ABSTRACT

Title of dissertation: COMMUTATIVE ENDOMORPHISM RINGS OF SIMPLE ABELIAN VARIETIES OVER FINITE FIELDS

Jeremy Bradford, Doctor of Philosophy, 2012

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

In this thesis we look at simple abelian varieties defined over a finite field $k = \mathbb{F}_{p^n}$ with $\mathrm{End}_k(A)$ commutative. We derive a formula that connects the p-rank $r(A)$ with the splitting behavior of p in $E = \mathbb{Q}(\pi)$, where π is a root of the characteristic polynomial of the Frobenius endomorphism. We show how this formula can be used to explicitly list all possible splitting behaviors of p in $\mathcal{O}_E$, and we do so for abelian varieties of dimension less than or equal to four defined over $\mathbb{F}_p$. We then look for when p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. This allows us to prove that the endomorphism ring of an absolutely simple abelian surface is maximal at p when $p \geq 3$. We also derive a condition that guarantees that p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. Last, we explicitly describe the structure of some intermediate subrings of p-power index between $\mathbb{Z}[\pi, \bar{\pi}]$ and $\mathcal{O}_E$ when A is an abelian 3-fold with $r(A) = 1$.

COMMUTATIVE ENDOMORPHISM RINGS OF SIMPLE ABELIAN VARIETIES OVER FINITE FIELDS

by

Jeremy Bradford

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2012

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor Patrick Brosnan
Professor William Gasarch
Professor Niranjan Ramachandran
Professor Harry Tamvakis

Table of Contents

Chapter 1

Introduction

The driving force behind this thesis is the problem of computing the endomorphism ring $\mathrm{End}_k(A)$ of a given abelian variety A defined over a finite field k. Computing the endomorphism ring of A gives information about the isomorphism class of A within its isogeny class because isomorphic varieties must have isomorphic endomorphism rings. Computing endomorphism rings also has potential applications to cryptography. In hyperelliptic curve cryptography, one needs to construct a hyperelliptic curve over a finite field such that its Jacobian has a specified number of points. In the genus two case, Eisenträger and Lauter developed a method for constructing such curves by using the Chinese Remainder Theorem [1]. Their CRT method requires checking whether or not the endomorphism ring of a Jacobian of a genus 2 curve is the full ring of integers in a CM field. A follow-up paper by Freeman and Lauter gave a probabilistic algorithm for determining whether the endomorphism ring of a Jacobian is the full ring of integers [2]. A general algorithm for computing the endomorphism ring of an abelian variety over a finite would be a natural extension of their work.

David Kohel explored this problem in [3] when A is an ordinary elliptic curve by using the graph of l-isogenies between elliptic curves in the same isogeny class as A. He discovered that the graph of l-isogenies has the general shape of a volcano,

where the elliptic curves with maximal endomorphism ring form the rim at the top and the elliptic curves with minimal endomorphism ring form the base. Kohel was able to develop an algorithm that computed the endomorphism ring by exploiting the structure of this graph. This graph is often referred to as the "isogeny volcano" and it has found a number of applications beyond simply computing the endomorphism ring. For example, Sutherland was able to use isogeny volcanos to compute specializations of modular polynomials [4].

More recently Bisson and Sutherland have developed other algorithms for calculating the endomorphism ring of A when A is an ordinary elliptic curve [5]. Their algorithms search for relations in the ideal class group to compute the conductor of $\mathrm{End}_k(A)$. Thus the algorithms of Bisson and Sutherland, like Kohel's algorithm, rely on the fact that $\mathrm{End}_k(A)$ is some order in the quadratic imaginary field $\mathbb{Q}\otimes\mathrm{End}_k(A)$. Orders in quadratic imaginary fields are completely determined by their conductor, or equivalently, by their index in the ring of integers. The algorithms of Kohel, Bisson, and Sutherland calculate this index and thus determine $\mathrm{End}_k(A)$.

For higher dimensional abelian varieties, we will restrict ourselves to the case where $\mathbb{Q}\otimes\mathrm{End}_k(A)$ is a field. In general, the index of $\mathrm{End}_k(A)$ in the ring of integers does not necessarily determine the order $\mathrm{End}_k(A)$. This means that an algorithm that computes the index of $\mathrm{End}_k(A)$ in the ring of integers will not be sufficient to pin down the endomorphism ring of A, a difficulty not encountered in the case of ordinary elliptic curves. We do not resolve this difficulty in this thesis but rather attempt to narrow down the possible orders that $\mathrm{End}_k(A)$ can be inside the ring of integers. It is known [6, 3.5] that $\mathrm{End}_k(A)$ must contain $\mathbb{Z}[\pi, \bar{\pi}]$ and so we will

focus on the index of $\mathbb{Z}[\pi, \bar{\pi}]$ in the ring of integers. Specifically we will look at the question of the maximality or non-maximality of $\mathbb{Z}[\pi, \bar{\pi}]$ at p.

We will show that the maximality or non-maximality of $\mathbb{Z}[\pi, \bar{\pi}]$ at p is connected with the p-rank of the abelian variety and the splitting behavior of p in the CM field $\mathbb{Q} \otimes \mathrm{End}_k(A)$. We prove a theorem that completely describes the relationship between the splitting behavior of p and the p-rank and then use this theorem to work out all possible splitting behaviors in the cases of abelian varieties defined over $\mathbb{F}_p$ up to dimension four. We also note that recent work of Zaytsev has significant overlap with this portion of the thesis. Zaytsev has been looking at the more general question of the isomorphism type of $A[p]$ as a finite group scheme. He is able to connect the splitting behavior of p in E with the first truncated Barsotti-Tate group scheme $A[p]$ for abelian varieties up to dimension three [7].

We use the classification of the possible splitting behaviors of p to examine when p divides the index $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. If A is an absolutely simple abelian surface, then we prove that p does not divide this index for $p \geq 17$. This allows us to prove that $\mathrm{End}_k(A)$ is maximal at p for $p \geq 3$. For higher dimensional abelian varieties, we find sufficient conditions on the p-rank and the splitting behavior of p to guarantee that $\mathbb{Z}[\pi, \bar{\pi}]$ is non-maximal at p.

We also briefly explore the problem of explicitly describing intermediate rings R between $\mathbb{Z}[\pi, \bar{\pi}]$ and the maximal order such that $[R : \mathbb{Z}[\pi, \bar{\pi}]]$ is divisible by p. It is not completely clear which of these intermediate rings can arise as the endomorphism ring of an abelian variety. Waterhouse and Nakamura have provided some results that guarantee the maximality of the endomorphism ring at p under certain

hypotheses [6, 5.3], [8]. However, they both make the rather strong assumption that $\mathrm{End}_k(A)$ contains the maximal order of the totally real subfield of index two. If a general algorithm for computing the endomorphism ring of an abelian variety over a finite field is to be developed, then it seems that we need to know more about the possible intermediate subrings. In this thesis we give the explicit structure of some intermediate subrings for abelian 3-folds with p-rank $r(A) = 1$. Under a certain hypothesis relating the coefficients of the characteristic polynomial of Frobenius, we show that there is always an intermediate subring with index p. Using numerical evidence, we also conjecture that this intermediate subring is unique.

Chapter 2

Background

The goals of this background chapter are (1) to introduce the notation used throughout the thesis, and (2) state definitions and results with the aim of making this thesis reasonably self-contained. We also hope that this background section will be illuminating by clearly showing how the the new results that we prove fit into the growing body of theory on endomorphism rings of abelian varieties over finite fields. Throughout this chapter, known results are stated without proof but citations are always provided.

2.1 Abelian Varieties

We begin with a short review of the theory of abelian varieties over finite fields (see [9] for a general reference). Let A be an abelian variety of dimension g defined over the finite field $k := \mathbb{F}_q$ where $q = p^n$. We will often assume that A is *absolutely simple*, which just means that A is simple and when we extend scalars to the algebraic closure $\bar{k}$ we have that $A \times_k \bar{k}$ is also simple. If k' is an extension of k contained in $\bar{k}$, then $A(k')$ denotes the set of points on A with coordinates in k'.

Since A is an abelian variety there is an addition morphism $A \times A \to A$ defined over k that makes $A(k')$ into an abelian group for every extension k' of k. For any positive integer m, $A(k')[m]$ will denote the m-torsion elements of the abelian group

$A(k')$. If $m \in \mathbb{N}$ is relatively prime to p, then $A(\bar{k})[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$. Thus for any prime $l \neq p$ we have $A(\bar{k})[l^d] \simeq (\mathbb{Z}/l^d\mathbb{Z})^{2g}$. Multiplication by l induces a map $A(\bar{k})[l^d] \to A(\bar{k})[l^{d-1}]$. The *Tate Module* is the inverse limit $T_l(A) := \varprojlim A(\bar{k})[l^d]$. $T_l(A)$ is therefore a free $\mathbb{Z}_l$-module of rank $2g$. On the other hand, $A(\bar{k})[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{r(A)}$ for some $0 \leq r(A) \leq g$. The integer $r(A)$ is the *p-rank* of A. Every integer from 0 to g arises as the p-rank of some abelian variety over k of dimension g. If $r(A) = g$ then A is said to be *ordinary*.

A *morphism of abelian varieties* $\varphi : A_1 \to A_2$ is a morphism of varieties which is defined over k and is also compatible with the addition maps of A_1 and A_2. In particular $\varphi : A_1(k') \to A_2(k')$ is a homomorphism of groups. If $\dim(A_1) = \dim(A_2)$, then an *isogeny* $\varphi : A_1 \to A_2$ is a morphism of abelian varieties with finite kernel. An *endomorphism of* A is a morphism of abelian varieties from A to A. For example, for every integer $m > 0$ there is a multiplication-by-m endomorphism $[m] : A \to A$ which takes a point $P \in A(\bar{k})$ to $[m](P) := P+P+\cdots+P$, the m-fold sum. Another example is the map $[-1](P) := -P$ which sends P to its additive inverse. Composing these two endomorphisms allows us to treat the integers $\mathbb{Z}$ as endomorphisms of A. Since A is defined over the finite field $k = \mathbb{F}_q$, there is also a distinguished endomorphism $F : A \to A$ induced by the q-th power Frobenius automorphism of the field $\bar{k}$. We call F the *Frobenius endomorphism* of A. It is known that an endomorphism φ of A defined over $\bar{k}$ is actually defined over k if and only if $F\varphi = \varphi F$. We denote the set of endomorphism of A defined over k by $\mathrm{End}_k(A)$. Under composition and point-wise addition, $\mathrm{End}_k(A)$ becomes a ring which we call the *endomorphism ring* of A.

If $l \neq p$ is a prime, then F induces a linear transformation on the Tate module $T_l(A)$. One way to define the characteristic polynomial of F is to take the characteristic polynomial of the linear transformation that F induces on $T_l(A)$. However, it is then far from clear that this is a polynomial with integer coefficients independent of the prime l. Thus we will instead use an alternative definition of the characteristic polynomial due to Weil. In order to describe this alternative, we need to give some more definitions.

For an abelian variety A over k, the *function field* $k(A)$ is the field of rational functions from A to $\mathbb{P}_1(k)$. Let $\alpha : A_1 \to A_2$ be a morphism of abelian varieties and let $\psi \in k(A_2)$. Then we can define $\alpha^*(\psi) := \psi \circ \alpha \in k(A_1)$. Thus $\alpha^* : k(A_2) \hookrightarrow k(A_1)$ allows us to identify $k(A_2)$ with a subfield of $k(A_1)$. If $\alpha \neq 0$ and $[k(A_1) : \alpha^* k(A_2)]$ is finite, then the *degree* of α is $[k(A_1) : \alpha^* k(A_2)]$. By convention, we define the degree of the zero morphism to be 0. For example, $\deg[n] = n^{2g}$ and $\deg F = q$ (see [9] I.7.2 and II.1.2). To define the characteristic polynomial of an endomorphism we use the following theorem:

Theorem 2.1 ([9] Theorem I.10.9)**.** *Let $\alpha \in \mathrm{End}_k(A)$. There is a unique monic polynomial $P_\alpha \in \mathbb{Z}[x]$ of degree $2g$ such that $P_\alpha(r) = \deg(\alpha - r)$ for all $r \in \mathbb{Z}$.*

The *characteristic polynomial* of the endomorphism α is the monic polynomial $P_\alpha \in \mathbb{Z}[x]$. In this thesis we let $f \in \mathbb{Z}[x]$ be the characteristic polynomial of the Frobenius endomorphism F. We will often assume that f is irreducible. In such cases we will identify a root π of f with the Frobenius endomorphism F and then by abuse of language will call the root π the Frobenius endomorphism.

