\mathrm{I}_{\ker}(\varphi)) = \deg(\varphi)$.

(iii) There exists an isogeny $\alpha : A \to B$ of degree coprime to $\deg(\varphi)$.

Proof For the first two statements, see [23] Proposition 5, 21. For part (c) we recall that Theorem 3.3.6 gave us a bijective map

$$\mathrm{Hom}_{\mathbb{F}_q}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(A), \mathrm{T}_\ell(B))$$

for $\ell \neq p$. Here, for $\mathcal{O} = \iota(\mathrm{End}(A))$, both sides have the structure of $\mathcal{O}_\ell$-modules. Let $\overline{\pi}$ denote the frobenius automorphism of $\overline{\mathbb{F}}_q/\mathbb{F}_q$, then $\mathbb{Z}[\pi]_\ell$ and $\mathbb{Z}[\overline{\pi}]_\ell$ have the same representation on Tate modules. Further we also have $K_\ell = \mathcal{O} \otimes \mathbb{Q}_\ell$. Since $\mathrm{End}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(A)) \cong \mathcal{O}_\ell$ and $\mathrm{End}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(B)) \cong \iota(\mathrm{End}(B))_\ell$ we have that the Tate modules, $\mathrm{T}_\ell(A)$ and $\mathrm{T}_\ell(B)$, are isomorphic as $\mathbb{Z}[\pi]_\ell$-modules if and only if $\mathcal{O}_\ell \cong \iota(\mathrm{End}(B))_\ell$. This is equivalent to $\mathrm{Hom}_{\mathbb{F}_q}(A, B) \otimes \mathbb{Z}_\ell$ being free as a $\mathcal{O}_\ell$-module. If these conditions holds for all $\ell \neq p$, since $\mathcal{O}$ is maximal at p, this is equivalent to $\mathrm{Hom}_{\mathbb{F}_q}(A, B)$ being projective as a left $\mathcal{O}$-module. Observing that $\mathrm{I}_{\ker}(\varphi) = \mathrm{Hom}_{\mathbb{F}_q}(A, B)\varphi$, we see the equivalence between the first two conditions. The degree map on isogenies in $\mathcal{O}$ equals the norm map on the ring $\mathcal{O}$. If the ideal $\mathrm{I}_{\ker}(\varphi) = \mathrm{Hom}_{\mathbb{F}_q}(A, B)\varphi$ has norm $\deg(\varphi)$, then it follows that there exists an isogeny of degree relatively prime to $\deg(\varphi)$. By decomposing an isogeny into isogenies of prime degrees, from condition (iii) we deduce that the $\mathbb{Z}$-orders $\mathcal{O} = \iota(\mathrm{End}(A))$ and $\iota(\mathrm{End}(B))$ are isomorphic by part (b). □

Statement (b) tells us that the primes dividing $c = [\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ will require special attention. Indeed by taking a sequence of ℓ-isogenies, for those primes ℓ dividing $[\,\mathcal{O}_K : \iota(\mathrm{End}(A))\,]$, it is possible to find an elliptic curve B isogenous to A with $\iota(\mathrm{End}(B)) = \mathcal{O}_K$. These ideas are central in Kohel's thesis for finding the exact endomorphism ring of a given ordinary elliptic curve.

We can even be more complete in our analysis of isogenies. The following theorem, which is essentially Proposition 23 in [23], tells us everything we need to know to make it possible to determine the exponent of ℓ in $[\,\iota(\mathrm{End}(A)) : \mathbb{Z}[\pi]\,]$, but first we make explicit the terminology which we will use in this section.

We use the language of Kohel, so an isogeny "down" is an isogeny $\varphi : A \to B$ of degree ℓ such that $[\,\iota(\mathrm{End}(A)) : \iota(\mathrm{End}(B))\,] = \ell$ whilst an ℓ-isogeny "up" is one with $[\,\iota(\mathrm{End}(B)) : \iota(\mathrm{End}(A))\,] = \ell$. In the case where the representatives of A and B are preserved we call the isogeny "horizontal". We say that A is "on the surface at ℓ" if ℓ does not divide the index $[\,\mathcal{O}_K : \iota(\mathrm{End}(A))\,]$ and we say that A is "on the floor at ℓ" if ℓ does not divide the index $[\,\iota(\mathrm{End}(A)) : \mathbb{Z}[\pi]\,]$. We might also say that A is "on level n at ℓ" if ℓ^n divides $[\,\mathcal{O}_K : \iota(\mathrm{End}(A))\,]$ but ℓ^{n+1} does not. For $d = \mathrm{disc}(K)$ the discriminant of K we let

$$\omega = \begin{cases} 0 & \text{if } \ell \text{ divides } d \\ -1 & \text{if } d \text{ is not a square mod } \ell \\ 1 & \text{if } d \text{ is a square mod } \ell \end{cases}$$

Proposition 4.4.3 *Let A be an ordinary elliptic curve over $\mathbb{F}_q$. Suppose A have representative $\mathcal{O} = \iota(\mathrm{End}(A))$ in K and let ℓ be a prime. The following list then classifies the possibilities of ℓ-isogenies over $\mathbb{F}_q$.*

(a) If ℓ does not divide $[\,\mathcal{O}_K : \mathcal{O}\,]$, then there are $(\omega + 1)$ ℓ-isogenies to elliptic curves B, such that B is in $[A]_{\equiv \mathbb{F}_q}$.

(b) If ℓ divides $[\,\mathcal{O}_K : \mathcal{O}\,]$, then there is only 1 isogeny up.

(c) If ℓ does not divide $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$, then there are no ℓ-isogenies down.

(d) If ℓ divides $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$ and ℓ divides $[\,\mathcal{O}_K : \mathcal{O}\,]$, then the number of ℓ-isogenies down is precisely ℓ.

(e) If ℓ divides $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$ and ℓ does not divide $[\,\mathcal{O}_K : \mathcal{O}\,]$, then there are $(\ell - \omega)$ ℓ-isogenies down.

Pectora roborant cultus recti

Proof Deuring's lifting theorems allow us to lift the elliptic curve A from $\mathbb{F}_q$ to $\mathbb{C}$ in such a way that the endomorphism ring is preserved. Suppose $A = \mathbb{C}/\langle 1, \tau\rangle$ where τ satisfies $a\tau^2 + b\tau + c = 0$ with $\gcd(a, b, c) = 1$. So $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}) = m = b^2 - 4ac$. Then there are $\ell + 1$ possibilities for the kernel of an ℓ-isogeny and they are $M_0 = \langle \frac{1}{\ell}, \tau\rangle$ and $M_k = \langle 1, \frac{1}{\ell}(\tau + k)\rangle$ where $k = 1, \ldots, \ell$, The image curves in these cases are $C_0 = C/M_0 \cong \mathbb{C}/\langle 1, \ell\tau\rangle$ and $C_k = C/M_k \cong \mathbb{C}/\langle \ell, k + \tau\rangle$. Our goal is to determine the representative $\mathcal{O}_k = \iota(\mathrm{End}_{\mathbb{C}}(C_k))$ for $k = 0, 1, \ldots, \ell$. We will do this using use Theorem 8.1 in [25]. Firstly we consider C_0. The number $\alpha = \ell\tau$ satisfies $a\alpha^2 + \ell b\alpha + \ell^2 c = 0$. If $\gcd(a, \ell b, \ell^2 c) = 1$ then $\mathcal{O}_0$ has discriminant $\ell^2 m$ and so M_0 is an ℓ-isogeny down. On the other hand if $\gcd(a, \ell b, \ell^2 c) \neq 1$, then it follows that ℓ divides a and we put $\overline{a} = \frac{1}{\ell}(a)$. If ℓ does not divide b then α is actually a root of $\overline{a}\alpha^2 + b\alpha + \ell c = 0$ from which we see that $\mathcal{O}_0 = \mathcal{O}$ (for example the ℓ-isogeny is horizontal). Suppose ℓ divides b and put $\overline{b} = \frac{1}{\ell}(b)$. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$ then, since $m = b^2 - 4ac$, it follows that ℓ^2 divides a and we put $\overline{a} = \frac{1}{\ell^2}(a)$ This means α satisfies $\overline{a}\alpha^2 + \overline{b}\alpha + c = 0$ which has dicriminant $\frac{m}{\ell}$ and hence we have an ℓ-isogeny up.
Now consider the elliptic curves C_k for $k = 1, \ldots, \ell$. The number $\alpha = \frac{1}{\ell}(k + \tau)$ is a root of $\ell^2 a\alpha^2 + \ell(b - 2ak)\alpha + (ak^2 - bk + c) = 0$. In the case $\gcd(l^2 a, \ell(b - 2ak), ak^2 - bk + c) = 1$ we see that $\mathcal{O}_k$ has discriminant $\ell^2 m$ and we have an isogeny down. The condition $\gcd(l^2 a, \ell(b - 2ak), ak^2 - bk + c) = 1$ fails if and only if ℓ divides $ak^2 - bk + c$. Note that there are several possibilities for the solubility of the equation $ak^2 - bk + c \equiv 0 \bmod \ell$.

If ℓ divides a and ℓ divides b then there is no solution. In this case ℓ divides m. In the case where ℓ divides $[\mathcal{O}_K : \mathcal{O}]$, we already found a single ℓ-isogeny up. If ℓ does not divide this index, then it follows that ℓ ramifies in K, and we already found a single ℓ-isogeny to an elliptic curve with representative equal to $\mathcal{O}$.
If ℓ divides a but does not divide b then we already found an ℓ-isogeny previously. In this case there is also the value $k = \frac{c}{b}$ which will give a horizontal ℓ-isogeny. Thus, in this case, we have two horizontal isogenies and the prime ℓ splits in K.
If ℓ does not divide a then the equation is a true quadratic. There is a repeated root if and only if ℓ divides $b^2 - 4ac$ (which again responds to the ramified case handled above) and so there is only one horizontal solution. Otherwise there are two distinct solutions (equivalently, the prime ℓ splits in K) and we obtain two horizontal ℓ-isogenies.
The final case is when ℓ is inert in K. In this case there will be no solutions to the quadratic (for example all values for k will give an ℓ-isogeny down, and so we get a total of ℓ isogenies down).
Finally, we must contemplate the Deuring reduction step. We reduce the elliptic curves C_k from $\mathbb{C}$ to some finite field $\mathbb{F}_{q^n}$. These elliptic curves will actually be defined over $\mathbb{F}_q$ if and only if the representative, $\mathcal{O}_k$, contains $\mathbb{Z}[\pi]$. This completes the proof of the classification. □

We remark that in each of the cases in Theorem 4.4.3, when there are several different isogenies to curves on the same level, then some of the image curves may actually be isomorphic. To explain this behaviour we consider pairs in

$$\Omega = \{(A, B)|\ B \in [A]_{\sim \mathbb{F}_q},\ \iota(\mathrm{End}(B)) \subseteq \mathcal{O}\}$$

up to isomorphism and define $\Theta = \{(B, \varphi)|\ (A, B) \in \Omega$ and φ an isogeny of degree $\ell\}$. It follows from Theorem 4.4.2 (c), by counting the number of projective ideals of norm ℓ, that if $\mathcal{O}$ is non-maximal at ℓ, then for all pairs $(B, \varphi) \in \Theta$, $\iota(\mathrm{End}(B)) \neq \mathcal{O}$ and $\#\{(B, \varphi) \in \Theta|\ B \in [A]_{\equiv \mathbb{F}_q}\} = (\omega + 1)$ otherwise. Furthermore if $\#\Theta > (\omega + 1)$, then all isogenies of degree ℓ is defined over $\mathbb{F}_q$ and there are exactly $(\ell - \omega)[\,\mathcal{O}^* : \iota(\mathrm{End}(B))^*\,]$ pairs in $\{(B, \varphi) \in \Theta \mid \iota(\mathrm{End}(B)) \subset \mathcal{O}\}$. Here the factor $[\,\mathcal{O}^* : \iota(\mathrm{End}(B))^*\,]$ is the size of the orbits of the action of automorphisms of A on the set of cyclic subgroups $A[\ell]$.