For any isogeny $\alpha : A \to B$ there is an isogeny $\bar{\alpha} : B \to A$ called the *dual isogeny* such that $\bar{\alpha}\alpha = [\deg \alpha]_A$ and $\alpha\bar{\alpha} = [\deg \alpha]_B$. Thus the relation "$A$ is isogenous to B" is an equivalence relation on abelian varieties over k. The *isogeny class of* A is the set of abelian varieties over k that are isogenous to A. Tate discovered a remarkable connection between the characteristic polynomial f of the Frobenius endomorphism and the isogeny class of the abelian variety:

Theorem 2.2 ([10] Theorem 1)**.** *Let A and B be abelian varieties over a finite field k, and let f_A and f_B be the characteristic polynomials of their Frobenius endomorphisms relative to k. Then*

(b) The following are equivalent:

(b1) B is k-isogenous to an abelian subvariety of A defined over k.

(b3) f_B divides f_A.

(c) The following are equivalent:

(c1) A and B are k-isogenous.

(c2) $f_A = f_B$.

(c4) $|A(k')| = |B(k')|$ for every finite extension k' of k.

Remark 2.3. To keep this introductory section brief we have only stated some of the parts of the original theorem in [10] but have enumerated these selections using the original enumeration given in [10].

For the sake of completeness of this introduction we include the following well-known theorem:

Theorem 2.4 ([9] Theorem II.1.1)**.** *Let A be an abelian variety over the finite field k, let f be the characteristic polynomial of the Frobenius endomorphism, and let k_m be the field extension of k of degree m. Write $f(x) = \prod_{i=1}^{2g}(x - a_i)$ for $a_i \in \mathbb{C}$. Then*

(a) $\#A(k_m) = \prod_{i=1}^{2g}(1 - a_i^m)$ for all $m \geq 1$, and

(b) (Riemann hypothesis) $|a_i| = q^{\frac{1}{2}}$.

A *Weil q-number* is a complex number $\pi \in \mathbb{C}$ such that if $\varphi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ is an embedding of fields, then $|\varphi(\pi)| = q^{\frac{1}{2}}$. A *Weil polynomial* is a polynomial in $\mathbb{Z}[x]$ whose roots are all Weil q-numbers. Two Weil q-numbers π_1 and π_2 are considered equivalent if they have the same minimal polynomial, or equivalently if there is an isomorphism $\varphi : \mathbb{Q}(\pi_1) \xrightarrow{\sim} \mathbb{Q}(\pi_2)$ such that $\varphi(\pi_1) = \pi_2$. By the Riemann hypothesis, the characteristic polynomial of Frobenius is a Weil polynomial. The converse is also true, due to Tate and Honda:

Theorem 2.5 ([11] Theorem 1)**.** *There is a bijection between the set of isogeny classes of simple abelian varieties over k and the equivalence classes of Weil q-numbers. The bijection is given by associating to a simple abelian variety A over k a root of the characteristic polynomial of Frobenius.*

2.2 Endomorphism Rings

We begin by stating some fundamental results in the theory of endomorphism rings of abelian varieties.

Theorem 2.6 ([9] I.10.6, I.10.15)**.** *For abelian varieties A and B over k, the set*

$\mathrm{Hom}_k(A, B)$ *of morphisms of abelian varieties from* A *to* B *is a finitely generated torsion-free* $\mathbb{Z}$*-module with rank at most* $4\dim(A)\dim(B)$*. In particular* $\mathrm{End}_k(A)$ *is a finitely generated torsion-free* $\mathbb{Z}$*-module with rank at most* $4\dim(A)^2$*.*

Theorem 2.7 ([10] Theorem 2)**.** *Let* A *be an abelian variety of dimension* g *over a finite field* k*. Let* F *be the Frobenius endomorphism of* A *relative to* k *and* f *its characteristic polynomial.*

(a) The algebra $E := \mathbb{Q}[F]$ *is the center of the semisimple algebra* $S = \mathbb{Q} \otimes \mathrm{End}_k(A)$*.*

(b) We have

$$2g \leq [S : \mathbb{Q}] \leq (2g)^2$$

(c) The following are equivalent:

(c1) $[S : \mathbb{Q}] = 2g$*.*

(c2) f *has no multiple root.*

(c3) $S = E$*.*

(c4) S *is commutative.*

(d) The following are equivalent:

(d1) $[S : \mathbb{Q}] = (2g)^2$*.*

(d2) f *is a power of a linear polynomial.*

(d3) $E = \mathbb{Q}$*.*

(d4) S is isomorphic to the algebra of g by g matrices over the quaternion algebra D_p over $\mathbb{Q}$ which is ramified only at p and ∞.

(d5) A is k-isogenous to the g-th power of a supersingular elliptic curve, all of whose endomorphisms are defined over k.

(e) A is k-isogenous to a power of a k-simple abelian variety if and only if f is a power of a $\mathbb{Q}$-irreducible polynomial P. When this is the case S is a central simple algebra over E which splits at all finite primes v of E not dividing $p = \mathrm{char}(k)$, but does not split at any real prime of E.

We will usually be dealing with simple abelian varieties. In these cases Theorem 2.7(e) will apply and thus $f = h^e$ for some irreducible polynomial $h \in \mathbb{Z}[x]$. The polynomial h will be a Weil polynomial (Theorem 2.4) with root π. Furthermore, $[S : E] = e^2$ (see [11, p.142] and also [12, Ch. IV]) hence the endomorphism ring of a simple abelian variety is commutative if and only if $e = 1$.

Theorem 2.5 says that a root π of a Weil polynomial h determines an isogeny class of simple abelian varieties. But isogenous abelian varieties have isomorphic endomorphism rings after tensoring with $\mathbb{Q}$, so we would like to be able to determine this ring S from the given root π. We do this by first calculating the local invariants of the central simple algebra S over the field $E = \mathbb{Q}(\pi)$. Theorem 2.7(e) states that we get a local invariant of $\frac{1}{2}$ at every real place of E and that S splits at every finite prime other than those that lie over p. If v is a place of E over p, then Tate proved ([11, Thm. 1])

$$\mathrm{inv}_v(S) \equiv \frac{v(\pi)}{v(q)}[E_v : \mathbb{Q}_p] = v(\pi)\frac{f_v}{n} \pmod 1 \tag{2.1}$$

where f_v is the degree of the residue field at v. The exponent e is the least common multiple of the denominators of the local invariants of the central simple algebra S. Since we are assuming that our abelian varieties are simple, every nonzero endomorphism of A is an isogeny. Recall that every isogeny α has a dual $\bar{\alpha} \in \mathrm{End}_k(A)$ such that $\alpha\bar{\alpha} = [\deg \alpha] \in \mathbb{Z}$. Thus when we formally extend scalars to form $S = \mathbb{Q} \otimes \mathrm{End}_k(A)$ we see that any nonzero endomorphism α has inverse $[\deg \alpha]^{-1} \otimes \bar{\alpha}$. Thus we get that S is a central division algebra over E. This means that the local invariants uniquely determine S ([12] VIII.4.2), hence we have recovered S from π.

We now sketch the structure of Weil q-numbers as described in detail in [6, Ch. 2]. First suppose that there is a real prime of E. Then $\pi = \pm\sqrt{q}$. If n is even then $\pi \in \mathbb{Z}$, $E = \mathbb{Q}$, S is the quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞, and A is a supersingular elliptic curve with all endomorphisms defined over k. If n is odd then $E = \mathbb{Q}(\sqrt{p})$, S is the quaternion algebra over $\mathbb{Q}(\sqrt{p})$ ramified only at the two infinite places, and A is a simple abelian surface. If E does not have a real prime, then let $\beta = \pi + \bar{\pi} = \pi + \frac{q}{\pi}$. Then $K = \mathbb{Q}(\beta)$ is a totally real subfield and π satisfies $X^2 - \beta X + q$, hence E is a quadratic imaginary extension of K. That is, E is a CM field with totally real subfield $K = \mathbb{Q}(\pi + q/\pi)$. In this thesis we will deal with this latter case almost exclusively.

2.3 Subrings of $\mathbb{Q} \otimes \mathrm{End}_k(A)$

This section will be dealing with the question of which subrings of $\mathbb{Q} \otimes \mathrm{End}_k(A)$ arise as endomorphism rings of abelian varieties. We will always assume that A is

simple. We do not yet require that $\mathrm{End}_k(A)$ be commutative. Thus $\mathbb{Q} \otimes \mathrm{End}_k(A)$ will be a central division algebra over $E = \mathbb{Q}(\pi)$, and $\mathrm{End}_k(A)$ is commutative if and only if $E = \mathbb{Q} \otimes \mathrm{End}_k(A)$.

2.3.1 Elliptic Curves

When dealing with an elliptic curve C we know that $\pi \in \mathrm{End}_k(C)$. Furthermore the characteristic polynomial of Frobenius is $X^2 - \beta X + q$ and $\beta = p + 1 - \#E(k)$, hence $\beta \in \mathbb{Z}$. In particular, $\bar{\pi} = \beta - \pi \in \mathbb{Z}[\pi]$. Therefore any subring of $\mathbb{Q} \otimes \mathrm{End}_k(C)$ that arises as the endomorphism ring of an elliptic curve contains at a minimum $\mathbb{Z}[\pi] = \mathbb{Z}[\pi, \bar{\pi}]$. Waterhouse fully analyzed which subrings between $\mathbb{Z}[\pi]$ and $\mathbb{Q} \otimes \mathrm{End}_k(C)$ arise as the endomorphism rings of elliptic curves:

Theorem 2.8 ([6] 4.2)**.** *Let S be the endomorphism algebra of an isogeny class of elliptic curves. The orders in S which are endomorphism rings of curves in the isogeny class are as follows:*

(a) If the curves are supersingular with all endomorphisms defined over k, the maximal orders.

(b) If the curves are not supersingular, all orders containing $\mathbb{Z}[\pi]$.

(c) If the curves are supersingular with not all endomorphisms defined over k, the orders which contain $\mathbb{Z}[\pi]$ and are maximal at p.

2.3.2 The Theorems of Waterhouse and Nakamura

Now let A be a simple abelian variety of dimension $g > 1$ with commutative endomorphism ring. By Theorem 2.7(c) we have that $E = \mathbb{Q}(\pi) = \mathbb{Q} \otimes \mathrm{End}_k(A)$. It is still true that $\bar{\pi} \in \mathrm{End}_k(A)$, but in general $\beta = \pi + \bar{\pi}$ will not be an integer. As a consequence, we should expect $\mathbb{Z}[\pi, \bar{\pi}]$ to strictly contain $\mathbb{Z}[\pi]$. This means that $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathrm{End}_k(A)$ will have to serve as our lower bound for possible endomorphism rings instead of the simpler ring $\mathbb{Z}[\pi]$. The task now is to analyze which subrings between $\mathbb{Z}[\pi, \bar{\pi}]$ and the ring of integers $\mathcal{O}_E$ may be the endomorphism ring of A.

One way to begin is to choose a prime $l \neq p$ and then localize to get $R_l := \mathbb{Z}_l \otimes R$ contained in $E_l := \mathbb{Q}_l \otimes E$. In the proof of Theorem 2.8, Waterhouse found the following result:

Porism 2.9 ([6] 4.3)**.** *Let E be the endomorphism algebra of an isogeny class of simple abelian varieties and assume E is commutative. Let R be any order in E containing $\mathbb{Z}[\pi, \bar{\pi}]$. Then there is a variety A in the isogeny class with $\mathrm{End}_k(A)_l = R_l$ for all primes $l \neq p$.*

This just leaves us to deal with subrings between $\mathbb{Z}[\pi, \bar{\pi}]$ and $\mathcal{O}_E$ whose index in $\mathcal{O}_E$ is divisible by p. By analyzing invariant sublattices of the Dieudonné module $T_p(A)$ and their corresponding orders, Waterhouse was able to prove the following theorem:

Theorem 2.10 ([6] 5.3)**.** *Let A be a simple variety with E commutative. Let K be the totally real subfield of index 2 in E, and assume that p splits completely in K. Assume also that $R = \mathrm{End}_k(A) \subseteq \mathcal{O}_E$ contains the ring of integers $\mathcal{O}_K$ of K. Then*

R is maximal at p.

This result was strengthened in a follow-up paper by Nakamura [8, Thm. 1]. Nakamura's theorem also assumes that $\mathrm{End}_k(A)$ contains $\mathcal{O}_K$, but he weakens the hypothesis that p splits completely in K. The hypothesis that he assumes in its place is a bit technical and so we do not reproduce the theorem here but instead refer the interested reader to the original article [8].