We will use these results and discuss a few practical methods for determining the endomorphism type of an ordinary elliptic curve. The first two methods works well for small prime divisors of the the index $[\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ whilst the third makes provision for larger prime divisors.

Explicit kernels

For $c = [\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ and $d = \mathrm{disc}(K)$, we can find an integer a such that $\mathcal{O}_K = [\,\frac{1}{c}(\pi - a)\,]$. For $\mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4q$, a has the property that $(x - a)^2 = x^2 - tx + 1 \bmod c$ and is determined by the conditions that $2a \equiv t \bmod c$ and $q - ta + a^2 \equiv 0 \bmod c^2$. In particular, the integers $a = \frac{1}{2}(t + m)$ and $a = \frac{1}{2}(t)$ satisfy these conditions if $d \equiv 1 \bmod 4$ and $d \equiv 0 \bmod 4$ respectively such that $\pi - a \equiv 0 \bmod c\mathcal{O}_K$.

The goal of the algorithm described here is to determine for each prime divisor, ℓ of c,

the largest power that divides $\pi - a$ in $\mathcal{O} = \iota(\mathrm{End}_{\mathbb{F}_q}(A))$. As we mentioned before, we expect the ring $\mathbb{Z}[\pi]$ to have discriminant equal to a small square multiple of d and for $\mathbb{Z}[\pi]$ itself to have small index in $\mathcal{O}_K$.

We observe that since A is ordinary, we have $\gcd(t, q) = 1$ and so π determines a linear automorphism

$$\pi : \ \mathcal{O}/c\mathcal{O} \to \mathcal{O}/c\mathcal{O}.$$

The integer a is a double eigenvalue modulo c of π and the objective is to find the largest integer n for which $\pi - a$ is the zero map on $\mathcal{O}/n\mathcal{O}$.

The most direct way to do this is to determine if a divisor n of c divides $\pi - a$ in $\mathcal{O}$ is by comparing the homomorphisms induced by π and a on the ring $\mathbb{F}_q[x, y]/\langle\, y^2 - x^3 - ax - b, \varphi_n \,\rangle$ where $\varphi_n(x, y)$ is the division polynomial for n.

We have $\pi - a = n\alpha$ for some $\alpha \in \mathcal{O}$ if and only if $A[n] \subseteq \mathrm{G}_{\mathrm{ker}}(\pi - a)$. Let $\mathbb{P}^1 = A/\langle \pm 1 \rangle$ and consider the maps induced on $\mathbb{P}^1$ by π and a respectively. By setting $\varphi_n(x)$ to be the generator of $\langle\, \varphi_n(x, y) \,\rangle \cap \mathbb{F}_q[x]$, we get the functions

$$\frac{\upsilon_a(x)}{\varphi_a(x, y)^2} \quad \text{and } \pi = x^q$$

and so one computes $x^q \varphi_a(x, y)^2 - \upsilon_a(x) \bmod \varphi_n(x)$ which equals zero if and only if n divides $\pi - a$ in $\mathcal{O}$. Note that we can take for a any of its coset representatives modulo n. By taking $n = \ell, \ell^2, \ldots$ up to the highest power of a prime ℓ dividing c we find the exponent of ℓ in the index $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$. Since we expect $\mathbb{Z}[\pi]$ to be contained in $\mathcal{O}$ with small index, we are likely to find that $A[\ell^r] \not\subseteq \mathrm{G}_{\mathrm{ker}}(\pi - a)$ well before treating the largest power of ℓ dividing c.

Example Consider the following two ordinary elliptic curves over $\mathbb{F}_{36709}$.

$$\begin{aligned} A: \ y^2 &= x^3 + 34917x + 3584 \\ B: \ y^2 &= x^3 + 27340x + 18738 \end{aligned}$$

They lie in the same isogeny class with associated Weil polynomial $\chi = x^2 - 82x + 36709$. Let $\mathcal{O}_K$ be the maximal order in the field $K = \mathbb{Q}(\sqrt{-140112})$. The index of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$ is 6 in both cases. Further, in each case we have that 1 is a coset representative for $a = 41$. We find $A[2] \not\subseteq A(\mathbb{F}_{36709})$ and $A[3] \subseteq A(\mathbb{F}_{36709})$ thus $[\,\mathrm{End}(A) : \mathbb{Z}[\pi]\,] = 3$. Similarly $A[2] \not\subseteq A(\mathbb{F}_{36709})$ and $A[3] \not\subseteq A(\mathbb{F}_{36709})$ so $[\,\mathrm{End}(B) : \mathbb{Z}[\pi]\,] = 1$. □

Note however that the method is not practical when a large power of ℓ divides c and in the next section we discuss a method for handling such a case.

Probing the levels

Let A be an ordinary elliptic curve over $\mathbb{F}_q$ and adapt the notation of Proposition 4.4.3. We look at primes ℓ dividing $\mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4q$. There exists $\ell + 1$ isogenies of degree ℓ over $\overline{\mathbb{F}}_q$ and we will show how to use Proposition 4.4.3 to determine the exponent of ℓ in $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$ for small primes ℓ.

By Proposition 4.4.3, of the $\ell+1$ isogenies of degree ℓ over $\overline{\mathbb{F}}_q$, exactly $(\omega+1)$ are defined over $\mathbb{F}_q$. Suppose A lies on the floor at ℓ, then there are no elliptic curves $B \in [A]_{\sim \mathbb{F}_q}$ on level greater than A at ℓ. If ℓ divides the index $[\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$, then by assumption A is not on the surface at ℓ, $(\omega+1)=1$ and the remaining ℓ curves which are ℓ-isogenous to A over $\overline{\mathbb{F}}_q$ are not defined over $\mathbb{F}_q$. This suggests the use of ℓ-isogenies to probe the levels down to the floor as described below.

Suppose ℓ is a prime dividing $[\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ and that A does not lie on the floor at ℓ. We construct an isogeny $\varphi : A \to B$ of degree ℓ. On the surface, the number of isogenies to curves lying at a greater level than A is at least $\max(\frac{1}{3}(\ell-1),1)$ and, at greater level, ℓ of the $\ell+1$ isogenies lead down. If we choose an isogeny φ such that B lies at greater level than A, then all isogenies except $m\varphi^{-1}$ continue our descent. Thus we construct isogenies until we reach the floor and by counting the number of levels down we get the exponent of ℓ in $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$.

Suppose that our initial choice of ℓ-isogeny did not begin this decent, then we overestimated the index $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$. For that reason we perform a second probe. By Proposition 4.4.3, if A does not lie on the surface at ℓ, one ℓ-isogeny leads up and ℓ isogenies of degree ℓ lead down to a greater level. If we were to begin a second probe along a different ℓ-isogeny, one path is certain to lead down and we conclude that the exponent of ℓ in $[\,\mathcal{O} : \mathbb{Z}[\pi]\,]$ is the minimum of the lengths of the two probes.

Finally if we start on the surface with respect to ℓ, then there are $(\omega+1)$ isogenies of degree ℓ to elliptic curves B in $[A]_{\equiv \mathbb{F}_q}$. If ℓ does not stay prime in $\mathcal{O}$, we may find ourselves in the unfortunate event of floating indefinitely along the surface before beginning our descent. However we do know the maximum exponent of ℓ to be that in $[\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$, so if the length of both probes exceeds this bound, we conclude that A lies on the surface.

Pectora roborant cultus recti

Example Consider the ordinary elliptic curve

$$A : y^2 = x^3 + 11639x + 21016 \quad \text{over} \quad \mathbb{F}_p$$

with $p = 22147$. The characteristic polynomial $\chi = x^2 + 28x + 22147$ is an ordinary Weil p-polynomial generating the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-87804})$ of discriminant $2^2 \cdot 3^4 \cdot 271$ in which p is totally split. For $\mathcal{O}_K$, the integral closure of $\mathbb{Z}$ in K, we have $\mathrm{disc}(\mathcal{O}_K) = 271$ and thus 271 divides $\mathrm{disc}(\mathrm{End}(A))$. Furthermore at $\ell = 2$, A is isogenous to a curve with j-invariant

$$\mathrm{j} = 11531 \bmod p$$

which lies at the floor of rationality. From the calculations done in Section 4.2, we see that A itself lies at the floor of rationality with respect to 3, so we conclude $\mathrm{disc}(\mathrm{End}(A)) = 2 \cdot 271$. □

This method works well from small primes but when a large prime divide the index $[\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ we will need another method.

Isolated endomorphism classes

Let $\mathcal{O} = \iota(\mathrm{End}(A))$. By decomposition of isogenies into isogenies of prime degrees and Theorem 4.4.2 (b) we see that for an isogeny $\varphi : A \to B$, $\deg(\varphi)$ is divisible by

$$[\,\mathcal{O}\iota(\mathrm{End}(B) : \mathcal{O}\,][\,\mathcal{O}\iota(\mathrm{End}(B) : \iota(\mathrm{End}(B))\,] = [\,\mathcal{O} : \mathcal{O}\cap\iota(\mathrm{End}(B))\,][\,\iota(\mathrm{End}(B) : \mathcal{O}\cap\iota(\mathrm{End}(B))\,].$$

Moreover by Theorem 3.6.4 if follows that for every $B \in [A]_{\sim\mathbb{F}_q}$ we have $\mathbb{Z}[\pi] \subseteq \iota(\mathrm{End}(B))$. Write $\mathbb{Z}[\pi] = \mathbb{Z} + c\mathcal{O}_K$ and consider an arbitrary isogeny $\varphi : A \to B$ of degree m. If $\gcd(m, c) = 1$, then B is in $[A]_{\equiv\mathbb{F}_q}$ and by Theorem 4.4.2 (c) $\mathrm{I}_{\ker}(\varphi)$ is a projective (hence finitely generated) $\mathcal{O}$-module with $m = 1$ if and only if $B \in [A]_{\cong\mathbb{F}_q}$. This gives us the bijection between the endomorphism class of A and the ideal class group of $\mathcal{O}$ as mentioned earlier.

We have two approaches which we might exploit for the determination $\mathcal{O}$ up to isomorphism. The first is to enumerate all of the $\mathrm{h}(\mathcal{O})$ elliptic curves in $[A]_{\equiv\mathbb{F}_q}$. This involves choosing a set of small prime generators for the ideal class group $\mathrm{H}(\mathcal{O})$ and using these to construct the corresponding endomorphisms in $\mathcal{O}$. The second involves computation of principal ideals with restricted norm in a representative, say R, for some $B \in [A]_{\sim\mathbb{F}_q}$ (a $\mathbb{Z}$-order containing π) and then determining the corresponding isogeny to determine if B is isomorphic to A.

If $c = [\,\mathcal{O}_K : \mathbb{Z}[\pi]\,]$ is divisible by a large prime ℓ then the $\mathbb{Z}$-orders containing the $\mathbb{Z}$-order, R, where

$$R = \mathbb{Z}[\,\tfrac{1}{\ell}(\pi - a)\,] \subseteq \mathcal{O}_K = \mathbb{Z}[\,\tfrac{1}{c}(\pi - a)\,]$$

have discriminants dividing $\frac{1}{\ell^2}(t^2 - 4q)$ and the class numbers of these orders divide $\mathrm{h}(R)$. Thus if we can enumerate the elliptic curves, up to isomorphism, in the endomorphism class of A until we exceed $\mathrm{h}(R)$, we can conclude that A lies on the floor with respect to ℓ.

Pectora roborant cultus recti

Such an calculation presupposes that we have determined $\mathrm{h}(R)$ and that we have small splitting primes in R from which we can feasibly construct sequences of isogenies of small degree to all members in the endomorphism class.

In order to enumerate the curves in the endomorphism class of A, up to isomorphism, we blindly explore the bounds of the class until we have determined the world to which A is confined. This fails to exploit the considerable knowledge given in Theorem 3.5.9 about the class group of $\mathcal{O}$ acting on the endomorphism class of A. Instead we can use algorithms for ideal class groups to find class group relations among small splitting primes $P_1, \ldots, P_n$ in the $\mathbb{Z}$-order, R. In doing so we obtain a principal ideal $wR = P_1^{s_1} \cdots P_n^{s_n} \subseteq R$, with exponent sum $u = s_1 + s_2 + \ldots + s_n$ and let $S = w\mathcal{O} \cap \mathcal{O}$. By constructing the sequence of isogenies

$$A = A_0 \to A/A[P_1] = A_1 \to A/A[P_1^2] = A_2 \to \ldots \to A/A[S] = A_u,$$

each of small degree, we obtain a curve $A_u = A/A[S]$ which is isomorphic to A if and only if S is principal. Typically we find w in the ring R containing $\mathbb{Z}[\pi]$ with large index, and we expect S to be nonprincipal in $\mathcal{O}$. In the incidental case that $R \subseteq \mathcal{O}$ we have constructed

a new endomorphism of A.

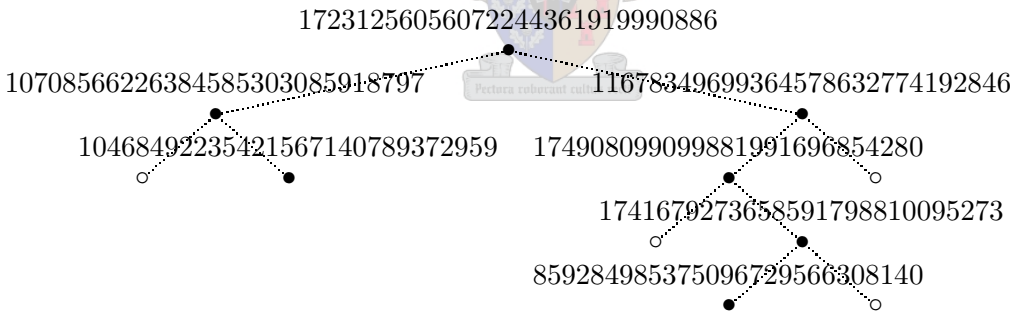
We note that any prime ideal P of $\mathcal{O}$ which does not divide the discriminant, $\mathrm{disc}(\mathbb{Z}[\pi])$, can be written in the form $P = \langle r, \pi - t\rangle$ for $r = \mathrm{norm}(P)$ and $t \in \mathbb{Z}$. The kernel of the isogeny $A \to A/A[P]$ is determined by the ideal

$$I = \langle \varphi_r(x,y), x^q\varphi_t(x,y)^2 - \upsilon_t(x)\rangle \subseteq \mathbb{F}_q[x,y]/\langle y^2 - x^3 - ax - b\rangle.$$

We let $\varphi(x)$ be a generator for $I \cap \mathbb{F}_q[x]$ and construct $A/A[P]$ using the ideas of Elkies.

Example By probing depths we find the exponents of small prime divisors of the discriminant of $\mathrm{disc}(\mathbb{Z}[\pi])$ in $\mathrm{disc}(\mathrm{End}(A))$ first.

Elliptic curves over $\mathbb{F}_{1774720755003177239886849307 3}$		
ℓ	j	Ξ_ℓ
2	172312560560722443619199908 86	$(1)^3$
	116783496993645786327741928 46	$(1)^3$
	17490809909988199169685428 0	$(1)^3$
	17416792736585917988100952 73	$(1)^3$
	85928498537509672956630814 0	$(1)(2)$
	10708566226384585303085918797	$(1)^3$
	10468492235421567140789372959	$(1)(2)$
3	172312560560722443619199908 86	$(1)(2)$
7	172312560560722443619199908 86	$(1)^8$
	67621066507837128957256754 31	$(1)(2)$



Consider the index at 2. Our first probe (walk down the left side of the tree) terminates after 4 isogenies. We do a second probe (walk down the right side of the tree) and find the sequence terminates at the floor of rationality after 2 isogenies. We take the minimum and conclude that the index at 2 is 4. From the table above we similarly find $[\mathrm{End}(A)_3 : \mathbb{Z}[\pi]_3] = 1$ and $[\mathrm{End}(A)_7 : \mathbb{Z}[\pi]_7] = 7$. In order to have the smallest possible class group we would like to find a curve lying near the surface for each prime 2, 3 and 7. It is easy to find a curve just one level above the floor of rationality at ℓ since the unique isogeny of degree ℓ over $\mathbb{F}_p$ going from a curve at the floor is to a curve with larger endomorphism ring. However, finding a curve at the surface involves a brute force search for one. Of the $\ell + 1$ elliptic curves isogenous to A via an isogeny of degree ℓ, only one lies at a depth less than A. So at each depth above the floor we must calculate up to $\ell + 1$ isogenies and determine the depth at which they lie with the methods described in the previous two sections. By

means of such a search we identify an elliptic curve with j-invariant

$$580821385975059568086463192 \bmod p$$

which lies at the surface with respect to 2, 3 and 7. We know that either $\mathrm{disc}(\mathrm{End}(A)) = -3 \cdot 547^2 \cdot 105953$ or $\mathrm{End}(A)$ is maximal with $\mathrm{disc}(\mathrm{End}(A)) = -3 \cdot 105953$. In the maximal order, $\mathcal{O}_K$ of K there exists a principal ideal $S_1 S_2^3$ of norm $13 \cdot 19^3$. It follows from the fact that 13 and 19 are coprime to $[\mathcal{O}_K : \mathbb{Z}[\pi]]$, that in any $\mathbb{Z}$-order, $\mathcal{O}$, containing $\mathbb{Z}[\pi]$, the primes P_1 and P_2 restrict to $(13, \pi - 3)\mathcal{O}$ and $(19, \pi + 3)\mathcal{O}$ in $\mathcal{O}$ respectively. $A/A[S_1]$ is isogenous to A via an isogeny of degree 13 induced by the ideal S_1. It has j-invariant

$$491225607620541146270113976 3 \bmod p.$$

Continuing as described above we then construct 3 isogenies induced by the ideal S_2 as well. We get a sequence of elliptic curves with the following j-invariants (taking mod p):

$$\begin{array}{c} 580821385975059568086463192 \\ \bullet \\ 491225607620541146270113976 3 \\ \bullet \\ 669576847411527478166178236 6 \\ \bullet \\ 100139838059437636125606584 88 \\ \bullet \\ 763088943985577825880020317 6 \end{array}$$

We see that the last j-invariant is not equal to the j-invariant of our curve lying at the surface, that $S_1 S_2^3$ is not principal in its endomorphism ring and thus $\mathrm{disc}(\mathrm{End}(A)) = -2^{18} \cdot 3^2 \cdot 7^{10} \cdot 547^2 \cdot 105953$. □

We now turn to the general case, so for the rest of this section C will denote a genus g hyperelliptic curve defined over $\mathbb{F}_q$ with Jacobian, $A = \mathrm{J}_C(\mathbb{F}_q)$, an ordinary g-dimensional abelian variety over $\mathbb{F}_q$. Let π be the Weil q-number associated to the frobenius element, then $K = \mathbb{Q}[\pi] = \mathrm{End}_{\mathbb{F}_q} \otimes \mathbb{Q}$ is a commutative semisimple $\mathbb{Q}$-algebra. All endomorphisms of A are defined over $\mathbb{F}_q$ and $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(A)$ is a $\mathbb{Z}$-order in K contained in a unique maximal $\mathbb{Z}$-order, $\mathcal{O}_K$.

Given any ordinary curve we first look at it's isogeny class and use Proposition 3.6.6 to determine the discriminant $\mathrm{disc}(\mathbb{Z}[\pi, q\pi^{-1}])$. It might be that $\mathcal{O}_K \cong \mathbb{Z}[\,\pi, q\pi^{-1}\,]$ in which case the endomorphism ring of A must be maximal as well.

Example Consider the Jacobian of the hyperelliptic curve defined by

$$C \ : \ y^2 = x^5 + x^4 + x^3 + x^2 + 3x + 4$$

over $\mathbb{F}_7$ with charateristic polynomial

$$\chi = x^4 + 4x^3 + 12x^2 + 28x + 49.$$

The Jacobian is ordinary and simple. $L = K$ is the number field generated by χ over the rationals. Here $\mathrm{disc}(\mathbb{Z}[\pi, q\pi^{-1}]) = 2^8 \cdot 3^3 \cdot 19 = \mathrm{disc}(\mathcal{O}_K)$ and thus the endomorphism ring must be the maximal order in K. □

By now we know that this is not always the case. In theory we can use the method used in the proof of Theorem 2.1.20 to construct a sequence of $\mathbb{Z}$-orders

$$R \subset \mathcal{O}_0 \subset \mathcal{O}_1 \subset \ldots \subset \mathcal{O}_m = \mathcal{O}_K$$

in K where we have a $\mathbb{Z}$-basis for each $\mathcal{O}_j$ and in particular we control the sizes of the discriminants. We can for each j determine if $\mathcal{O}_j \subseteq \mathcal{O}$ by checking if the generators of the ring $\mathcal{O}_j$ are endomorphisms. We can do this by computing the group structure of $A(\mathbb{F}_{p^k})$ for small values of k and use the generators found, to explicitly compute the action of frobenius on various torsion subgroups to determine whether or not certain elements of $\mathcal{O}_K$ are endomorphisms.