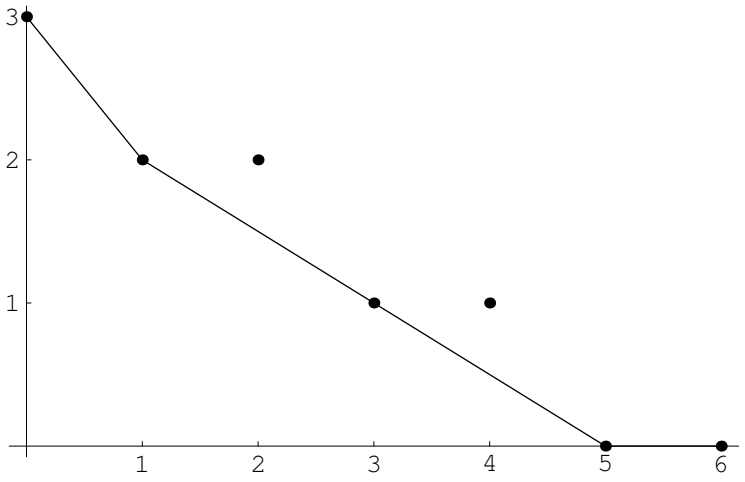
2.4 Newton Polygons

2.4.1 Definitions and Properties

Let $h(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Let l be a prime and consider the set $S_h := \{(0, \mathrm{ord}_l\, a_0), (1, \mathrm{ord}_l\, a_1), \ldots, (d-1, \mathrm{ord}_l\, a_{d-1}), (d, 0)\}$ of points in the plane. The *Newton Polygon* $\mathrm{Np}_l(h)$ is the lower convex hull of the points in S_h. That is, $\mathrm{Np}_l(h)$ is the highest convex sequence of connected line segments connecting $(0, \mathrm{ord}_l\, a_0)$ to $(d, 0)$ such that all the points in S_h lie on or above this sequence of line segments. $\mathrm{Np}_l(h)$ may be constructed as follows: start with a vertical line ℓ drawn through $(0, \mathrm{ord}_l\, a_0)$ and rotate ℓ about this point counterclockwise until ℓ touches another point in S_h. In fact, ℓ may now touch several points in S_h, so we draw the line segment joining $(0, \mathrm{ord}_l\, a_0)$ to the last such point $(i_1, \mathrm{ord}_l\, a_{i_1})$ in S_h that ℓ currently touches. This line segment is the first segment of $\mathrm{Np}_l(h)$. Next we rotate ℓ further about $(i_1, \mathrm{ord}_l\, a_{i_1})$ until ℓ hits a further point in S_h. As before, ℓ may be touching more than one point in S_h, so we draw the segment joining $(i_1, \mathrm{ord}_l\, a_{i_1})$ to the last such point $(i_2, \mathrm{ord}_l\, a_{i_2})$ in S_h that ℓ currently touches. This line segment is

the second segment of $\mathrm{Np}_l(h)$. We repeat this process of rotating ℓ about the point $(i_j, \mathrm{ord}_l\, a_{i_j})$ counterclockwise until we hit another point in S_h and then drawing a line segment from $(i_j, \mathrm{ord}_l\, a_{i_j})$ to the furthest point $(i_{j+1}, \mathrm{ord}_l\, a_{i_{j+1}})$ that ℓ currently touches to get the next line segment of $\mathrm{Np}_l(h)$.

For example, let $f(x) = x^6 + 3x^5 + 5x^4 + 5x^3 + 25x^2 + 75x + 125$. Then the Newton polygon $\mathrm{Np}_5(f)$ is



We have the following standard result:

Lemma 2.11 ([13], IV Lemma 4)**.** *Let F be the splitting field of h in $\mathbb{C}$ and let $\mathfrak{L}$ be a prime of $\mathcal{O}_F$ lying over l. Let $h(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_d)$ be the factorization of h in F. Let v be the extension of* ord_l *to F induced by the prime $\mathfrak{L}$ and let $\lambda_i = -v(\alpha_i)$. If λ is the slope of a segment of* $\mathrm{Np}_l(h)$ *having horizontal length m, then precisely m of the λ_i are equal to λ.*

When the characteristic polynomial of Frobenius f is irreducible, we have designated π to be some chosen root of f. When we need to enumerate the complete set of roots of f in $\mathbb{C}$ we will use both $\{\alpha_1, \ldots, \alpha_{2g}\}$ and $\{\pi_1, \bar{\pi}_1, \ldots, \pi_g, \bar{\pi}_g\}$. We

then let $\beta_i := \pi_i + \bar{\pi}_i$ and likewise $\beta := \pi + \bar{\pi}$. Thus β_i and β are totally real and $K = \mathbb{Q}(\beta)$. We let E' be the splitting field of f in $\mathbb{C}$ and let K' be $\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_g)$, the Galois closure of K in $\mathbb{C}$. With this notation we have:

Theorem 2.12 ([14] Proposition 3.1)**.**

(a) $r(A)$ *is the sum of the multiplicities of the non-zero roots of the* (*mod* p)*-reduced characteristic polynomial* f *.*

(b) $r(A) = \#\{\alpha_i \notin \mathscr{P} | 1 \leq i \leq 2g\}$ *where* $\mathscr{P}$ *is a prime ideal over* p *in the ring of integers of* E'*.*

(c) $r(A) = \#\{\beta_i \notin \mathscr{P} | 1 \leq i \leq g\}$ *where* $\mathscr{P}$ *is a prime ideal over* p *in the ring of integers of* K'*.*

Putting these last two results together easily yields:

Corollary 2.13. $r(A)$ *is the length of the zero-slope segment of* $\mathrm{Np}_p(f)$*.*

We next state a result which will be expanded into a more general theorem in this thesis:

Theorem 2.14 ([14] Proposition 3.2)**.** *Let* $A/\mathbb{F}_q$ *be an* $\mathbb{F}_q$*-simple abelian variety. Then:*

(a) A is ordinary (i.e. $r(A) = g$*) if and only if the ideals* (π) *and* $(\bar{\pi})$ *(equivalently the ideals* $(\pi + \bar{\pi})$*,* (p)*) are relatively prime in* E*.*

(b) $r(A) = 0$ *if and only if every prime* $\mathscr{P}|(p)$ *divides* (π) *in* E *(equivalently, divides* $(\pi + \bar{\pi})$*).*

(c) A is $\bar{k}$-isogenous to a power of a supersingular elliptic curve if and only if $(\pi) = (\bar{\pi})$.

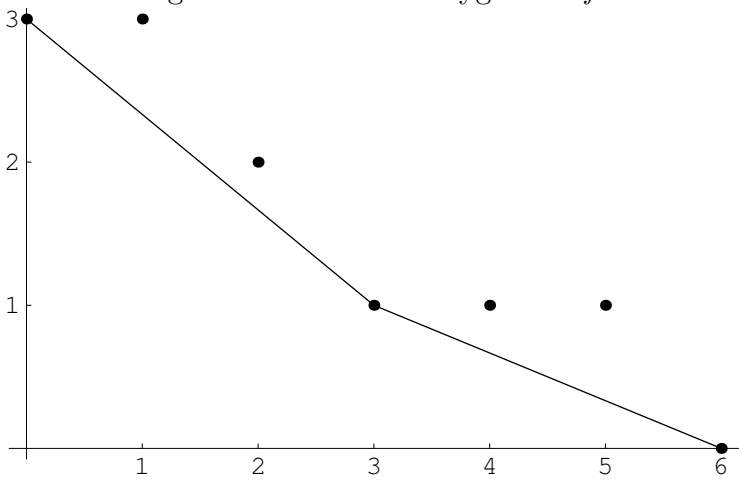
If A is an abelian variety and f the characteristic polynomial of Frobenius, then A is *supersingular* if $\mathrm{Np}_p(f)$ is just a single line segment. An abelian variety is supersingular if and only if $A \times_k \bar{k}$ falls under case (d5) of Theorem 2.7 over $\bar{k}$ [15, 4.2]. If A is an elliptic curve or abelian surface, then supersingular is equivalent to $r(A) = 0$. When $q = p$, this can be seen by examining the possible Newton polygons. The characteristic polynomial of Frobenius f is a Weil polynomial, and thus it must be of the form $f(x) = x^2 + a_1 x + p$ if A is an elliptic curve or $f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_1 p x + p^2$ if A is an abelian surface (see Section 2.5). It is then easy to see that, if $\mathrm{Np}_p(f)$ has a vertex, then it also has a zero-slope segment. However, when $g \geq 3$, such Newton Polygons are possible. For example consider the Weil polynomial $f(x) = x^6 - 5x^5 + 15x^4 - 35x^3 + 75x^2 - 125x + 125$ for $p = 5$. We see that $\mathrm{Np}_5(f)$ has no zero-slope segment, yet it is not a single line segment because of the vertex at $(3, 1)$. Thus for $g \geq 3$, supersingular is not equivalent to $r(A) = 0$.

2.4.2 Newton Polygons and Local Invariants

The Newton polygon can be helpful when calculating the local invariants. Let f be an irreducible Weil polynomial, π a root of f, and $E = \mathbb{Q}(\pi)$. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_E$ over p, and let $v_\mathfrak{p}$ be the corresponding valuation. Recall from equation (2.1) that the local invariant $i_\mathfrak{p}$ is given by

$$i_\mathfrak{p} \equiv \frac{v_\mathfrak{p}(\pi)}{v_\mathfrak{p}(q)} [E_\mathfrak{p} : \mathbb{Q}_p] \pmod 1$$

Figure 2.1: Newton Polygon for f



This formula can be rewritten if we introduce some new notation. Let $\overline{\mathbb{Q}}_p$ be a fixed algebraic closure of $\mathbb{Q}_p$ and let $\alpha_1, \ldots, \alpha_{2g}$ be the roots of f in $\overline{\mathbb{Q}}_p$. Each completed field $E_\mathfrak{p}$ can be embedded into $\overline{\mathbb{Q}}_p$ in $d_\mathfrak{p} := [E_\mathfrak{p} : \mathbb{Q}_p]$ different ways because $E_\mathfrak{p}$ is separable over $\mathbb{Q}_p$. Each embedding of $E_\mathfrak{p}$ into $\overline{\mathbb{Q}}_p$ sends π to one of the roots α_i of f. It is known that the valuation v_p on $\mathbb{Q}_p$ extends uniquely to a valuation on $\overline{\mathbb{Q}}_p$. If $\varphi_i : E_\mathfrak{p} \hookrightarrow \overline{\mathbb{Q}}_p$ is an embedding, then we take $v_\mathfrak{p}$ to be normalized so that it agrees with the pullback of v_p via φ_i. That is, for all $x \in E_\mathfrak{p}$, we have that

$$v_\mathfrak{p}(x) = v_p(\varphi_i(x)).$$

In particular we have that $v_\mathfrak{p}(\pi) = v_p(\varphi_i(\pi))$.

If $\alpha_{i_1}, \ldots, \alpha_{i_{d_\mathfrak{p}}}$ are all the images of π under all embeddings of $E_\mathfrak{p}$, then we may define

$$f_\mathfrak{p}(x) := \prod_{j=1}^{d_\mathfrak{p}} (x - \alpha_{i_j}).$$

Each $f_\mathfrak{p}$ corresponds to a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugacy class of roots of f [16, Thm. II.2], $f_\mathfrak{p}$ is irreducible in $\mathbb{Z}_p[x]$, and $f = \prod f_\mathfrak{p}$. Let $\pi_\mathfrak{p}$ be a representative of the Galois

conjugacy class of roots of $f_{\mathfrak{p}}$. All the roots of $f_{\mathfrak{p}}$ have the same p-adic valuation, hence

$$i_{\mathfrak{p}} \equiv \frac{v_{\mathfrak{p}}(\pi)}{v_{\mathfrak{p}}(q)}[E_{\mathfrak{p}} : \mathbb{Q}_p] = \frac{v_p(\pi_{\mathfrak{p}})d_{\mathfrak{p}}}{v_p(q)} = \frac{v_p(f_{\mathfrak{p}}(0))}{n} \pmod 1 \tag{2.2}$$

In this new equation, we get that $i_{\mathfrak{p}} \equiv \frac{v_p(\pi_{\mathfrak{p}})d_{\mathfrak{p}}}{n} \pmod 1$. We can now see clearly the connection with Newton polygons. The negatives of the slopes of the segments of the Newton polygon will correspond to the numbers $v_p(\pi_{\mathfrak{p}})$ in the numerators of the local invariants. For example, consider the irreducible Weil polynomial $f(x) = x^2 + px + p^4$. This polynomial has no real roots, hence the only non-integer local invariants must come from primes over p. The Newton polygon $\mathrm{Np}_p(f)$ has two segments with slopes -3 and -1. These two segments each have horizontal length one, so therefore $f = (x - \alpha_1)(x - \alpha_2)$ where $x - \alpha_1$ and $x - \alpha_2$ are the irreducible factors of f in $\mathbb{Z}_p[x]$. In particular, we get two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ over p. Without loss of generality we may assume that $f_{\mathfrak{p}_1}(x) = x - \alpha_1$, $f_{\mathfrak{p}_2}(x) = x - \alpha_2$, $v_p(\alpha_1) = 3$, and $v_p(\alpha_2) = 1$. Applying equation (2.2) we get that $i_{\mathfrak{p}_1} = \frac{3}{4}$ and $i_{\mathfrak{p}_2} = \frac{1}{4}$. The least common multiple of the denominators of the local invariants is 4, hence the polynomial $(x^2+px+p^4)^4$ is the characteristic polynomial of a simple abelian variety of dimension 4 defined over $\mathbb{F}_{p^4}$ with non-commutative endomorphism ring.