We know that every endomorphism ring in the isogeny class of A including A contains the ring $R = \mathbb{Z}[\pi, q\pi^{-1}]$. To test whether $\alpha \in \mathcal{O}_K$ is an endomorphism, we express it a polynomial in π and integral denominators determined by the coefficients of π as an element in $\mathcal{O}_K$. By the arguments in section 3.5.2, in each case it suffices to check whether the numerator acts as zero on the n-torsion, where n is the denominator. The ideal I_ℓ for a prime ℓ, constructed in section 4.2.2, can likewise be constructed for any odd n to represent n-torsion divisors. This can be used to test the action of endomorphisms on the n-torsion subgroup of A. For example, to check that π^k (or any other polynomial in π) acts like a on the n-torsion, it suffices to check that in $\mathbb{F}_q[x_1, x_2, y_1, y_2]$, $\pi^k(D) \equiv aD \bmod I_n$. We remark that even though the algorithm is not fully implemented yet, this is not practical for large n.

We've seen that in the genus 1 case we can use information about the ℓ-isogenous curves to determine if a high power of a small prime divides the index of $\mathbb{Z}[\pi, q\pi^{-1}]$ in $\mathcal{O}$. Further we could also use the fact that every ideal is a kernel ideal and that every subgroup of A is of the form $A/\mathrm{G}_{\ker}(M)$ for some ideal M in $\mathcal{O}$ to, with the methods in Section 4.3.1, then construct isogenies to other elliptic curves from only knowing their kernel. In this fashion we could obtain a chain of isogenies and use this information to determine if a large prime divide the index of $\mathbb{Z}[\pi, q\pi^{-1}]$ in $\mathcal{O}$. In genus greater than 1 we know about the abelian varieties ℓ-isogenous to the Jacobian but in general these need not be Jacobians. Furthermore, as we've seen in the previous chapter, in $g \geq 2$, the conditions on ideals above only hold in very special cases. And even in those cases this seems to be hopeless since we have no method of constructing isogenies.

In the next section we'll illustrate the the ideas mentioned above by using a similar strategy to test if the endomorphism ring is the full ring of integers. To do this we restrict to genus 2 hyperelliptic curves.

Maximality

Let C be hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$ with Jacobian, $A = \mathrm{J}_{\mathbb{F}_q}(C)$, a simple ordinary 2-dimensional abelian variety over $\mathbb{F}_q$. Then $K = \mathrm{End}(A) \otimes \mathbb{Q}$ is a CM field of

dimension 4 over $\mathbb{Q}$. Let K^+ be it's totally real subfield. We have $K = \mathbb{Q}(\alpha)$,

$$\alpha = \begin{cases} i\sqrt{a+b\sqrt{d}} & \text{where } d = \frac{1}{4}\text{disc}_{\mathbb{Z}}(\mathcal{O}_{K^+}) \text{ if } \text{disc}_{\mathbb{Z}}(\mathcal{O}_{K^+}) \equiv 0 \bmod 4 \\ i\sqrt{a+b\frac{-1+\sqrt{d}}{2}} & \text{where } d = \text{disc}_{\mathbb{Z}}(\mathcal{O}_{K^+}) \text{ if } \text{disc}_{\mathbb{Z}}(\mathcal{O}_{K^+}) \equiv 1 \bmod 4 \end{cases}$$

The first case corresponds to when $\alpha = a+b\sqrt{d}$ is squarefree and totally positive ($a \pm b\sqrt{d} > 0$). Assume further that K^+ has class number one. In this case we can find an integral basis for the ring of integers in K such that

$$\mathcal{O}_K = \mathcal{O}_{K^+}[\gamma], \quad \gamma \in \mathcal{O}_K.$$

Since A is simple, the $\mathbb{Z}$-orders in K containing $\mathbb{Z}[\pi, q\pi^{-1}]$ are exactly the representatives for elements in the isogeny class of A and so $\mathcal{O}$ is an $\mathbb{Z}$-order in K such that $\mathbb{Z}[\pi, q\pi^{-1}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. The smaller the index of $\mathbb{Z}[\pi, q\pi^{-1}]$ in $\mathcal{O}_K$, the less work it takes to decide if the endomorphism ring of A is maximal. The next proposition gives a bound for the index of $\mathbb{Z}[\pi, q\pi^{-1}]$ in $\mathcal{O}_K$.

Proposition 4.4.4 *Let $K = \mathbb{Q}(\alpha)$ be a quartic CM field, where $\alpha = i\sqrt{a+b\sqrt{d}}$ with $a, b, d \in \mathbb{Z}$ and d and $\gcd(a, b)$ square free. Let $\mathcal{O}_K$ be its ring of integers. Assume for simplicity that the Frobenius endomorphism is of the form $\pi = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})\alpha$ with $c_1, \ldots, c_4 \in \mathbb{Z}$, that $a^2 - b^2 d$ is square free and that K^+ is a principal ideal domain.*

$$\text{Then} \quad \begin{cases} [\,\mathcal{O}_K : \mathbb{Z}[\sqrt{d}, \alpha]\,] = 2 \text{ and } [\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,] \leq 8c_2(c_3^2 - c_4^2 d) \text{ if } d \equiv 2, 3 \bmod 4. \\ [\,\mathcal{O}_K : \mathbb{Z}[\sqrt{d}, \alpha]\,] = 4 \text{ and } [\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,] \leq 16c_2(c_3^2 - c_4^2 d) \text{ if } d \equiv 1 \bmod 4. \end{cases}$$

Proof We have $\pi + q\pi^{-1} - 2c_1 = 2c_2\sqrt{d}$, $(2c_2c_3 - c_4(\pi + q\pi^{-1} - 2c_1))(\pi - q\pi^{-1}) = 4c_2(c_3^2 - c_4^2 d)\alpha$ and $(c_3 - c_4\sqrt{d})(\pi - q\pi^{-1}) = 2(c_3^2 - c_4^2 d)\alpha$. So $\mathbb{Z}[2c_2\sqrt{d}, 4c_2(c_3^2 - c_4^2 d)\alpha] \subseteq \mathbb{Z}[\pi, q\pi^{-1}]$. Since K^+ is a principal ideal domain, we have a relative integral basis of $\mathcal{O}_K$ over $\mathcal{O}_{K^+}$. We can choose a relative basis of the form $\{1, \gamma\}$, and by [34], in the case that $d \equiv 2, 3 \bmod 4$, we have $[\,\mathcal{O}_K : \mathbb{Z}[\sqrt{d}, \alpha]\,] = 2$ and

$$\gamma = \begin{cases} \frac{1}{2}\alpha, \\ \frac{1}{2}(1 + \alpha), \\ \frac{1}{2}(\sqrt{d} + \alpha) \text{ or} \\ \frac{1}{2}(1 + \sqrt{d} + \alpha). \end{cases}$$

For $d \equiv 1 \bmod 4$, $[\,\mathcal{O}_K : \mathbb{Z}[\sqrt{d}, \alpha]\,] = 4$ and

$$\gamma = \begin{cases} \frac{1}{4}(1 + \sqrt{d} + 2\alpha), \\ \frac{1}{4}(-1 + \sqrt{d} + \alpha) \text{ or} \\ \frac{1}{4}(-b + \sqrt{d} + 2\alpha). \end{cases}$$

We have

$$\mathbb{Z}[\pi, q\pi^{-1}] \subseteq \mathbb{Z}[\pi, q\pi^{-1}, \sqrt{d}] \subseteq \mathbb{Z}[\sqrt{d}, \alpha] \subseteq \mathcal{O}_K$$

with $[\,\mathbb{Z}[\pi, q\pi^{-1}, \sqrt{d}] : \mathbb{Z}[\pi, q\pi^{-1}]\,] \leq 2c_2$ and $[\,\mathbb{Z}[\sqrt{d}, \alpha] : \mathbb{Z}[\pi, q\pi^{-1}, \sqrt{d}]\,] \leq 2(c_3^2 - c_4^2 d)$. If $d \equiv 2, 3 \bmod 4$, then $[\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,] \leq 8c_2(c_3^2 - c_4^2 d)$ and if $d \equiv 1 \bmod 4$ then

$[\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,] \leq 16c_2(c_3^2 - c_4^2 d)$. □

When $a_2 - b_2 d$ is not square free the representation of the ring of integers can become more complicated (see [34]), but the index $[\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,]$ is still a constant multiple of $c_2(c_3^2 - c_4^2 d)$. Using the relative basis of $\mathcal{O}_K$ over $\mathcal{O}_{K^+}$ we can also determine which denominators can occur in the coefficients c_i of the frobenius endomorphism and generalize our argument to the general case.

From this we see that, for example, to show that the endomorphism ring of A is the full ring of integers $\mathcal{O}_K$, it suffices to test whether $\sqrt{d}$ is an endomorphism, where $2c_2\sqrt{d} = \pi + q\pi^{-1} - 2c_1$ and whether α is an endomorphism, where $(4c_2(c_3^2 - c_4^2 d))\alpha = (2c_2c_3 - c_4(\pi + q\pi^{-1} - 2c_1))(\pi - q\pi^{-1})$. Here the c_i's are the coefficients of π written in the relative basis. Finally we have to check that γ is an endomorphism, where γ is one of the 7 possible elements listed in the proof of Proposition 4.4.4 in the case that $a^2 - b^2 d$ is square free. If any one of these conditions fails, we conclude that the endomorphism ring of the curve is not isomorphic to the full ring of integers, $\mathcal{O}_K$ in K. When $a^2 - b^2 d$ is not square free then the relative integral basis is listed in the table in [34].

Example Consider the genus 2 hyperelliptic curve

$$C:\ y^2 = 5x^6 + 21x^5 + 36x^4 + 7x^3 + 29x^2 + 32x + 10 \quad \text{over } \mathbb{F}_{43}.$$

Let $A = \mathrm{J}_{\mathbb{F}_{43}}(C)$ be the Jacobian variety. The characteristic polynomial of the frobenius element is given by

$$\chi = x^4 - 8x^3 + 50x^2 - 344x + 1849.$$

It is an irreducible ordinary weil polynomial. The endomorphism algebra of A is isomorphic to the CM field

$$K = \mathbb{Q}(\alpha), \quad \alpha = i\sqrt{a + b\sqrt{d}} = i\sqrt{13 - 3\sqrt{13}}.$$

The CM field K has real quadratic subfield $K^+ = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{13})$ and 43 splits completely in K^+. For $\lambda = \frac{1}{2}(\sqrt{13} + 1)$, we note that the ring of integers in K^+,

$$\mathcal{O}_{K^+} = \mathbb{Z}[\lambda]$$

is a principal ideal domain and the ring of integers in K is given by

$$\mathcal{O}_K = \mathcal{O}_{K^+}[\alpha] = \mathbb{Z} + \lambda\mathbb{Z} + (\mathbb{Z} + \lambda\mathbb{Z})\alpha.$$

The discriminants are given by $\mathrm{disc}(\mathcal{O}_K) = 2^6 \cdot 13^3$ and $\mathrm{disc}(\mathbb{Z}[\pi, q\pi^{-1}]) = 2^{14} \cdot 3^2 \cdot 13^3$ giving $[\,\mathcal{O}_K : \mathbb{Z}[\pi, q\pi^{-1}]\,] = 2^4 \cdot 3$. The prime 43 factors in K/K^+ as

$$43 = \pi\epsilon_{\mathbb{C}}(\pi) = (-3 + 2\lambda + (-2 - \lambda)\alpha) \cdot (-3 + 2\lambda + (2 + \lambda)\alpha)$$

and we observe that

$$\frac{\pi^4 - 1}{12} = -2 + 24\sqrt{13} + \frac{1}{2}17\sqrt{13}i\sqrt{13 - 3\sqrt{13}} + \frac{1}{2}113i\sqrt{13 - 3\sqrt{13}} \in \mathcal{O}_K,$$

so if $\mathrm{End}(A)$ is maximal then A must have the full 12-torsion defined over $\mathbb{F}_{43}^4$. It turns out that this is the case here. From Section 3.5.2 we know that for any $\alpha = \frac{1}{n}(f(\pi)) \in \mathcal{O}_K$ (with f a function in π) is an endomorphism if and only if $f(\pi)$ acts as zero on n-torsion. So for example $\lambda = \frac{1}{4}(\pi + q\pi^{-1} + 6)$ is an endomorphism if and only if $\pi + q\pi^{-1} + 6$ acts as zero on 4-torsion or equivalently $\pi + q\pi^{-1}$ acts as multiplication by 2 on 4-torsion. We see that all 4-torsion is defined over a degree 4 extension and we can compute a group structure over a degree 4 extension with generators $\{D_1, D_2, D_3, D_4\}$. We compute the action of the frobenius on each basis element and get the set $\{\pi(D_1), \pi(D_2), \pi(D_3), \pi(D_4)\}$. We write these in terms of the elements in the basis. In this way the action of π on 4-torsion can be expressed as a 4×4 matrix. We find $q\pi^{-1}$ by the fact that $\pi q \pi^{-1} = q$ and the multiplication by q acts as as multiplication by 3 on 4-torsion. The matrices for π and $q\pi^{-1}$ are given by

$$\begin{bmatrix} 1 & 0 & 1 & 3 \\ 2 & 1 & 1 & 0 \\ 0 & 2 & 3 & 5 \\ 2 & 2 & 2 & 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 3 & 1 \\ 2 & 1 & 3 & 0 \\ 0 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}$$

respectively. From this it is not hard to see that $\pi + q\pi^{-1}$ acts as multiplication by 2 on 4-torsion so λ is an endomorphism of A and thus $\mathrm{End}(A)$ is the maximal $\mathbb{Z}$-order in K. $\square$

4.4.2 Supersingular elliptic curves

Let A be a supersingular elliptic curve over $\mathbb{F}_q$, let $L = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ be its endomorphism algebra and associated the frobenius endomorphism with a Weil q-number, π. Note that supersingular elliptic curves are almost-ordinary abelian varieties The rank of their group of p-torsion points over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ is equal to zero. We have that π^2 is equal to a root of unity ζ_m times a power of p. Thus suppose $\mathrm{End}_{\mathbb{F}_q}(A) \neq \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ is commutative and $\pi \notin \mathbb{Z}$, then determining the isomorphism type of $\mathrm{End}_{\mathbb{F}_q}(A)$ amounts to determining the index of $\mathbb{Z}[\pi]$ in $\mathrm{End}_{\mathbb{F}_q}(A)$ locally at 2 since $\mathrm{End}_{\mathbb{F}_q}(A)$ is always maximal at p and $\mathbb{Z}[\pi]$ is locally maximal everywhere outside of 2 and p. In this case the methods developed for ordinary elliptic curves can be used to determine the index, We therefore only consider the case where $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$.

We have seen that $\mathrm{End}(A)$ is a $\mathbb{Z}$-order in the uniquely determined (up to isomorphism) definite quaternion algebra L over $\mathbb{Q}$ ramified at exactly p and ∞.

Theorem 4.4.5 *Let R be a $\mathbb{Z}$-order in L which is a representative for some B in the isogeny class of A. Suppose L is non-commutative.*

(a) For all integral left R-ideal M we have $\mathrm{I}_{\mathrm{ker}}(M) = M$.

(b) $\{[B]_{\cong_{\mathbb{F}_q}} | \ B \in [A]_{\equiv_{\mathbb{F}_q}}\}$ forms a homogeneous space for the Brandt groupoid and contains $\mathrm{h}(R)$ isomorphism classes. For each such R, there are one or two isomorphism classes depending on if the R-ideal P with $P^2 = pR$ is principal or not.

Proof It follows directly from Proposition 3.5.8(b) that every ideal is a kernel ideal. Equivalent to the proof of Theorem 4.4.1 we have the ideal class group operating freely on the isomorphism classes of curves with representative R. We must show that there is only one

orbit. Again we simply look at lattices. At $\ell \neq p$ we have (as we saw) $\mathbb{M}_2(\mathbb{Z}_\ell)$ acting on $\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$ and obviously are all given by powers of the maximal ideal generated by . Take R as a representative for A. By Proposition 3.5.4 all the other B we want can be obtained from ideals M having $\mathrm{End}(A/\mathrm{G}_{\ker}(M) = R$. By Proposition 3.5.7(b) these are the two-sided fractional ideals. But it can be shown that every two-sided fractional ideal in R has the form nR or nP. These present one ideal class if P is principal, two otherwise. □

An equivalence of categories

Deuring proved in his classical article that there is a bijection between the fractional two-sided ideal classes of a maximal $\mathbb{Z}$-order, $\mathcal{O}$, in L of a certain type and the j-invariants of supersingular elliptic curves with endomorphism ring of that type in an algebraically closed field of characteristic p.

Let A be a supersingular elliptic curve over $\mathbb{F}_q$. Let M be a set of isogenies of A and let $\mathcal{O}$ be a maximal $\mathbb{Z}$-order in L. From Theorem 3.5.8 (b) we have that every integral left $\mathcal{O}$-ideal, M, is a kernel ideal and every finite subgroup of A is of the form $\mathrm{G}_{\ker}(M)$ for some projective integral left $\mathcal{O}$-ideal M.

Proposition 4.4.6 *Let $M \subseteq \mathrm{Hom}(B, A)$ be a left $\mathrm{End}(A)$-module and let $N \subseteq \mathrm{Hom}(A, B)$ be a right $\mathrm{End}(A)$-module. Then there exists an elliptic curve C over $\mathbb{F}_q$ and an isogeny $\delta : B \to C$ such that $M = \mathrm{Hom}(C, A)\delta$. Likewise there exists an elliptic curve C over $\mathbb{F}_q$ and an isogeny $\delta : C \to B$ such that $N = \delta\mathrm{Hom}(A, C)$.*

Proof By means of an isogeny $\varphi : A \to B$ there exist embeddings of M and $\mathrm{Hom}(B, A)$ in $\mathrm{End}(A)$ as integral left $\mathrm{End}(A)$-ideals such that $M\varphi \subseteq \mathrm{Hom}(B, A)\varphi \subseteq \mathrm{End}(A)$. Let $C = A/\mathrm{G}_{\ker}(M\varphi)$ and let $\alpha : A \to C$ be the isogeny with kernel $\mathrm{G}_{\ker}(M\delta)$. There exists an isogeny $\delta : B \to C$ such that $\delta = \alpha\varphi$ because $\ker(\varphi) \subseteq \ker(\alpha)$. So we have

$$M\varphi = \{\delta \in \mathrm{End}(A) \mid \mathrm{G}_{\ker}(M\varphi) \subseteq \mathrm{G}_{\ker}(\delta)\} = \mathrm{Hom}(C, A)\alpha$$

and thus $M = \mathrm{Hom}(C, A)\delta$. The result holds for N by taking duals. □

Let $\mathcal{O}$ be a maximal $\mathbb{Z}$-order in L containing an element of reduced norm q. For M and N, projective right $\mathcal{O}$-modules of rank 1, let $\varphi : M \to N$ be a $\mathcal{O}$-module homomorphism. Both M and N are locally free and for each prime ℓ and we can find generators $a \in M_\ell$ and $b \in N_\ell$ such that $M_\ell = a\mathcal{O}_\ell$ and $N_\ell = b\mathcal{O}_\ell$. Then the image of a under the map $\varphi \otimes \mathbb{Z}_\ell$ is bc_ℓ for some $c_\ell \in \mathcal{O}_\ell$. This allows us to define the reduced norm map on $\mathrm{Hom}(M, N)$ by setting

$$\begin{aligned} \overline{\mathrm{n}}\mathrm{orm} : \mathrm{Hom}(M, N) &\to \mathbb{Z} \\ \varphi &\mapsto \prod_\ell \#(\mathbb{Z}_\ell/\overline{\mathrm{n}}\mathrm{orm}(c_\ell)\mathbb{Z}_\ell). \end{aligned}$$

With this definition at hand we can define a category $\mathcal{L}_q$ with objects the pairs (M, π_M) where M is a projective right $\mathcal{O}$-module of rank 1 and π_M an endomorphism of M of reduced norm q. A morphism of objects (M, π_M) and (N, π_N) in $\mathcal{L}_q$ is defined to be the homomorphism $\varphi : M \to N$ satisfying $\varphi\pi_M = \pi_N\varphi$.

Consider the category $\mathcal{A}_q$ consisting of pairs (A, π_A) where A is an elliptic curve over $\mathbb{F}_q$ and π_A the frobenius endomorphism relative to $\mathbb{F}_q$. A morphism of objects (A, π_A) and (B, π_B) in $\mathcal{A}_q$ is defined to be a homorphism $\varphi : A \to B$ such that $\varphi\pi_A = \pi_B\varphi$.