2.5 Classification of Weil polynomials

Weil polynomials corresponding to the characteristic polynomial of Frobenius of a simple abelian variety A have been classified when A is an elliptic curve, an abelian surface, or an abelian 3- or 4-fold. Classification of Weil polynomials is usually a two-

step process. The first step is determining the Weil polynomials of a given degree. Such a polynomial h then has an exponent e which is completely determined by h (see Section 2.2). The second step is to find conditions on the coefficients of h that cause e to have the property that $\deg h^e = 2g$, where g is the dimension of the class of abelian varieties under investigation (in our case $g = 1, 2, 3$ or 4). The resulting polynomial h will then have the property that h^e is the characteristic polynomial of Frobenius for an isogeny class of simple abelian varieties of dimension g. In this thesis we will only be dealing with the case where $\mathrm{End}_k(A)$ is commutative, which corresponds to $e = 1$.

A preliminary observation to the classification of Weil polynomials is to recall Theorem 2.4, which says that the characteristic polynomial of Frobenius f is always a Weil polynomial. In particular, if f has no real root, then over the real numbers we get a factorization

$$f(x) = \prod_{i=1}^{g} (x^2 - \beta_i x + q).$$

If we expand this product, we see that the coefficients of f have a symmetry. In particular, we get that f is of the form

$$f(x) = x^{2g} + a_1 x^{2g-1} + a_2 x^{2g-2} + \cdots + a_g x^g + a_{g-1} q x^{g-1} + a_{g-2} q^2 x^{g-2} + \cdots + q^g.$$

2.5.1 Elliptic Curves

The classification of Weil polynomials corresponding to elliptic curves is due to Waterhouse:

Theorem 2.15 ([6] 4.1)**.** *Let $k = \mathbb{F}_q$ where $q = p^n$. The isogeny classes of ellip-*

tic curves defined over k are in one-to-one correspondence with rational integers β having $|\beta| \leq 2\sqrt{q}$ and satisfying one of the following conditions:

(a) $(\beta, p) = 1$*;*

(b) If n *is even :* $\beta = \pm 2\sqrt{q}$*;*

(c) If n *is even and* $p \not\equiv 1 \pmod 3$ *:* $\beta = \pm\sqrt{q}$*;*

(d) If n *is odd and* $p = 2$ *or* 3 *:* $\beta = \pm p^{\frac{n+1}{2}}$*;*

(e) If either (i) n *is odd or (ii)* n *is even and* $p \not\equiv 1 \pmod 4$ *:* $\beta = 0$*;*

The first of these are not supersingular; the second are supersingular and have all their endomorphisms defined over k; the rest are supersingular but do not have all their endomorphisms defined over k.

Remark 2.16. The corresponding characteristic polynomial of Frobenius is always $h^e = x^2 - \beta x + q$. Cases (a) and (c)-(e) have h irreducible and $e = 1$ while in case (b) we get $h(x) = x \pm \sqrt{q}$ and $e = 2$. The condition $|\beta| \leq 2\sqrt{q}$ ensures that h is a Weil polynomial while the conditions (a) and (c)-(e) ensure that the local invariants determined by h yield $e = 1$.

2.5.2 Abelian Surfaces

The classification of Weil polynomials of abelian surfaces is primarily due to Rück. He proved the following theorem:

Theorem 2.17 ([17] 1.1)**.** *The set of irreducible Weil polynomials $f(X)$ of degree four that correspond to simple abelian surfaces is the set of polynomials $f(X) =$*

$X^4 + a_1X^3 + a_2X^2 + a_1qX + q^2$ *where the integers* a_1 *and* a_2 *satisfy the following conditions:*

(a) $|a_1| < 4\sqrt{q}$ *and* $2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q$,

(b) $a_1^2 - 4a_2 + 8q$ *is not a square in* $\mathbb{Z}$,

(c) one of the following conditions is satisfied:

(i) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$ *and* $(a_2 + 2q)^2 - 4qa_1^2$ *is not a square in* $\mathbb{Z}_p$.

(ii) $v_p(a_2) = 0$.

(iii) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$ *and* $h(X)$ *has no root in* $\mathbb{Z}_p$.

Remark 2.18. Condition (a) ensures that f is a Weil polynomial, condition (b) makes f irreducible, and condition (c) ensures that $e = 1$. The three cases (i), (ii), and (iii) in (c) correspond to surfaces with p-rank 1, 2, and 0, respectively.

We now look at the possibility that $f = h^2$ or $f = h^4$ for h an irreducible Weil polynomial. If $f = h^4$, then h is linear and thus h has a real root. The case when h has a real root has already been discussed in the closing paragraph of Section 2 of this chapter. This leaves the case where $f = h^2$ for h an irreducible Weil quadratic polynomial with no real root. Let $h(x) = x^2 - \beta x + q$, let π be a root, and let $E = \mathbb{Q}(\pi)$. In order to guarantee that h has no real root we need $|\beta| < 2\sqrt{q}$. We also need to get $e = 2$, where e is the least common multiple of the denominators of the local invariants. In particular, we need the local invariants for the primes of $\mathcal{O}_E$ over p to be equal to $\frac{1}{2}$. If the Newton polygon $\mathrm{Np}_p(h)$ has a vertex at $(1, v_p(\beta))$, then $v_p(\beta) < \frac{n}{2}$. Examining the slopes of the Newton polygon we get that

the local invariants are $\frac{v_p(\beta)}{n}$ and $\frac{n-v_p(\beta)}{n}$. However, the condition that $v_p(\beta) < \frac{n}{2}$ means that $\frac{v_p(\beta)}{n}$ cannot be $\frac{1}{2}$, a contradiction. Therefore, $(1, v_p(\beta))$ cannot be a vertex of $\mathrm{Np}_p(h)$. But this means that $\mathrm{Np}_p(h)$ is just a single line segment, hence h corresponds to a supersingular abelian variety. However, no supersingular abelian variety is absolutely simple [15, 4.2], so we ignore this case.

2.5.3 Abelian 3-folds

The classification of Weil polynomials of abelian 3-folds is primarily due to Haloui. First we remark that if $f = h^e$ is the characteristic polynomial of Frobenius corresponding to an isogeny class of simple abelian 3-folds, then f does not have a real root. This is due to the analysis of Weil q-numbers given at the end of section 2.2. Such Weil q-numbers always correspond to either a supersingular elliptic curve or an abelian surface. Thus if f has a real root, the corresponding abelian 3-fold is not simple. This allows us to eliminate the cases $e = 2$ and $e = 6$, so either $e = 1$ and f is irreducible or else $f = h^3$.

The first theorem in the classification of abelian 3-folds will simply assume that the characteristic polynomial of Frobenius f does not have a real root. Thus the roots of f occur as pairs of complex conjugate Weil q-numbers and so f must be of the form $f(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^2 + a_1q^2x + q^3$. We have the following result due to Haloui:

Theorem 2.19 ([18] 1.1)**.** *Let $f(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^2 + a_1q^2x + q^3$. Then f is a Weil polynomial with no real root if and only if the following conditions*

hold:

(a) $|a_1| < 6\sqrt{q}$,

(b) $4\sqrt{q}|a_1| - 9q < a_2 \leq \frac{a_1^3}{3} + 3q$,

(c) $-\frac{2a_1^3}{27} + \frac{a_1 a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leq a_3 \leq -\frac{2a_1^3}{27} + \frac{a_1 a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}$,

(d) $-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} < a_3 < -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}$.

Next we state conditions for when such an f is irreducible:

Proposition 2.20 ([18] 1.3)**.** *Set*

$$r = -\frac{a_1^2}{3} + a_2 - 3q, \quad s = \frac{2a_1^3}{27} - \frac{a_1 a_2}{3} - qa_1 + a_3,$$
$$\Delta = s^2 - \frac{4}{27}r^3, \quad u = \frac{-s+\sqrt{\Delta}}{2}.$$

Then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $\Delta \neq 0$ and u is not a cube in $\mathbb{Q}(\sqrt{\Delta})$.

Last we give conditions that ensure $e = 1$:

Theorem 2.21 ([18] 1.4)**.** *Let $f(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^2 + a_1q^2x + q^3$ be an irreducible Weil q-polynomial. Then f is the characteristic polynomial of an abelian 3-fold if and only if one of the following conditions holds:*

(a) $v_p(a_3) = 0$,

(b) $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, *and f has no root of valuation $n/2$ in $\mathbb{Q}_p$,*

(c) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, *and f has no root of valuation $n/2$ in $\mathbb{Q}_p$,*

(d) $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$ *and* f *has no root in* $\mathbb{Q}_p$,

(e) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) \geq 3n/2$, *and* f *has no root in* $\mathbb{Q}_p$ *nor factor of degree three in* $\mathbb{Z}_p[x]$.

The p-ranks of abelian varieties in (a)-(e) are respectively 3,2,1,0, and 0. The abelian varieties in case (e) are supersingular.

The case where $e = 3$ is dealt with in [19]. We will not be dealing with this case so we omit the statement of the theorem.

2.5.4 Abelian 4-folds

The classification of abelian 4-folds is due to Haloui, Singh and Xing. However, there are errors in the draft of the paper of Haloui and Singh ([20]) that was placed in the arXiv. Thus the statement of the theorems in this thesis will not exactly match those found in [20]. Since we are primarily interested in Weil polynomials corresponding to simple abelian varieties, we may again restrict to Weil polynomials that do not have any real roots. We already know that the general form for the characteristic polynomial of Frobenius is $f(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 + a_2q^2x^2 + a_1q^3x + q^4$. We have the following theorem:

Theorem 2.22 ([20] 1.1)**.** *Let* $f(X) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 +$

$a_2q^2x^2 + a_1q^3x + q^4$ be a polynomial with integer coefficients. Set

$$\begin{aligned} r_2 &= -\tfrac{3a_1^2}{8} + a_2 - 4q \\ r_3 &= \tfrac{a_1^3}{8} - qa_1 - \tfrac{a_1a_2}{2} + a_3 \\ r_4' &= -\tfrac{3a_1^4}{256} + \tfrac{qa_1^2}{2} + \tfrac{a_1^2a_2}{16} - \tfrac{a_1a_3}{4} - 2qa_2 + 2q^2 \\ j &= e^{\frac{2\pi i}{3}} \\ \omega &= \tfrac{1}{24}\left(-8r_2^6 - 540r_2^3r_3^2 + 729r_3^4 + i9|r_3|(-r_3^2 - \tfrac{8}{27}r_2^3)^{3/2}\right)^{1/3} \end{aligned}$$

where ω is some third root. Now let $S := \{\omega + \bar{\omega} + \frac{r_2^2}{6}, j\omega + \overline{j\omega} + \frac{r_2^2}{6}, \bar{j}\omega + j\bar{\omega} + \frac{r_2^2}{6}\}$. S is a set of three real numbers so let $\gamma_1 \leq \gamma_2 \leq \gamma_3$ be the three elements of S arranged from least to greatest. Then f is a Weil polynomial with no real root if and only if the following conditions hold:

(a) $|a_1| < 8\sqrt{q}$,

(b) $6\sqrt{q}|a_1| - 20q < a_2 \leq \frac{3a_1^2}{8} + 4q$,

(c) $-9qa_1 - 4\sqrt{q}a_2 - 16q\sqrt{q} < a_3 < -9qa_1 + 4\sqrt{q}a_2 + 16q\sqrt{q}$,

(d) $-\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 - (-\frac{2}{3}r_2)^{3/2} \leq a_3 \leq -\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 + (-\frac{2}{3}r_2)^{3/2}$,

(e) $2\sqrt{q}|qa_1 + a_3| - 2qa_2 - 2q^2 < a_4$,

(f) $\gamma_1 - r_4' \leq a_4 \leq \gamma_2 - r_4'$.

The next theorem assumes that f is irreducible and then finds conditions that force $e = 1$:

Theorem 2.23 ([20] 1.2)**.** *Let $f(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 + a_2q^2x^2 + a_1q^3x + q^4$ be an irreducible Weil polynomial. Then f is the characteristic polynomial of an abelian 4-fold if and only if one of the following conditions holds:*

(a) $v_p(a_4) = 0$,

(b) $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$, *and* f *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(c) $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq n$, *and* f *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(d) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 2n$, *and* f *has no root of valuation* $n/2$ *nor factor of degree three in* $\mathbb{Q}_p$,

(e) $v_p(a_1) = 0$, $v_p(a_2) \geq n/3$, $v_p(a_3) \geq 2n/3$, $v_p(a_4) = n$, *and* f *has no root of valuation* $n/3$ *or* $2n/3$ *in* $\mathbb{Q}_p$,

(f) $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$, $v_p(a_4) \geq 3n/2$, *and* f *has no root in* $\mathbb{Q}_p$,

(g) $v_p(a_1) \geq n/4$, $v_p(a_2) \geq n/2$, $v_p(a_3) = 3n/4$, $v_p(a_4) = n$, *and* f *has no root in* $\mathbb{Q}_p$ *nor factor of degree 2 or 3 in* $\mathbb{Q}_p$,

(h) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) = 3n/2$, $v_p(a_4) \geq 2n$, *and* f *has no root in* $\mathbb{Q}_p$ *nor factor of degree 3 in* $\mathbb{Q}_p$.