Theorem 4.4.7 *The categories $\mathcal{L}_q$ and $\mathcal{A}_q$ are equivalent.*

Proof We define a functor D_q from $\mathcal{A}_q$ to $\mathcal{L}_q$ as follows. For any maximal $\mathbb{Z}$-order $\mathcal{O}$ in L we know that $\mathcal{O}$ is a representative for an endomorphism ring of an elliptic curve, C, over $\mathbb{F}_q$. We fix such a curve and identify its endomorphism ring with $\mathcal{O}$. The functor takes an object (A, π_A) in $\mathcal{A}_q$ to an object $(\mathrm{D}_q(A), \mathrm{D}_q(\pi_A))$ in $\mathcal{L}_q$ where $\mathrm{D}_q(A) = \mathrm{Hom}(C, A)$ and $\mathrm{D}_q(\pi_A)$ is the endomorphism of $\mathrm{D}_q(A)$ given by left composition with π_A. For any morphism of objects (A, π_A) and (B, π_B) in $\mathcal{A}_q$, given by $\varphi : A \to B$, there exist a well defined morphism $\mathrm{D}_q(\varphi) : \mathrm{Hom}(C, A) \to \mathrm{Hom}(C, B)$, given by left composition by φ, satisfying the condition $\mathrm{D}_q(\varphi)\mathrm{D}_q(\pi_A) = \mathrm{D}_q(\pi_A)\mathrm{D}_q(\varphi)$. Note that one can also have defined $\mathcal{L}_q$ taking projective right $\mathcal{O}$-modules instead. The two categories are dual in the sense that there exists an contravariant equivalence between them. The definition of $\mathcal{L}_q$ as a category of projective right $\mathcal{O}$-modules ensures that the functor D_q is covariant.
In order to prove that the categories are equivalent it will suffice to prove that the functor D_q is full and faithful and that each object in $\mathcal{L}_q$ is isomorphic to an object in the image of D_q. It is clear that D_q is faithful. To prove that D_q is full we need to show that every right $\mathcal{O}$-module homomorphism $\varphi : \mathrm{Hom}(C, A) \to \mathrm{Hom}(C, B)$ arises by composing on the left with an isogeny $\varrho : A \to B$. From Proposition 4.4.6 the image of φ in $\mathrm{Hom}(C, B)$ is of the form $\varrho\mathrm{Hom}(C, A)$. Comparing φ with left multiplication by ϱ, the two $\mathcal{O}$-module homomorphisms differ only up to a unit in the left order, $\mathrm{O}_{\mathrm{left}}(\mathrm{Hom}(C, A))$. Thus multiplying ϱ by a unit $\varphi = \mathrm{D}_q(\varrho)$ has the required form. The equivalence of the commutativity relations $\varphi\mathrm{D}_q(\pi_A) = \mathrm{D}_q(\pi_A)\varphi$ and $\varrho\pi_A = \pi_A\varrho$ is trivially verified.
It remains to show that every object (M, π_M) in $\mathcal{L}_q$ is isomorphic to an object of the form $(\mathrm{D}_q(A), \mathrm{D}_q(\pi_A))$. Every fractional ideal of a maximal $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$ is locally free at all finite primes ℓ in $\mathbb{Z}$, so it follows from [29] Theorem 40.5 that $\mathcal{O}$ is a hereditary $\mathbb{Z}$-order in L (every one-sided fractional $\mathcal{O}$-ideal is projective). Thus a projective $\mathcal{O}$-module is projective of rank 1 if it is isomorphic to a fractional $\mathcal{O}$-ideal. Let (M, π_M) be an object in $\mathcal{L}_q$. Since $\mathcal{O}$ is hereditary we can embed M as a fractional right $\mathcal{O}$-ideal. By Proposition 4.4.6 $M \cong \varrho\mathrm{Hom}(C, B)$ and so $M \cong \mathrm{Hom}(C, B)$. This isomorphism $\pi_M : M \to M$ induces a homomorphism of right $\mathcal{O}$-modules, $\mathrm{Hom}(C, B) \to \mathrm{Hom}(C, B)$, of reduced norm q and by Proposition 4.4.6 this map is given by composition to the left by the element π_B. By arguments given in [14], this asserts the existence of an elliptic curve A over $\mathbb{F}_q$ and an isomorphism to B over some extension of $\mathbb{F}_q$ such that $\pi_B \mapsto \pi_A$ under the isomorphism of endomorphism rings which completes our proof. □

Isogenies and quadratic modules

The equivalence of categories described in the previous section carries over not only the structure of maps of objects in the respective categories, but also relates the additional structure of the degree map on isogenies of supersingular elliptic curves over $\mathbb{F}_q$ to the reduced norm on morphisms of projective $\mathcal{O}$-modules where $\mathcal{O}$ is a maximal $\mathbb{Z}$-order in a definite quaternion algebra L over $\mathbb{Q}$.

Let A and B be supersingular elliptic curves over $\mathbb{F}_q$. As a $\mathbb{Z}$-module $M = \mathrm{Hom}(A, B)$ has rank 4 and its degree map gives $(V, q_V) = (\mathrm{Hom}(A, B) \otimes \mathbb{Q}, \deg)$ the structure of a quadratic space over $\mathbb{Q}$ such that M is a $\mathbb{Z}$-lattice in V.

Suppose A and B are isogenous. Consider the pair $(M, q_M) = (\mathrm{Hom}(A, B), \deg)$. If the associated bilinear map $b_M(\varphi, \varrho) = q_M(\varphi + \varrho) - q_M(\varphi) - q_M(\varrho) = \deg(\varphi + \varrho) - \deg(\varphi) - \deg(\varrho)$ on isogenies φ and ϱ in M can be extended by linearity to all of V, then (M, q_M) is a quadratic module over $\mathbb{Z}$ contained in (V, q_V).

Theorem 4.4.8 *For any positive definite module (M, q_M) over $\mathbb{Z}$ such that $\det_{\mathbb{Z}}(M, q_M) = p^2$, there exists supersingular elliptic curves over $\mathbb{F}_q$ such that $(M, q_M) \equiv (\mathrm{Hom}(A, B), \deg)$ as quadratic modules over $\mathbb{Z}$.*

Proof From Proposition 2.3.26 there exists a $\mathbb{Z}$-order $\mathcal{O}$ in the quaternion algebra ramified at p and ∞ such that M has the structure of a left projective module over $\mathcal{O}$. By the equivalence of categories in Theorem 4.4.7 every projective module arises as a module of homomorphisms of supersingular elliptic curves. □

Theorem 4.4.9 *Consider the quadratic module $(M, q_M) = (\mathrm{Hom}(A, B), \deg)$ over $\mathbb{Z}$ for isogenous supersingular elliptic curves A and B over $\mathbb{F}_q$.*

(a) Suppose $\mathcal{O}$ is representated by the elliptic curve, C, in the isogeny class of A and B. Then for all $\alpha \in M$ and associated quadratic modules, $(\mathrm{Hom}(C, A), \deg)$ and $(\mathrm{Hom}(C, B), \deg)$, over $\mathbb{Z}$, there exists a similitude

$$\varphi_\alpha : \ \mathrm{Hom}(C, A) \to \mathrm{Hom}(C, B)$$

with similitude factor $q_M(\alpha)$.

(b) Every $\varphi \in M$ determines a $\mathrm{O}_{\mathrm{left}}(M, q_M)$-module embedding

$$\begin{array}{rccc} \iota_\varphi : & M & \to & \mathrm{O}_{\mathrm{left}}(M, q_M) \\ & \alpha & \mapsto & \alpha \circ \deg(\varphi)\varphi^{-1} \end{array}$$

of M into its left order as a left $\mathrm{O}_{\mathrm{left}}(M, q_M)$-submodule. Conversely all $\mathrm{O}_{\mathrm{left}}(M, q_M)$-module structures on M arising from an embedding of M into $\mathrm{O}_{\mathrm{left}}(M, q_M)$ are given by ι_φ for some φ in M.

(c) For any other supersingular elliptic curves C and D over $\mathbb{F}_q$ we have $(M, q_M) \equiv (\mathrm{Hom}(C, D), \deg)$ as quadratic modules over $\mathbb{Z}$ if and only if one of the following holds where $\overline{\pi}_p$ denotes the p^{th}-power frobenius automorphism of $\overline{\mathbb{F}}_q$.

(i) $A(\overline{\mathbb{F}}_q) \cong C(\overline{\mathbb{F}}_q)$ and $B(\overline{\mathbb{F}}_q) \cong D(\overline{\mathbb{F}}_q)$.
(ii) $A(\overline{\mathbb{F}}_q) \cong \overline{\pi}_p(C(\overline{\mathbb{F}}_q))$ and $B(\overline{\mathbb{F}}_q) \cong \overline{\pi}_p(D(\overline{\mathbb{F}}_q))$.
(iii) $A(\overline{\mathbb{F}}_q) \cong D(\overline{\mathbb{F}}_q)$ and $B(\overline{\mathbb{F}}_q) \cong C(\overline{\mathbb{F}}_q)$.
(iv) $A(\overline{\mathbb{F}}_q) \cong \overline{\pi}_p(D(\overline{\mathbb{F}}_q))$ and $B(\overline{\mathbb{F}}_q) \cong \overline{\pi}_p(C(\overline{\mathbb{F}}_q))$.

(d) For the quadratic module $(N, q_N) = (\mathrm{Hom}(B, A), \deg)$ *over* $\mathbb{Z}$ *consisting of the dual isogenies equipped with the degree map. There exists an unique* $\mathbb{Z}$*-module homomorphism*

$$\varphi : \ \mathrm{Cliff}(M) \to S = \begin{bmatrix} \mathrm{O}_{\mathrm{left}}(M, q_M) & M \\ N & \mathrm{O}_{\mathrm{right}}(M, q_M) \end{bmatrix}$$

such that $\iota_S \iota_M = \varphi$.

(e) Any $\mathbb{Z}$*-order* $\mathcal{O}$ *in some quadratic extension of* $\mathbb{Q}$ *with* $\overline{\mathrm{d}}\mathrm{isc}(\mathcal{O}) = \det_{\mathbb{Z}}(N, q_N)$ *for some binary quadratic module* (N, q_N) *over* $\mathbb{Z}$ *such that*

(i) $q_N(N)$ *is not contained in any proper ideal in* $\mathbb{Z}$ *and*

(ii) there exists a $\mathbb{Z}$*-module homomorphism* $\varphi : \ N \to M$ *satisfying*

(1) $q_M(\varphi(\alpha)) = q_N(\alpha)$ *for all* α *in* N *and*

(2) M/N *is torsion-free as* $\mathbb{Z}$*-module*

optimally embeds into $\mathrm{O}_{\mathrm{left}}(M, q_M)$ *and* $\mathrm{O}_{\mathrm{right}}(M, q_M)$.

(f) Let (N, q_N) *denote the quadratic submodule of* (M, q_M) *consisting of all inseparable isogenies equipped with the degree map. Then* $(N, q_N) \equiv (\mathrm{Ext}_3(M), \Phi_3)$ *as bilinear modules over* $\mathbb{Z}$.