The p-ranks of abelian varieties in cases (a)-(h) are 4,3,2,1,1,0,0, and 0. The abelian varieties in case (h) are supersingular.

The other possibilities are $e = 2$ and $e = 4$, both of which are worked out in [19]. We will not be dealing with these cases so we omit the statement of the theorem.

Chapter 3

The splitting of p and the p-rank

Proposition 3.1. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$. Let $E' = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ and let $p \in \mathbb{Z}$ be a prime. Let α be a fixed root of f, let $\mathscr{P}_0$ be a fixed prime over p in E', let $a = \mathrm{ord}_{\mathscr{P}_0}(\alpha)$, and let N be the number of roots of f with $\mathscr{P}_0$-adic valuation equal to a. Then*

$$N = d\left(\frac{\#\{\mathscr{P} : \mathscr{P} \text{ divides } p \text{ and } \mathrm{ord}_{\mathscr{P}}(\alpha) = a\}}{\#\{\mathscr{P} : \mathscr{P} \text{ divides } p\}}\right) \tag{3.1}$$

where $\mathscr{P}$ runs through the primes of E'.

Proof. Let $G = \mathrm{Gal}(E'/\mathbb{Q})$, $H \leq G$ the stabilizer of α, and $D \leq G$ the stabilizer of $\mathscr{P}_0$. G acts transitively on the roots of f so we may pick elements $\tau_i \in G$ with the property that $\tau_i(\alpha_i) = \alpha$. Suppose that $\tau \in H\tau_i \cap H\tau_j$. Then $\tau = h\tau_i$ for some $h \in H$ and thus $\tau(\alpha_i) = h(\tau_i(\alpha_i)) = h(\alpha) = \alpha$, and likewise $\tau(\alpha_j) = \alpha$. But τ is an isomorphism and f has distinct roots, so $i = j$. Thus $\{H\tau_i : 1 \leq i \leq d\}$ are the right cosets of H. By relabeling if necessary we may assume without loss of generality that

(i) $\mathrm{ord}_{\mathscr{P}_0}(\alpha_1) = \mathrm{ord}_{\mathscr{P}_0}(\alpha_2) = \cdots = \mathrm{ord}_{\mathscr{P}_0}(\alpha_N) = a$

(ii) $\mathrm{ord}_{\mathscr{P}_0}(\alpha_i) \neq a$ if $i > N$.

Thus we now get

$$\begin{aligned}
\frac{\#\{\mathscr{P} : \mathscr{P} \mid p, \mathrm{ord}_{\mathscr{P}}(\alpha) = a\}}{\#\{\mathscr{P} : \mathscr{P} \mid p\}} &= \frac{\#\{\tau(\mathscr{P}_0) : \mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = a, \tau \in G\}}{[G : D]} \\
&= \frac{\#\{\tau : \mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = a\}/|D|}{[G : D]} \\
&= \frac{\#\{\tau : \mathrm{ord}_{\mathscr{P}_0}(\tau^{-1}(\alpha)) = a\}}{|G|} \\
&= \frac{\#\{\tau | \tau(\alpha_i) = \alpha \text{ for some } 1 \leq i \leq N\}}{|G|} \\
&= \frac{\#\left(\bigcup_{i=1}^{N} H\tau_i\right)}{|G|} \\
&= N \cdot \frac{|H|}{|G|} \\
&= N \cdot \frac{1}{[G : H]} \\
&= \frac{N}{d}
\end{aligned}$$

□

Remark 3.2. The Newton polygon $\mathrm{Np}_p(f)$ of f in the above theorem will have a segment of length N with slope a/e where e is the ramification index of p in E'. Normally we think of the Newton polygon as a local object due to the choice of a prime $\mathscr{P}_0$ over p. However, the right hand side of (3.1) is determined with the global data. Thus this theorem provides a kind of dual way to view the Newton polygon. Instead of fixing a particular prime $\mathscr{P}_0$, we may instead fix the root α and compute the right hand side of (3.1).

Theorem 3.3. *Let A be a simple abelian variety over k with commutative endomorphism ring, $r(A)$ the p-rank of A, f the characteristic polynomial of Frobenius,*

π a root of f in $\mathbb{C}$, and $\beta = \pi + \bar{\pi}$. Let $E = \mathbb{Q}(\pi)$ and $K = \mathbb{Q}(\beta)$. Let E' be the Galois closure of E in $\mathbb{C}$ and let K' be the Galois closure of K in $\mathbb{C}$. Then we have

$$r(A) = 2g\left(\frac{\#\{\mathscr{P} : \mathscr{P} \text{ divides } p \text{ and } \pi \notin \mathscr{P}\}}{\#\{\mathscr{P} : \mathscr{P} \text{ divides } p\}}\right) \tag{3.2}$$

where $\mathscr{P}$ runs through the primes of E', and

$$r(A) = g\left(\frac{\#\{P : P \text{ divides } p \text{ and } \beta \notin P\}}{\#\{P : P \text{ divides } p\}}\right). \tag{3.3}$$

where P runs through the primes of K'.

Proof. Equation (3.2) follows immediately from Corollary 2.13 and the above remark. Equation (3.3) will follow from (3.2). First we observe that K' and E' are both Galois over $\mathbb{Q}$ and so the splitting behavior of the prime P in E' is independent of the choice P. In other words, if one prime P over p in K' is split/ramified/inert in E', then all primes over p in K' are split/ramified/inert in E'.

Suppose that P is ramified or inert in E' and $\mathscr{P}$ is the prime in E' over P. This is equivalent to having $\mathscr{P}^c = \mathscr{P}$. We have that $\pi\bar{\pi} = q \in \mathscr{P}$ and $\mathscr{P}$ is prime, so either $\pi \in \mathscr{P}$ or $\bar{\pi} \in \mathscr{P}$. If $\bar{\pi} \in \mathscr{P}$, then taking conjugates gives $\pi \in \mathscr{P}^c = \mathscr{P}$. Thus we must have that $\pi, \bar{\pi} \in \mathscr{P}$, and therefore we also must have $\beta \in P$. As shown above, this behavior is independent of the choice of prime P, so we get that $\pi \in \mathscr{P}$ for all primes $\mathscr{P}$ over p in E' and that $\beta \in P$ for all primes P over p in K'. In particular,

$$\#\{\mathscr{P} : \mathscr{P} \text{ divides } p \text{ and } \pi \notin \mathscr{P}\} = \#\{P : P \text{ divides } p \text{ and } \beta \notin P\} = 0.$$

Thus (3.3) agrees with (3.3) in this case, namely $r(A) = 0$.

Suppose that P is a prime in K' which does not contain β. Then the argument in the previous paragraph shows that we must have that P splits in E', and consequently all primes in K' over p split in E'. Let $\mathscr{P}$ and $\mathscr{P}^c$ be the distinct primes in E' that lie over P. We know that π must lie in at least one of $\{\mathscr{P}, \mathscr{P}^c\}$, so without loss of generality we may assume that $\pi \in \mathscr{P}$ and by taking conjugates we also get that $\bar{\pi} \in \mathscr{P}^c$. As $\beta = \pi + \bar{\pi}$ and $\beta \notin P$ by assumption, it follows that $\pi \notin \mathscr{P}^c$. Thus

$$\#\{\mathscr{P} : \mathscr{P} \text{ divides } P \text{ and } \pi \notin \mathscr{P}\} = 1.$$

Now suppose that there is a prime $\mathscr{P}$ in E' such that $\pi \notin \mathscr{P}$. But $\pi\bar{\pi} = q \in \mathscr{P}$, hence $\bar{\pi} \in \mathscr{P}$. Taking conjugates gives $\pi \in \mathscr{P}^c$. Let $P = \mathscr{P} \cap \mathcal{O}_K$. Then we have that $\beta \notin P$ and

$$\#\{\mathscr{P} : \mathscr{P} \text{ divides } P \text{ and } \pi \notin \mathscr{P}\} = 1.$$

Putting this together with the previous paragraph gives

$$\#\{\mathscr{P} : \mathscr{P} \text{ divides } p \text{ and } \pi \notin \mathscr{P}\} = \#\{P : P \text{ divides } p \text{ and } \beta \notin P\}.$$

Since every prime in K' splits in E', the denominator in (3.3) is half the value of the denominator in (3.2). Thus the formula in (3.3) follows from (3.2). □

Proposition 3.4. *Let f, E', and α be as in Proposition 3.1. Let $E = \mathbb{Q}(\alpha)$ and let $\mathscr{P}_1, \ldots, \mathscr{P}_s$ be the primes of E over p. For each $\mathscr{P}_i$ let e_i be the ramification index of $\mathscr{P}_i$ over p and f_i the degree of the extension of residue fields for $\mathscr{P}_i$ over p. Let e be the ramification index of p in the Galois extension E' and let a/e be a slope of*

a segment of $\mathrm{Np}_p(f)$ *with length* N. *Let* $S_a = \{i : \mathrm{ord}_{\mathscr{P}_i}(\alpha) = \frac{ae_i}{e}, 1 \leq i \leq s\}$. *Then*

$$N = \sum_{i \in S_a} e_i f_i. \tag{3.4}$$

Proof. We already have that E' is the Galois closure of E in $\mathbb{C}$. Let g_i denote the number of primes in E' that lie over $\mathscr{P}_i$. Since E' is Galois over $\mathbb{Q}$, it is also Galois over E. Thus we can let a_i be the ramification index of $\mathscr{P}_i$ in E' and let b_i be the degree of the extension of residue fields with respect to $\mathscr{P}_i$. As E' is Galois over E we get that

$$[E' : E] = a_1 b_1 g_1 = a_2 b_2 g_2 = \cdots = a_s b_s g_s. \tag{3.5}$$

Now let m be the degree of the extension of residue fields with respect to p in E'. We then have that $a_i e_i = e$ and $b_i f_i = m$ for all $1 \leq i \leq s$. Thus dividing (3.5) through by em we get

$$\frac{g_1}{e_1 f_1} = \frac{g_2}{e_2 f_2} = \cdots = \frac{g_s}{e_s f_s}.$$

We now turn to Proposition 3.1. With our notation, $\#\{\mathscr{P} : \mathscr{P} \mid p\} = \sum_{i=1}^{s} g_i$. Furthermore, if $\mathscr{P}$ lies over $\mathscr{P}_i$, then $\mathrm{ord}_{\mathscr{P}}(\alpha) = a$ if and only if $\mathrm{ord}_{\mathscr{P}_i}(\alpha) = \frac{a}{a_i} = \frac{ae_i}{e}$.

If we define $S_i := \{\mathscr{P} : \mathscr{P} \mid \mathscr{P}_i\}$, then $g_i = |S_i|$. Putting it all together we get

$$\begin{aligned}
N &= d\left(\frac{\#\{\mathscr{P} : \mathscr{P} \mid p, \operatorname{ord}_{\mathscr{P}}(\alpha) = a\}}{\#\{\mathscr{P} : \mathscr{P} \mid p\}}\right) \\
&= d\left(\frac{\#\{\mathscr{P} : \mathscr{P} \text{ divides } \mathscr{P}_i \text{ for some } i \in S_a\}}{\#\{\mathscr{P} : \mathscr{P} \mid p\}}\right) \\
&= d\left(\frac{\sum_{i\in S_a} |S_i|}{\sum_{j=1}^{s} g_j}\right) \\
&= d\sum_{i\in S_a}\left(\frac{|S_i|}{\sum_{j=1}^{s} g_j}\right) \\
&= d\sum_{i\in S_a}\left(\frac{g_i}{\sum_{j=1}^{s} \frac{e_j f_j}{e_i f_i} g_i}\right) \\
&= d\sum_{i\in S_a}\left(\frac{e_i f_i}{\sum_{j=1}^{s} e_j f_j}\right) \\
&= d\sum_{i\in S_a}\left(\frac{e_i f_i}{d}\right) \\
&= \sum_{i\in S_a} e_i f_i
\end{aligned}$$

□

Remark 3.5. This gives a refinement of the relation $d = \sum_{i=1}^{s} e_i f_i$.

Theorem 3.6. *Let A be a simple abelian variety of dimension g defined over the finite field $k = \mathbb{F}_q$ for $q = p^n$. Let $r(A)$ denote the p-rank of the abelian group $A(\bar{k})[p]$. Let $f \in \mathbb{Z}[x]$ be the characteristic polynomial of the Frobenius endomorphism of A and suppose that f is irreducible. Let π be a root of f, $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, $K = \mathbb{Q}(\beta)$. For each prime P in K over p and $\mathscr{P}$ in E over p, let $e(P)$ and $e(\mathscr{P})$ be the ramification index of P and $\mathscr{P}$ over p, respectively, and let $f(P)$ and $f(\mathscr{P})$ be degree of the extension of $\mathbb{Z}/p\mathbb{Z}$ corresponding the the primes P and $\mathscr{P}$, respectively.*

Then

$$r(A) = \sum_{\pi \notin \mathscr{P}} e(\mathscr{P}) f(\mathscr{P}) \tag{3.6}$$

where the sum ranges over the primes in E over p not containing π, and

$$r(A) = \sum_{\beta \notin P} e(P) f(P) \tag{3.7}$$

where the sum ranges over the primes in K over p not containing β.

Proof. (3.6) follows from Proposition 3.4 by letting $\alpha = \pi$ and $a = 0$. The proof of (3.7) follows from the fact that any prime P of K that does not contain β must split in E as $\mathscr{P}$ and $\mathscr{P}^c$. But E is quadratic over K, so if P splits then we get that $e(P) = e(\mathscr{P}) = e(\mathscr{P}^c)$ and $f(P) = f(\mathscr{P}) = f(\mathscr{P}^c)$. Exactly one of $\{\mathscr{P}, \mathscr{P}^c\}$ does not contain π and thus every summand in (3.7) appears in (3.6). Conversely, if $\pi \notin \mathscr{P}$ for some $\mathscr{P}$, then $\mathscr{P}^c \neq \mathscr{P}$ and $\pi \in \mathscr{P}^c$. Furthermore, if we let $P = \mathscr{P} \cap \mathcal{O}_K$, then $e(P) = e(\mathscr{P})$ and $f(P) = f(\mathscr{P})$ because E is quadratic over K and P splits in E. Since $\beta = \pi + \bar{\pi}$, $\pi \notin \mathscr{P}$, and $\bar{\pi} \in \mathscr{P}$, we see that $\beta \notin P$. Thus every summand in (3.6) appears in (3.7), hence (3.6) and (3.7) have the same summands. □

Remark 3.7.

(a) Equation (3.7) is easily seen to be qualitatively correct because $g = [K : \mathbb{Q}] = \sum_P e(P) f(P)$. Thus $r(A)$ must lie between 0 and g, as required.

(b) This theorem extends Theorem 2.14, which was only able to determine the extremes, either $r(A) = 0$ or $r(A) = g$.

Example 3.8. *(Elliptic Curves)* Let C be an elliptic curve over k with $\mathbb{Q} \otimes \mathrm{End}_k(C)$ commutative. Then $E = \mathbb{Q}(\pi)$ is a quadratic imaginary extension of $\mathbb{Q}$. Suppose

that in $\mathcal{O}_E$ we get a factorization $(p) = \mathscr{P}\mathscr{P}^c$. Then we must have that $(\pi) = \mathscr{P}^i(\mathscr{P}^c)^{n-i}$. The two local invariants are therefore i/n and $(n-i)/n$. In order for these to be integers, we must have $i \in \{0, n\}$. Thus, only one of $\{\mathscr{P}, \mathscr{P}^c\}$ contains π and so equation (3.6) gives $r(C) = 1$. If p is inert or ramifies in E, then there is only one prime $\mathscr{P}$ in E over p and it must contain π. Thus (3.6) gives $r(C) = 0$.

Example 3.9. *(Abelian Surfaces)* This example is contained in the proof of [14, Thm. 3.7] but we present it here in light of Theorem 3.6 which gives the calculations a slightly different flavor than that found in [14]. Let A/k be an absolutely simple abelian variety of dimension 2. Then the factorization of (p) in E can only be one of the following cases:

a) $(p) = \mathscr{P}_1^2(\mathscr{P}_1^c)^2$ (p ramifies in K)

b) $(p) = \mathscr{P}_1\mathscr{P}_1^c$ (p is inert in K)

c) $(p) = \mathscr{P}_1\mathscr{P}_1^c\mathscr{P}_2^s,\ 1 \leq s \leq 2$ (p splits completely in K but not in E)

d) $(p) = \mathscr{P}_1\mathscr{P}_1^c\mathscr{P}_2\mathscr{P}_2^c$ (p splits completely in E)

Note that cases like $(p) = \mathscr{P}^4$ are not possible. If $(p) = \mathscr{P}^4$, then $(\pi) = \mathscr{P}^2$ and $(\bar{\pi}) = \mathscr{P}^2$. Thus $(\pi) = (\bar{\pi})$, hence A is supersingular, contradicting the hypothesis that A is absolutely simple.

In case a), the factorization of the ideal (π) in E is $\mathscr{P}_1^i(\mathscr{P}_1^c)^{2n-i}$ for some $0 \leq i \leq 2n$. The local invariants i/n and $(2n-i)/n$ are integers if and only if $i \in \{0, n, 2n\}$. The case $i = n$ is not possible because then $(\pi) = (\bar{\pi})$ and A would be supersingular hence not absolutely simple. Thus (π) is either $\mathscr{P}_1^{2n}$ or $(\mathscr{P}_1^c)^{2n}$. Without loss of generality we may assume that $(\pi) = (\mathscr{P}_1)^{2n}$. The sum in (3.6) only contains one summand corresponding to $\mathscr{P}_1^c$. For $\mathscr{P}_1^c$ we have $e_1 = 2$ and $f_1 = 1$

and thus $r(A) = 2$ by Theorem 3.6.

In case b), in order for the local invariants integers, it must be that (π) is $\mathscr{P}_1^n$ or $(\mathscr{P}_1^c)^n$. Without loss of generality assume $(\pi) = (\mathscr{P}_1)^n$. Since p is inert in K it follows that $e_1 = 1$ and $f_1 = 2$ for the prime $\mathscr{P}_1^c$ and therefore $r(A) = 2$.

In case c) we have that (π) is $\mathscr{P}_1^n \mathscr{P}_2^{sn/2}$ or $(\mathscr{P}_1^c)^n \mathscr{P}_2^{sn/2}$. Without loss of generality assume that $(\pi) = (\mathscr{P}_1)^n \mathscr{P}_2^{sn/2}$. Thus $\mathscr{P}_1^c$ is the only prime over p in E that does not contain π. We have that $e_1 = 1$ and $f_1 = 1$ for $\mathscr{P}_1^c$ and so $r(A) = 1$.

In case d) the ideal (π) is $\mathscr{P}_1^n \mathscr{P}_2^n$, $\mathscr{P}_1^n (\mathscr{P}_2^c)^n$, $(\mathscr{P}_1^c)^n \mathscr{P}_2^n$, or $(\mathscr{P}_1^c)^n (\mathscr{P}_2^c)^n$. For all primes in E over p we have that $e_i = f_i = 1$. In every one of the four cases for the factorization of (π) we see that π is not contained in exactly two primes of the primes of E over p and thus $r(A) = 2$.

Example 3.10. *(Abelian 3-folds)* The case of abelian 3-folds can be handled similarly to that of abelian surfaces if one is patient enough to enumerate all possible splitting behaviors of p in K and E. We will not do this exhaustively here, but we will hit upon some highlights. For an example of such an analysis, suppose that A is defined over $k = \mathbb{F}_p$. Suppose that $(p) = P_1 P_2^2$ in K and suppose that P_1 splits in E into $\mathscr{P}_1$ and $\mathscr{P}_1^c$. Suppose also that P_2 is inert in E, and let $\mathscr{P}_2$ be the unique prime in E lying over P_2. Then it must be that (π) is $\mathscr{P}_1 \mathscr{P}_2$ or $\mathscr{P}_1^c \mathscr{P}_2$. Without loss of generality assume that it is the first case. Then $\beta \notin P_1$ and $\beta \in P_2$. Therefore by Theorem 3.6 we get that $r(A) = 1$. An example of an abelian 3-fold with this behavior is the isogeny class corresponding to the Weil polynomial $f(x) = x^6 - 3x^5 + 10x^3 - 75x + 125$.

One difference between abelian surfaces and abelian 3-folds is that the splitting

of p completely determines $r(A)$ for an abelian surface, but for abelian 3-folds the splitting of p is not quite strong enough. We also need to know the factorization of (π) into primes in E. For example, let $f_1(x) = x^6 - 5x^5 + 17x^4 - 47x^3 + 85x^2 - 125x + 125$ and let $f_2(x) = x^6 - 4x^5 + 10x^4 - 25x^3 + 50x^2 - 100x + 125$. These are the characteristic polynomials for the Frobenius endomorphisms of non-isogenous absolutely simple abelian 3-folds A_1 and A_2 defined over $k = \mathbb{F}_5$. In both cases we see that (p) factors as $P_1P_2^2$ in K and as $\mathscr{P}_1\mathscr{P}_1^c\mathscr{P}_2^2(\mathscr{P}_2^c)^2$ in E. However, in the case of A_1, we see that $(\pi_1) = \mathscr{P}_1\mathscr{P}_2^2$ while in the case of A_2, we get $(\pi_2) = \mathscr{P}_1\mathscr{P}_2\mathscr{P}_2^c$. It follows that $\beta_1 \notin P_1, P_2$ while $\beta_2 \notin P_1$, $\beta \in P_2$. Applying formula (3.7) we see that $r(A_1) = 3$ and so A_1 is ordinary while $r(A_2) = 1$.

Now let $f(x) = x^6 - 5x^5 + 15x^4 - 35x^3 + 75x^2 - 125x + 125$. Then $(p) = \mathscr{P}^3(\mathscr{P}^c)^3$ in E and p is totally ramified in K. In this case $(\pi) = \mathscr{P}^2\mathscr{P}^c$ and $(\bar{\pi}) = \mathscr{P}(\mathscr{P}^c)^2$. Thus π lies in every prime of E over p and so $r(A) = 0$, but $(\pi) \neq (\bar{\pi})$ and therefore A is not supersingular. A case such as this is impossible for surfaces.

Chapter 4

The Index $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$

In this section we study the p-part of $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. By Porism 2.9, this is the more interesting part. We know that $\mathrm{End}_k(A)$ always contains $\mathbb{Z}[\pi, \bar{\pi}]$, so if $\mathbb{Z}[\pi, \bar{\pi}]$ is maximal at p then so is $\mathrm{End}_k(A)$. First we study the case of elliptic curves and abelian surfaces to motivate the idea that the splitting behavior of p in E can be used to prove the maximality or non-maximality of $\mathbb{Z}[\pi, \bar{\pi}]$ at p. We then consider the case of higher dimensional abelian varieties.

4.1 Elliptic Curves

Let C be an elliptic curve defined over $k = \mathbb{F}_q$ and assume that $\mathbb{Q} \otimes \mathrm{End}_k(C)$ is a quadratic imaginary extension of $\mathbb{Q}$. Let $f(x) = x^2 - \beta x + q$ be the characteristic polynomial of Frobenius, π a root of f, and $E = \mathbb{Q}(\pi)$. In this case $\beta = \pi + \bar{\pi} \in \mathbb{Z}$ and therefore $\mathbb{Z}[\pi] = \mathbb{Z}[\pi, \bar{\pi}]$, thus we restrict ourselves to studying $[\mathcal{O}_E : \mathbb{Z}[\pi]]$. Since f is quadratic, its discriminant is $f'(\pi)^2$ and by definition this is the same as the discriminant of the free $\mathbb{Z}$-module $\mathbb{Z}[\pi]$, denoted $\Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi])$ (see [16, III §3] for basic facts about discriminants). Therefore, $\Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi]) = f'(\pi)^2 = (2\pi - \beta)^2 = (\pi - \bar{\pi})^2$. If $r(C) = 1$, then by Example 3.8 we get that p splits in E into distinct primes $\mathscr{P}$ and $\mathscr{P}^c$. Without loss of generality $\pi \in \mathscr{P}$, $\pi \notin \mathscr{P}^c$ and therefore $\pi - \bar{\pi} \notin \mathscr{P}$ and

$\pi - \bar{\pi} \notin \mathscr{P}^c$. Putting these together we get that $p \nmid \Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi])$. But

$$\Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi]) = [\mathcal{O}_E : \mathbb{Z}[\pi]]^2 \Delta_{E/\mathbb{Q}}(\mathcal{O}_E)$$

so if p does not divide the left hand side, then neither can it divide $[\mathcal{O}_E : \mathbb{Z}[\pi]]$. Therefore, $\mathbb{Z}[\pi]$ is maximal at p.

On the other hand, if $r(A) = 0$, then it is true that $\mathrm{End}_k(C)$ is maximal at p, but $\mathbb{Z}[\pi]$ need not be maximal at p (see [6, 4.2] and the example that follows). For example, if $\pi = 3\frac{1-\sqrt{-3}}{2}$ then this π corresponds to a supersingular elliptic curve over $\mathbb{F}_9$ which does not have all its endomorphisms defined over the base field. $\mathbb{Z}[\pi]$ has conductor 3 in $\mathcal{O}_E = \mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$ and thus is not maximal at 3. If we try to duplicate the proof of the previous paragraph we can see where that argument breaks down. In this example we note that 3 ramifies as $\mathscr{P}^2$ in E and $\pi, \bar{\pi} \in \mathscr{P}$. Thus $\Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi]) = (\pi - \bar{\pi})^2 \in (\mathscr{P}^2 \cap \mathbb{Z}) = (3)$. Since $\Delta_{E/\mathbb{Q}}(\mathbb{Z}[\pi])$ is not prime to p we cannot conclude that $[\mathcal{O}_E : \mathbb{Z}[\pi]]$ is prime to p. Therefore we see that in the case of elliptic curves the splitting behavior of p in E strongly affects whether or not $\mathbb{Z}[\pi]$ is maximal at p. This will be the motivation for the way we will study $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$.