Proof For an isogeny $\alpha : \ A \to B$ in M consider quadratic modules

$$(N, q_N) = (\mathrm{Hom}(C, A), \deg) \ \text{ and } \ (\Lambda, q_\Lambda) = (\mathrm{Hom}(C, B), \deg)$$

contained in the quadratic spaces

$$(V, q_V) = (\mathrm{Hom}(C, A) \otimes \mathbb{Q}, \deg) \ \text{ and } \ (W, q_W) = (\mathrm{Hom}(C, B) \otimes \mathbb{Q}, \deg).$$

The induced map $\varphi_{\mathbb{Q}} : \ V \to W$, $\lambda \mapsto \alpha\lambda$ is a $\mathbb{Q}$-vector space homomorphism such that the restriction map $\alpha_{\mathbb{Z}} : \ N \to \Lambda$ satisfies $q_\Lambda(\alpha_{\mathbb{Z}}(\lambda)) = q_M(\alpha) q_N(\lambda)$. It follows that $\varphi_\alpha = \alpha_{\mathbb{Z}}$ is a similitude with similitude factor $q_M(\alpha) = \deg(\alpha)$. Note however that in general φ_α is not a similarity. This proves (a).

Statement (b) follows from the arguments in the proof of Proposition 4.4.6 and the equivalence of categories in the previous section.

For $(N, q_N) = (\mathrm{Hom}(C, D), \deg)$, each of the four possibilities implies that (M, q_M) is isometric to (N, q_N). Conversely if (M, q_M) is isometric to (N, q_N) then the isometry determines a unique isomorphism of $\mathrm{Cliff}(M)$ with $\mathrm{Cliff}(N)$. Where M is isomorphic to N as a left $e\mathrm{Cliff}_0(M)$-module. The two quaternionic module structures on N are precisely the natural ones on N and the isometric module $(\Lambda, q_\Lambda) = (\mathrm{Hom}(D, C), \deg)$ consisting of dual isogenies. But as representative for A, $\mathcal{O}$ arises up to isomorphism only as the endomorphism ring of curves isomorphic to A and $\overline{\pi}_p(A(\overline{\mathbb{F}}_q)$. By the equivalence of categories in 4.4.7, these are the only possibilities and we have proven (c).

Multiplication in the matrix ring, S, is given by matrix multiplication and composition of isogenies. The homomorphism of N to S via the map

$$\alpha \mapsto \begin{bmatrix} 0 & \alpha \\ \deg(\alpha)\alpha^{-1} & 0 \end{bmatrix}$$

is compatible with the degree map so there exists an unique map φ, commuting with the injection of N in S and the even Clifford algebra $\mathrm{Cliff}_0(M)$ embeds in $\mathrm{O}_{\mathrm{left}}(N, q_N) \times$

$\mathrm{O}_{\mathrm{right}}(M, q_M)$.
Statement (e) follows from Theorem 2.3.24, so its remains to prove (f). Let $(\Lambda, q_\Lambda) = (\mathrm{End}(B), \deg)$ (with associated bilinear map b_Λ) be the quadratic module over $\mathbb{Z}$ associated to a supersingular elliptic curve B over $\mathbb{F}_q$. The singular quadratic discriminant map

$$\begin{aligned} \mathrm{disc} : \Lambda &\to \mathbb{Z} \\ \alpha &\mapsto \mathrm{disc}(\mathbb{Z}[\alpha]) = \mathrm{disc}(\{1, \alpha\}) = -(b_\Lambda(1,1)b_\Lambda(\alpha,\alpha) - b_\Lambda(1,\alpha)^2) \end{aligned}$$

on Λ induces a positive definite quadratic determinant map $\det : \Lambda \to \mathbb{Z},\ \alpha \mapsto -\mathrm{disc}(\alpha)$ on $\Lambda/\mathbb{Z}$. As for the quadratic module (M, q_M) there is no distinguised element playing the role of 1. We do note however that for any α and φ in M, we can express the determinant of the $\mathbb{Z}$-submodule $\mathbb{Z}\varphi + \mathbb{Z}\alpha$ as

$$\det(\mathbb{Z}\varphi + \mathbb{Z}\alpha) = b_M(\varphi,\varphi)b_M(\alpha,\alpha) - b_M(\varphi,\alpha)^2.$$

We use this to give the restriction of the determinant map on Λ to the Λ-submodule $N = \iota_\varphi(M)$ by letting

$$\begin{aligned} \det : N &\to \mathbb{Z} \\ \alpha &\mapsto \det(\mathbb{Z}\varphi + \mathbb{Z}\alpha). \end{aligned}$$

Let (M, q_M) be a quaternary quadratic module over $\mathbb{Z}$ with associated left $\mathcal{O}$-module structure making M into a projective left $\mathcal{O}$-module for some some $\mathbb{Z}$-order $\mathcal{O}$ in a quaternion algebra over $\mathbb{Q}$. For any α in M, consider the quadratic submodule $(\Lambda, q_\Lambda) = (\alpha \wedge M, q_\Lambda)$ of $(N, q_N) = (\mathrm{Ext}_2(M), \Phi_2)$. By setting $n = 4$ and $r = 1$ in Theorem 2.2.3 we get $\det(\Lambda, q_\Lambda) = b_M(\alpha,\alpha)^2\det(M, q_M)$. For any two linearly independant α and β in M, consider the binary quadratic submodule $(\Lambda, q_\Lambda) = (\alpha \wedge \beta \wedge M, q_\Lambda)$ of $(N, q_N) = (\mathrm{Ext}_3(M), \Phi_3)$. By setting $n = 4$ and $r = 2$ in Theorem 2.2.3 we get $\det(\Lambda, q_\Lambda) = \det(\alpha \wedge \beta)\det(M, q_M)$. Furthermore the bilinear submodule $(\Gamma, q_\Gamma) = (\mathrm{diff}(\mathcal{O})M, b_\Gamma)$ of (M, b_M) is isometric to the bilinear module (N, b_N). In particular the bilinear form b_N is even and $\overline{\mathrm{disc}}(\mathcal{O}) = \langle b_N(u,v) \mid u, v \in N\rangle$ (See [23] Theorem 73). The rest now follows from this and by noting that the separable isogenies in M are precisely the isogenies of degree divisible by p and thus the inseparable isogenies are those in $\mathrm{diff}(\mathrm{O}_{\mathrm{right}}(\mathrm{End}(B), \deg)) \cdot \mathrm{Hom}(A, B)$ and also those in $\mathrm{Hom}(A, B) \cdot \mathrm{diff}(\mathrm{O}_{\mathrm{left}}(\mathrm{End}(A), \deg))$. □

Example Recall the setup in Section 2.3.2 and consider the form q of Gauss. The determinant forms introduced in Theorem 4.4.9 serve as a useful tool for presenting this phenomenon. We get that the quadratic form representing the discriminants of imaginary quadratic subrings of $\mathcal{O}$ is given by

$$g(x_1, x_2, x_3) = 3x_1^2 + 2x_1x_2 - 2x_1x_3 + 3x_2^2 + 2x_3x_2 + 3x_3^2.$$

This is the quadratic form associated to the quadratic module, $(\mathcal{O} \cdot 1, \Phi_2)$, contained in $(\mathrm{Ext}_2(M), \Phi_2)$, by means of a choice of basis.

Let $\{\alpha_1, \alpha_2, \alpha_3\}$ be a basis for the quadratic module (M, q_M) associated to q such that

$$q_M(x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3) = q(x_1, x_2, x_3)$$

and let $\{\omega_1, \omega_2, \omega_3\}$ be a basis for the quadratic module (N, q_N) associated to g such that

$$q_N(x_1\omega_1 + x_2\omega_2 + x_3\omega_3) = g(x_1, x_2, x_3).$$

Then the map

$$\varphi: \ M \to N \text{ given by } \begin{cases} \varphi(\alpha_1) = \omega_1 + \omega_2 + \omega_3. \\ \varphi(\alpha_2) = \omega_1 - \omega_2 + \omega_3. \\ \varphi(\alpha_3) = \omega_1 - \omega_2 - \omega_3. \end{cases}$$

on generators is a representation of quadratic modules over $\mathbb{Z}$. Under this map the basis for N is given by

$$\omega_1 = \tfrac{1}{2}(\varphi(\alpha_1) + \varphi(\alpha_3)).$$
$$\omega_2 = \tfrac{1}{2}(\varphi(\alpha_1) - \varphi(\alpha_2)).$$
$$\omega_3 = \tfrac{1}{2}(\varphi(\alpha_2) + \varphi(\alpha_3)).$$

so that $q(x_1, x_2, x_3)$ represents a discriminant of a rank 2 subring of $\mathcal{O}$ if and only if $x_1 \equiv x_2 \equiv x_3 \bmod 2$. □

Knowledge about the subrings optimally embedded in the rings of endomorphisms of supersingular elliptic curves provides strong information about the isomorphism class of this order as indicated by the following proposition.

Proposition 4.4.10 *Let A be a supersingular elliptic curve over $\mathbb{F}_q$ and let R be a $\mathbb{Z}$-order in a complex imaginary quadratic extension of $\mathbb{Q}$. R optimally embeds into* End(A) *if and only if* j(A) *is a root of the class equation modulo p for the discriminant* disc(R)*. In particular A is one of* h(R) *elliptic curves in $[A]_{\sim_{\mathbb{F}_q}}$ containing an optimal embedding of R.*

Proof From Deuring's lifting theorem, A can be lifted to an elliptic curve B over $\overline{\mathbb{Q}}$ with endomorphism ring R. Thus j(B) satisfies the class equation of degree h(R) and j(A) is one of h(R) roots of the reduction of the class polynomial modulo p. □

Higher genus

Similar to the elliptic case Theorem 3.7.7 shows that for simple supersingular abelian varieties that if $L = \mathbb{Q}(\pi)$ we need only to consider the case locally at 2. The prominence of 2 comes in from the fact that the endomorphism ring must contain $\mathbb{Z}[\pi]$ which is either the maximal order in L or has index 2 otherwise. This is essentially the same problem we had in the ordinary case. The quaternion case is discussed in the next section.

4.5 Final remarks

In this section we look at possibilities for further research.

Suppose A is a supersingular hyperelliptic Jacobian with L a quaternion algebra over $K = \mathbb{Q}(\pi)$. We've shown that $\mathbb{Z}[\pi]$ is a Bass order in K and thus we can represent the Tate modules as torsion free modules over a Bass order. From this one can obtain the group structure of A but this was not the motivating goal though. In Section 2.3 we have

looked at the orders in quaternion algebras over number fields keeping our theory very general. It would be interresting to see what connections there are between the structure of the endomorphism rings of the Tate modules (considered as modules over a Bass order) and the orders in the quaternion algebra.

We've mentioned the problem of the isogeny class not entirely consisting of hyperelliptic Jacobians. We wanted to use properties depending on the fact that the variety is the Jacobian of a hyperelliptic curve.