4.2 Abelian Surfaces

We begin by proving a general fact that will hold in higher dimensions.

Lemma 4.1. *Let A be any simple abelian variety of dimension g defined over $k = \mathbb{F}_q$. Let f be the characteristic polynomial of Frobenius, π a root of f, $\beta = \pi + \bar{\pi}$, and $K = \mathbb{Q}(\beta)$. Then $[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]] = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2$.*

Proof. Let $\{\alpha_0, \alpha_2, \ldots, \alpha_{g-1}\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We also have that $\{\beta^i : 0 \leq i \leq g-1\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\beta]$. Because $\mathbb{Z}[\beta] \subseteq \mathcal{O}_K$, we may find integers c_{ij} such that

$$\beta^i = \sum_{j=0}^{g-1} c_{ij}\alpha_j, \qquad 0 \leq i \leq g-1.$$

Let M be the $g \times g$ matrix with ij-entry c_{ij}. Next we observe that π satisfies a monic quadratic polynomial over $\mathcal{O}_K$, hence the set $S = \{1, \pi\}$ is an $\mathcal{O}_K$-basis for $\mathcal{O}_K[\pi]$. Actually, π is quadratic over the integral domain $\mathbb{Z}[\beta]$, hence S is also a $\mathbb{Z}[\beta]$-basis for $\mathbb{Z}[\beta][\pi]$. But $\mathbb{Z}[\pi, \bar{\pi}] = \mathbb{Z}[\beta][\pi]$, hence S is a $\mathbb{Z}[\beta]$-basis for $\mathbb{Z}[\pi, \bar{\pi}]$. Thus we get that $\mathcal{B}_1 := \{\alpha_i\pi^s : 0 \leq i \leq g-1, 0 \leq s \leq 1\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K[\pi]$ and $\mathcal{B}_2 := \{\beta^i\pi^s : 0 \leq i \leq g-1, 0 \leq s \leq 1\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\pi, \bar{\pi}]$. In particular, we get the relations

$$\beta_i\pi^s = \sum_{j=0}^{g-1} c_{ij}\alpha_j\pi^s, \qquad s \in \{0, 1\}.$$

The change of basis matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$ is block diagonal:

$$\begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}.$$

Therefore, we get

$$[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]] = (\det M)^2 = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2.$$

□

Theorem 4.2. *Let A be an absolutely simple abelian surface defined over the finite field $k = \mathbb{F}_q$ with $\mathbb{Q} \otimes \mathrm{End}_k(A)$ a field. Let π be a root of the characteristic polynomial of the Frobenius endomorphism of A, let $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, and $K = \mathbb{Q}(\beta)$.*

(a) If $q = p$, then $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$ is not divisible by p for $p > 13$.

(b) If $r(A) = 2$, then p does not divide $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$.

(c) If $r(A) = 1$, then p does not divide $[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]]$.

Proof. Part (a) for when A is ordinary has already been dealt with by Freeman and Lauter in [2]. We we will prove it in a slightly different manner, namely we will use our knowledge of the connection between $r(A)$ and the possible factorizations of p in E.

We will prove (b) first, so assume that A is ordinary. We then have that

$$\begin{aligned}
[\mathcal{O}_E : \mathcal{O}_K[\pi]]^2 &= \frac{\Delta_{E/\mathbb{Q}}(\mathcal{O}_K[\pi])}{\Delta_{E/\mathbb{Q}}(\mathcal{O}_E)} \\
&= \frac{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_K[\pi]))\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)^2}{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E))\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)^2} \\
&= \frac{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_K[\pi]))}{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E))}
\end{aligned}$$

where the second line follows from the relative discriminant formula [21, III.2.10]. We can deal with the numerator as follows: as above, $\mathcal{O}_K[\pi]$ has an $\mathcal{O}_K$-basis composed of $\{1, \pi\}$. This allows us to calculate

$$\Delta_{E/K}(\mathcal{O}_K[\pi]) = \det \begin{pmatrix} 1 & 1 \\ \pi & \bar{\pi} \end{pmatrix}^2 = (\pi - \bar{\pi})^2.$$

Thus the numerator becomes $N_{K/\mathbb{Q}}((\pi - \bar{\pi})^2)$. Since A is ordinary, the principal ideals (π) and $(\bar{\pi})$ in $\mathcal{O}_E$ are relatively prime by Theorem 2.14(a). Therefore, for every prime $\mathscr{P}$ in E over p we have that exactly one of $\{\mathrm{ord}_{\mathscr{P}}(\pi), \mathrm{ord}_{\mathscr{P}}(\bar{\pi})\}$ is nonzero. It then follows that the principal ideals $(\pi - \bar{\pi})$ and (p) are relatively

prime. Thus the numerator $N_{K/\mathbb{Q}}((\pi - \bar{\pi})^2)$ is not divisible by p. We therefore conclude that p cannot divide $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$. Thus, if p does divide $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$ then p must divide $[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]] = [\mathcal{O}_k : \mathbb{Z}[\beta]]^2$. This proves part (b).

Assume in addition that $q = p$. If $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$ are the two real embeddings of K, then the fact that π is a Weil p-number gives us the Hasse bound

$$|\sigma_i \beta| = |\sigma_i(\pi + \bar{\pi})| \leq |\pi| + |\bar{\pi}| = 2\sqrt{p}$$

where equality holds if and only if $\pi = \bar{\pi}$. But if $\pi = \bar{\pi}$, then A is not absolutely simple, contradicting our hypothesis. Thus, we may assume that $|\sigma_i \beta| < 2\sqrt{p}$. Next, since K is a quadratic extension of $\mathbb{Q}$, we have that β is quadratic over $\mathbb{Z}$, hence $\{1, \beta\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\beta]$. We therefore get the estimate

$$\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta]) = \begin{pmatrix} 1 & 1 \\ \sigma_1\beta & \sigma_2\beta \end{pmatrix}^2 \leq (|\sigma_1\beta| + |\sigma_2\beta|)^2 < 16p$$

Because K is a real quadratic extension, we also know that $\Delta_{K/\mathbb{Q}}(\mathcal{O}_K) \geq 5$. Therefore, if p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$, we get

$$p^2 \leq [\mathcal{O}_K : \mathbb{Z}[\beta]]^2 = \frac{\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])}{\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)} < \frac{16p}{5}.$$

The only p for which this could hold are $p \leq 3$. This proves part (a) for when A is ordinary.

Now drop the two assumptions that A is ordinary and $q = p$, and suppose instead that $r(A) = 1$. From Example 3.9, the only possible splitting of p for $r(A) = 1$ is $p\mathcal{O}_K = P_1 P_2$ and $p\mathcal{O}_E = \mathscr{P}_1 \mathscr{P}_1^c \mathscr{P}_2^s$ for $1 \leq s \leq 2$. Furthermore we may assume without loss of generality that $(\pi) = \mathscr{P}_1^n \mathscr{P}_2^{ns/2}$ and $\bar{\pi} = (\mathscr{P}_1^c)^n \mathscr{P}_2^{ns/2}$. In

particular, we get that $\beta \notin P_1$, $\beta \in P_2$. Next we observe that K is Galois over $\mathbb{Q}$ because it is a quadratic extension, hence P_1 and P_2 are Galois conjugate. Therefore, by relabeling the real embeddings σ_1 and σ_2 if necessary, we get that

$$\begin{array}{ll} P_1 \nmid (\sigma_1\beta) & P_2 \mid (\sigma_1\beta) \\ P_1 \mid (\sigma_2\beta) & P_2 \nmid (\sigma_2\beta) \end{array}.$$

Therefore we conclude that the principal ideals $(\sigma_2\beta - \sigma_1\beta)$ and (p) are relatively prime. In the previous paragraph we calculated

$$\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta]) = (\sigma_2\beta - \sigma_1\beta)^2$$

Putting these two facts together we see that $p \nmid \Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])$. As

$$\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta]) = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2 \Delta_{K/\mathbb{Q}}(\mathcal{O}_K)$$

we see that if p cannot divide the left hand side, then neither can it divide $[\mathcal{O}_K : \mathbb{Z}[\beta]]$. Therefore, if p does divide $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$, then p divides $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$. This proves (c).

Now assume in addition that $q = p$ and that p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. By part (c), we get that p divides $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$. Because π is a Weil p-number, we get that $|\sigma_i(\pi - \bar{\pi})^2| \leq 4p$, with equality holding if and only if $\pi = -\bar{\pi}$. However, if $\pi = -\bar{\pi}$, then A would not be absolutely simple. Thus we may assume that $|\sigma_i(\pi - \bar{\pi})^2| < 4p$. This gives us the following estimate:

$$|N_{K/\mathbb{Q}}((\pi - \bar{\pi})^2)| = |\sigma_1(\pi - \bar{\pi})^2 \sigma_2(\pi - \bar{\pi})^2| < (4p)(4p) = 16p^2.$$

From the previous paragraph, we observe that $q = p$ and $r(A) = 1$ implies that $s = 2$, thus $p\mathcal{O}_K = P_1P_2$ and $p\mathcal{O}_E = \mathscr{P}_1\mathscr{P}_1^c\mathscr{P}_2^2$. This means that P_1 splits in E and

P_2 ramifies in E. In particular, P_2 will divide $\Delta_{E/K}(\mathcal{O}_E)$. Taking norms from K to $\mathbb{Q}$, we see that $N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E)) \geq p$. Using the relative discriminant formula, we get the inequality

$$\begin{aligned} p^2 \leq [\mathcal{O}_E : \mathcal{O}_K[\pi]]^2 &= \frac{\Delta_{E/\mathbb{Q}}(\mathcal{O}_K[\pi])}{\Delta_{E/\mathbb{Q}}(\mathcal{O}_E)} \\ &= \frac{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_K[\pi]))\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)^2}{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E))\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)^2} \\ &= \frac{N_{K/\mathbb{Q}}((\pi - \bar{\pi})^2)}{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E))} < \frac{16p^2}{p} = 16p. \end{aligned}$$

The only primes p that can satisfy this inequality are those for which $p \leq 13$. This proves (a) for when $r(A) = 1$. Since $r(A) = 0$ implies that A is not absolutely simple, we have completed the proof of (a). □

Corollary 4.3. *Let A be an abelian surface as in Theorem 4.2 defined over $\mathbb{F}_p$ for $p > 2$. Then* $\mathrm{End}_k(A)$ *is maximal at p.*

Proof. For $p > 13$ this follows immediately from the theorem. For $3 \leq p \leq 13$, a computer system such as Magma can enumerate all possible Weil polynomials by using Theorem 2.17 and then check that $\mathbb{Z}[\pi, \bar{\pi}]$ is maximal at p for each one. □

Example 4.4. If $q \neq p$, then it is possible to have p divide $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$, as hinted at by parts (b) and (c) of the theorem. For example, let $f_1(x) = x^4+x^3+19x^2+25x+625$ and let π_1 be a root of $f_1(x)$. Then $f_1(x)$ corresponds to an isogeny class of ordinary abelian varieties and $\mathbb{Z}[\pi_1, \bar{\pi}_1]$ has index 25 inside the ring of integers of $\mathbb{Q}(\pi_1)$. Let $f_2(x) = x^4 + x^3 + 5x^2 + 25x + 625$ and let π_2 be a root of $f_2(x)$. Then $f_2(x)$

corresponds to an isogeny class of abelian varieties with p-rank one and $\mathbb{Z}[\pi_2, \bar{\pi}_2]$ has index 15 inside the ring of integers of $\mathbb{Q}(\pi_2)$.

Remark 4.5. As in the case of elliptic curves, the splitting behavior of p in K and E is what enables the proof to work. This provides further evidence that the splitting behavior of p in E for higher dimensional varieties will influence whether or not $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$ is divisible by p.

4.3 Higher dimensional abelian varieties

Throughout this subsection A will be an absolutely simple abelian variety of dimension $g \geq 3$ with commutative endomorphism ring. We let f be the characteristic polynomial of Frobenius, π a root of f, $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, and $K = \mathbb{Q}(\beta)$.

Proposition 4.6. *Let $q = p$ for $p \geq 3$. If there exists a prime P in K over p with ramification index e such that $\beta \in P$ and $e \geq 2$, then p divides $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$.*

Proof. We already have that

$$[\mathcal{O}_E : \mathcal{O}_K[\pi]] = \frac{N_{K/\mathbb{Q}}((\pi - \bar{\pi})^2)}{N_{K/\mathbb{Q}}(\Delta_{E/K}(\mathcal{O}_E))}.$$

The only way p can appear in the denominator is if some prime P of K ramifies in E. E is a quadratic extension of K, hence any prime of K that ramifies in E has ramification index equal to two. Since $p > 2$, it follows that all primes over p in K that ramify in E are tamely ramified. Thus, if P is a prime over p in K that ramifies in E, then P divides $\Delta_{E/K}(\mathcal{O}_E)$ exactly once [22, I.5 Thm. 2]. These are the only such primes of K over p that divide $\Delta_{E/K}(\mathcal{O}_E)$.