Hyperelliptic Jacobians are principally polarized abelian varieties of CM type and in principal the theory of Shimura and Taniyama allows one to list a complete set of isomorphism classes of g-dimensional simple, principally polarized abelian varieties of CM type over $\mathbb{C}$ for a given CM field of degree deg $2g$, whose reflex field is contained in a CM field. However, the results in the published literature are unsatisfactory. For example, they don't give a good description of the largest abelian extension of a field obtainable in this fashion.

The isomorphism classes are given by period matrices Ω_i. For each period matrix Ω_i we can determine all even theta constants (up to a given precision)

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega_i, 0),\ \delta^t \epsilon \equiv \ \bmod 2 \text{ where } \theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega_i, 0) = \sum_{n \in \mathbb{Z}^g} e^{\pi i (n+\frac{1}{2}\delta)^t \Omega_i (n+\frac{1}{2}\delta) + 2(n+\frac{1}{2}\delta)^t \frac{1}{2}\epsilon}.$$

By using these one can then compute absolute invariants and use Mestre's algorithm to decide whether Ω_i is hyperelliptic and compute the equation $y^2 = f(x)$ of the affine curve over $\mathbb{F}_q$ whose Jacobian corresponds to Ω_i if it exists. I refer the reader to [40] where they address the hyperelliptic Schotty problem and show how Mestre's algorithm can be generalized to obtain an equation for the curve. Recall in section 4.1 we had an example of two curves defined over a finite field whose Jacobians where isomorphic as projective varieties but the curves itself were not isomorphic. However, by Torelli's theorem (see [33] Section 12.) a curve is uniquely determined by its principally polarized Jacobian so with the above method we can obtain set of isomorphism classes of genus g hyperelliptic curves C, defined over $\mathbb{F}_q$, such that their Jacobians is of a given CM type.

It is well know that Jacobians of hyperelliptic curves of genus 2 are exactly the principal polarized abelian varieties of dimension 2, so knowing about the principally polarized abelian varieties in the isogeny class could give additional information, even if it is just in the genus 2 case.

Consider a genus 2 ordinary hyperelliptic curve C over $\mathbb{F}_q$ with Jacobian $A = \mathrm{J}_{\mathbb{F}_q}(C)$. If A is simple then the endomorphism algebra is a CM field of degree 4.

Suppose $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is isomorphic to a CM field K of degree 4 which is either not Galois or Galois with Galois group $\mathbb{Z}/4\mathbb{Z}$. Let K^+ be the totally real quadratic subfield. Choose a CM-type $(K, \Phi) = (K, \{\varphi_1, \varphi_2\})$ of K. For each element of the ideal class group of O_K, choose a representative ideal M_i, and find an integral basis $1, \lambda_i$ for it over the ring of integers of $\mathcal{O}_{K^+}$ in K^+. Each ideal class corresponds to an isomorphism class of an abelian variety over $\mathbb{C}$ via Shimura's theory. The principal polarization(s) on the abelian variety and the corresponding 2×2 period matrix (matrices) Ω_i are given in [34] Section 4.2 and

p.62. The entries of Ω_i are given in terms of λ_i, the CM-type, (K, Φ), and β, the generator of the ring of integers of K^+. For each period matrix, evaluate the ten even theta constants up to some amount of precision. The three absolute Igusa invariants, $\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3$, associated to each period matrix are defined as combinations of the ten even theta constants. Take the product over all possible period matrices to form the three Igusa class polynomials:

$$\begin{aligned} h_1(x) &= \prod_{\Omega_i}(x - \mathrm{j}_1(\Omega_i)) \\ h_2(x) &= \prod_{\Omega_i}(x - \mathrm{j}_2(\Omega_i)) \\ h_3(x) &= \prod_{\Omega_i}(x - \mathrm{j}_3(\Omega_i)). \end{aligned}$$

This is analogous to computing the Hilbert class polynomial associated to an imaginary quadratic field K. The Hilbert class polynomial has integer coefficients so the case of a quartic CM field is different because there are three class polynomials, their coefficients are rational numbers, and the amount of precision required to compute them is not known in advance.

If a principally polarized abelian variety is ordinary we can even say more.

Deligne's down-to-earth description of the category of ordinary abelian varieties over a finite field is expanded upon in [15] to include the concept of a polarization. Deligne's description shows that the category of abelian varieties in an isogeny class is equivalent to the category whose objects are lattices in K, that are modules over the ring $R = \mathbb{Z}[\pi, q\pi^{-1}]$ and whose morphisms are R-module homomorphisms. If R is the ring of integers of K, the objects of this last category are simply the fractional ideals of K. Thus the isomorphism classes of abelian varieties in the isogeny class correspond to the ideal classes of K.

Pectora roborant cultus recti

Using the ideas of Howe, we can check if the isogeny class contains a polarization and in special cases we can give an exact formula for the number of principal polarized abelian varieties lying in a specific isogeny class of a simple ordinary abelian variety.

Suppose χ is an irreducible polynomial of degree $2g$ whose middle coefficient is coprime to q and whose complex roots all have magnitude $\sqrt{q}$. Then via Theorem 3.4.2 χ corresponds to an isogeny class of simple g-dimensional ordinary abelian varieties over $\mathbb{F}_q$. Let π be a root of χ in $\overline{\mathbb{Q}}$. Let K be the CM field $K = \mathbb{Q}(\pi)$, let K^+ be the maximal real subfield of K and consider the $\mathbb{Z}$-order $R = \mathbb{Z}[\pi, q\pi^{-1}]$ of K.

Theorem 4.5.1 *Suppose K/K^+ is ramified at a finite prime, that the unit group of K is equal to the unit group of K^+ and that R is equal to the maximal $\mathbb{Z}$-order in K. Then the number of isomorphism classes of principal polarized abelian varieties (A, λ) in the isogeny class corresponding to χ is equal to the quotient*

$$\frac{\mathrm{h}(K)}{\mathrm{h}(K^+)}$$

of the class number of K by the class number of K^+.

Using the ideas mentioned above to assist in the determination of the Jacobian of a hyperelliptic curve is a topic for further research.

Bibliography

[1] L. Adleman and M.D. Huang. Counting points on curves and abelian varieties over finite fields. *J. Symbolic Comput.*, 32:171–189, 2001.

[2] H. Aslaksen. Quaternionic determinants. *Math. Intelligencer*, 18:57–65, 1996.

[3] J. Boxall and D. Grant. Examples of torsion points on genus two curves. *Proc. Amer. Math. Soc.*, 10:4533–4555, 2000.

[4] D.G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Math. Comp.*, 48:95–101, 1987.

[5] D.G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal für die Reine und Angewandte Mathematik*, 447:91–145, 1994.

[6] H. Cohen. *A course in Computational Algebraic Number Theory*. Springer-Verlag, New York, 1993.

[7] P. Deligne. Varietes abeliennes ordinaires sur un corps fini. *Invent. Math.*, 8:238–243, 1969.

[8] R.K. Dennis and B. Farb. *Noncommutative algebra*. Springer-Verlag, New York, 1993.

[9] N. Elkies. Explicit isogenies. *Harvard University, Cambridge*, Draft, 1991.

[10] K. Friedl and L. Ronyai. Polynomial time solution of some problems in computational algebra. *Proc. 17th Ann. ACM Symposium on Theory of Computing*, pages 153–162, 1985.

[11] P. Gaundry and E. Schost. Modular equations for hyperelliptic curves. *Math. Comp.*, 74:429–454, 2005.

[12] C. Greither. On the two generator problem for the ideals of an one dimensional ring. *J. Pure Appl. Algebra*, 24:265–276, 1982.

[13] M. Hindry and J.H. Silverman. *Diophantine geometry: An introduction*. Springer-Verlag, New York, 2000.

[14] T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, pages 83–95, 1967.

[15] E.W. Howe. Principally polarized ordinary abelian varieties over finite fields. *J. Math. Soc. Japan*, pages 83–95, 1967.

[16] E.W. Howe. Constructing distinct curves with isomorphic jacobians. *J. Number Theory*, 56:381–390, 1996.

[17] T.W. Hungerford. *Algebra*. Springer-Verlag, New York, 1980.

[18] K. Ireland and M.Rosen. *Classical Introduction Modern Number Theory*. Springer-Verlag, New York, 1992.

[19] G. Ivanyos and L. Ronyai. Finding maximal orders in semisimple algebras over the rationals. *Computational Complexity*, 3:246–261, 1993.

[20] H. Jacobinski. Two remarks about hereditary orders. *Proc. Amer. Math. Soc.*, 28:1–8, 1971.

[21] S. Johansson. On fundamental domains of arithmetic fuchsian groups. *Math. Comp.*, 74:339–349, 2000.

[22] N. Koblitz. *Algebraic Aspects of Cryptography: An elementary introduction to hyperelliptic curves)*. Springer-Verlag, New York, 1998.

[23] D. Kohel. Endomorphism rings of elliptic curves over finite fields. *University of California, Berkeley*, PhD Thesis, 1996.

[24] S. Lang. *Algebraic number theory, Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[25] S. Lang. *Elliptic functions*. Springer-Verlag, New York, 1987.

[26] L. Levy and R. Wiegand. Dedekind-like behaviour of rings with two generators. *J. Pure Appl. Algebra*, 37:41–58, 1985.

[27] J.S. Milne. Abelian varieties. *University of Michigan, Ann Arbor*, Lecture Notes for Math 731, 1991.

[28] O. O'Meara. *Introduction to quadratic forms*. Springer-Verlag, New York, 1973.

[29] I. Reiner. *Maximal Orders*. Academic Press, London, 1975.

[30] L. Ronyai. Algorithmic properties of maximal orders in simple algebras over the rationals. *Computational Complexity*, 2:225–243, 1992.

[31] J.P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88:492–517, 1968.

[32] J.H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1986.

[33] J.H. Silverman and G. Cornell. *Abelian varieties, Arithmetic Geometry*. Springer-Verlag, New York, 1986.

[34] B.K. Spearman and K.S. Williams. Relative integral bases for quartic fields over quadratic subfields. *Acta Math.*, 70:185–192, 1996.

[35] J. Swallow. Quadratic descent for quaternion algebras. *Comm. Algebra*, 29:4523–4544, 2002.

[36] J. Tate. Endomorphism rings of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[37] J. Velu. Isogenies entre courbes elliptiques. *Comptes Rendus Mathematique, Paris*, 273:238–241, 1971.

[38] M.F. Vigneras. *Arithmetique des Algebres de Quaternions*. Springer-Verlag, New York, 1980.

[39] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. of Math.*, 2:521–560, 1969.

[40] J. H. Weber. Hyperelliptic simple factors of $J_0(N)$ with dimension at least 3. *Experiment. Math.*, 6:273–287, 1994.

[41] H.J. Zhu. Supersingular abelian varieties. *J. Number Theory*, 86:61–77, 1983.