Next we examine what power of P can divide the principal ideal $((\pi - \bar{\pi})^2)$ and we get three cases:

case 1: P is ramified in E. Let $\mathscr{P}$ be the prime in E that lies over P and let e be the ramification index of P over p. We know that $\pi\bar{\pi} = p$ and that $\mathrm{ord}_{\mathscr{P}}(p) = 2e$. Furthermore $\mathscr{P}^c = \mathscr{P}$ and thus it must be that $\pi, \bar{\pi} \in \mathscr{P}^e$. Therefore $(\pi - \bar{\pi})^2 \in (\mathscr{P}^{2e} \cap \mathcal{O}_K) = P^e$.

case 2: P splits in E. Let $P\mathcal{O}_E = \mathscr{P}\mathscr{P}^c$. Then $\mathrm{ord}_{\mathscr{P}}(y) = \mathrm{ord}_P(y)$ for every $y \in K$ because $\mathscr{P}$ is not ramified over P. Thus we get that

$$\mathrm{ord}_P((\pi - \bar{\pi})^2) = \mathrm{ord}_{\mathscr{P}}((\pi - \bar{\pi})^2) \geq 2\min\{\mathrm{ord}_{\mathscr{P}}(\pi), \mathrm{ord}_{\mathscr{P}}(\bar{\pi})\}.$$

case 3: P is inert in E. Let $\mathscr{P}$ be the prime in E over P and let e be the ramification index of P over p. Then by an argument analogous to that of case 1 we get $\pi, \bar{\pi} \in \mathscr{P}^{e/2}$ and thus $(\pi - \bar{\pi})^2 \in P^e$.

Consider the fractional ideal $I = ((\pi - \bar{\pi})^2)/\Delta_{E/K}(\mathcal{O}_E)$ in K. The analysis done so far is summarized as follows:

$$\mathrm{ord}_P(I) \geq \begin{cases} e-1 & \text{if } P \text{ ramifies in } E \\ 2\min\{\mathrm{ord}_{\mathscr{P}}(\pi), \mathrm{ord}_{\mathscr{P}}(\bar{\pi})\} & \text{if } P \text{ splits in } E \\ e & \text{if } P \text{ is inert in } E \end{cases} \tag{4.1}$$

It follows that $\mathrm{ord}_P(I) \geq 0$ for all primes P over p. Therefore $\mathrm{ord}_p(N_{K/\mathbb{Q}}(I)) \geq 0$ and strict inequality will hold if $\mathrm{ord}_P(I) > 0$ for some P. Suppose now that we have a prime P with $\beta \in P$ and $e \geq 2$. If P ramifies or is inert then we get $\mathrm{ord}_P(I) > 0$ from (4.1). If P splits, then the additional hypothesis $\beta \in P$ implies that $\pi \in \mathscr{P}$

and $\pi \in \mathscr{P}^c$, or equivalently, $\mathrm{ord}_{\mathscr{P}}(\pi) > 0$ and $\mathrm{ord}_{\mathscr{P}}(\bar{\pi}) > 0$. Thus we see from (4.1) that $\mathrm{ord}_P(I) > 0$ in all cases, hence p divides $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$. □

Proposition 4.7. *If $q = p$, $p \geq 3$, and p splits completely in K, then $[\mathcal{O}_E : \mathcal{O}_K[\pi]]$ is not divisible by p.*

Proof. Let I be the fractional ideal defined in the proof of Proposition 4.6. It will be sufficient to prove that $\mathrm{ord}_P(I) = 0$ for all primes P over p in K. Suppose that P is inert in E, with $\mathscr{P}$ the unique prime of E lying over P. Then we have that $\mathscr{P}^c = \mathscr{P}$, so in particular $\mathrm{ord}_{\mathscr{P}}(\pi) = \mathrm{ord}_{\mathscr{P}}(\bar{\pi})$. Because p splits completely in K, we know that the ramification index of P over p is one. Thus we get

$$1 = \mathrm{ord}_P(p) = \mathrm{ord}_P(\pi\bar{\pi}) = \mathrm{ord}_{\mathscr{P}}(\pi\bar{\pi}) = 2\,\mathrm{ord}_{\mathscr{P}}(\pi).$$

But this is a contradiction because $\mathrm{ord}_{\mathscr{P}}(\pi)$ must be an integer. Therefore, P either splits in E or ramifies in E.

Suppose that P splits in E into $\mathscr{P}$ and $\mathscr{P}^c$. If π is in both $\mathscr{P}$ and $\mathscr{P}^c$, then $\mathrm{ord}_{\mathscr{P}}(\pi) > 0$ and $\mathrm{ord}_{\mathscr{P}}(\bar{\pi}) > 0$. Thus we get

$$1 = \mathrm{ord}_P(p) = \mathrm{ord}_P(\pi\bar{\pi}) = \mathrm{ord}_{\mathscr{P}}(\pi\bar{\pi}) > 2$$

a contradiction. Therefore, by relabeling if necessary, we may assume that $\pi \in \mathscr{P}$, $\pi \notin \mathscr{P}^c$. It then follows that

$$\mathrm{ord}_P((\pi - \bar{\pi})^2) = \mathrm{ord}_{\mathscr{P}}((\pi - \bar{\pi})^2) = 2\min\{\mathrm{ord}_{\mathscr{P}}(\pi), \mathrm{ord}_{\mathscr{P}}(\bar{\pi})\} = 0.$$

In particular, we get that $\mathrm{ord}_P(I) = 0$.

Suppose P ramifies in E. Let $\mathscr{P}$ be the unique prime of E that lies over P. Completing E at $\mathscr{P}$ gives us a totally and tamely ramified quadratic field extension

$E_w = \mathbb{Q}_p(\sqrt{\beta})$ over $\mathbb{Q}_p$ for some $\beta \in \mathbb{Z}_p$ with $v_p(\beta) = 1$ [16, II Prop. 12]. Thus we may represent π as $x+y\sqrt{\beta}$ where $x, y \in \mathbb{Q}_p$. In E we have that $\mathrm{ord}_{\mathscr{P}}(\pi) = \mathrm{ord}_{\mathscr{P}}(\bar{\pi})$, hence $v_p(\pi) = v_p(\bar{\pi})$ when we identify π and $\bar{\pi}$ with their images in E_w. This gives us the equation

$$1 = v_p(p) = v_p(\pi\bar{\pi}) = 2v_p(\pi) = 2\min\left\{v_p(x), v_p(y) + \frac{1}{2}\right\}.$$

Since $v_p(x)$ and $v_p(y)$ are either integers or ∞, the only possible way this equation holds is if $\mathrm{ord}_p(x) > 0$ and $\mathrm{ord}_p(y) = 0$. Next we note that complex conjugation on E fixes $\mathscr{P}$, hence complex conjugation on E extends to be the nontrivial field automorphism of E_w over $\mathbb{Q}_p$. This means that the image of $\bar{\pi}$ in E_w is given by $x - y\sqrt{\beta}$. With this identification of π and $\bar{\pi}$ in E_w, we get that

$$\mathrm{ord}_P((\pi - \bar{\pi})^2) = v_p((\pi - \bar{\pi})^2) = v_p(4y^2\beta) = 1.$$

Because P is tamely ramified in E, it follows that P divides $\Delta_{E/K}(\mathcal{O}_E)$ exactly once [22, I.5 Thm. 2], and thus

$$\mathrm{ord}_P(I) = \mathrm{ord}_P((\pi - \bar{\pi})^2) - \mathrm{ord}_P(\Delta_{E/K}(\mathcal{O}_E)) = 0.$$

Therefore, in all cases, $\mathrm{ord}_P(I) = 0$, hence $[\mathcal{O}_E : \mathcal{O}_K[\pi]] = N_{K/\mathbb{Q}}(I)$ is not divisible by p. □

Remark 4.8. This result partially proves Theorem 2.10. However, Proposition 4.7 is false when $q = p^n$ for $n > 1$. For example, let f be the Weil polynomial $f(x) = x^6 - 23x^5 + 247x^4 - 1565x^3 + 6175x^2 - 14375x + 15625$, let π be a root of f, $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, and $K = \mathbb{Q}(\beta)$. Then 5 splits completely in K, but $[\mathcal{O}_E : \mathcal{O}_K[\pi]] = 5$.

This example seems to contradict a remark in [6]. Remark 1 immediately after [6, 5.3] claims that any order containing $\mathcal{O}_K[\pi]$ is an order arising from an abelian variety. In particular, $R := \mathcal{O}_K[\pi]$ is a ring containing $\mathcal{O}_K[\pi]$ and so, according to the remark, should correspond to the endomorphism ring of an abelian variety. However, Theorem 2.10 says that R must also be maximal at p. But we have that $[\mathcal{O}_E : R] = 5$, so it seems that either the remark is false, or else 2.10 is false. We suspect that it is the remark that is false.

Proposition 4.9. *Assume that $p > g$ and also assume that A is not ordinary. Let $P_1, \ldots, P_s$ be the primes in K over p. Let e_i be the ramification index of P_i over p and let f_i be the residue class degree of P_i. Since A is not ordinary, $\beta \in P_i$ for some $1 \leq i \leq s$. Let $e_{\max} = \max\{e_i : \beta \in P_i\}$. If*

$$\frac{(g - r(A))(g - r(A) - 1)}{e_{\max}} > g - \sum_{i=1}^{s} f_i \tag{4.2}$$

then p divides $[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]]$.

Proof. By Lemma 4.1 we have $[\mathcal{O}_K[\pi] : \mathbb{Z}[\pi, \bar{\pi}]] = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2$ so we focus on

$$[\mathcal{O}_K : \mathbb{Z}[\beta]]^2 = \frac{\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])}{\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)}.$$

Looking first at the denominator, we know that P_i is tamely ramified in K (as $p > g$ by hypothesis) and thus $P_i^{e_i - 1}$ appears in the different $\mathfrak{D}_{K/\mathbb{Q}}$ and no higher power of P_i divides the different [22, I.5 Thm. 2]. Thus

$$\operatorname{ord}_p(\Delta_{K/\mathbb{Q}}(\mathcal{O}_K)) = \sum_{i=1}^{s} f_i(e_i - 1) = g - \sum_{i=1}^{s} f_i.$$

This is the term in the right hand side of (4.2).

Next we compute a lower bound on the power of p that divides $\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])$. Let K' be the Galois closure of K in $\mathbb{C}$. For each P_i that contains β and for $\mathscr{P}_i$ a prime of K' that lies over P_i, we see that $\beta \in \mathscr{P}_i^{e/e_i}$ where e is the ramification index of p in K'. In particular, $\beta \in \mathscr{P}_i^{e/e_{\max}}$. The power $e/e_{\max}$ is independent of the prime P_i and is also independent of the choice of a Galois conjugate of β, by which we mean the following: let $\beta_1, \ldots, \beta_g$ be the Galois conjugates of β and let $\mathscr{P}$ be a prime of K'. If $\beta_i \in \mathscr{P}$, then $\beta_i \in \mathscr{P}^{e/e_{\max}}$.

By the definition of discriminant we have $\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta]) = \prod_{i<j}(\beta_j - \beta_i)^2$. Let $\mathscr{P}$ be a prime of K' over p and let $S_{\mathscr{P}} = \{(i,j) : i < j, \beta_i \in \mathscr{P}, \beta_j \in \mathscr{P}\}$. Then by the last paragraph, we have that $\operatorname{ord}_{\mathscr{P}}((\beta_j - \beta_i)^2) \geq 2e/e_{\max}$ for all pairs $(i,j) \in S_{\mathscr{P}}$. In particular,

$$\operatorname{ord}_{\mathscr{P}}(\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])) \geq |S_{\mathscr{P}}| \left(\frac{2e}{e_{\max}}\right).$$

Now we calculate $|S_{\mathscr{P}}|$. By Theorem 2.12 we know that exactly $r(A)$ of the Galois conjugates of β are not contained in $\mathscr{P}$. By relabeling we may assume that $\beta_i \notin \mathscr{P}$ if $i \leq r(A)$ and $\beta_i \in \mathscr{P}$ if $i > r(A)$. Thus $S_{\mathscr{P}} = \{(i,j) : r(A) < i < j \leq g\}$. We then have that

$$|S_{\mathscr{P}}| = \sum_{n=1}^{g-r(A)-1} n = \frac{(g-r(A))(g-r(A)-1)}{2}.$$

Thus we get the estimate

$$\operatorname{ord}_{\mathscr{P}}(\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])) \geq |S_{\mathscr{P}}| \left(\frac{2e}{e_{\max}}\right) = \frac{e(g-r(A))(g-r(A)-1)}{e_{\max}}.$$

Since p has ramification index e in K', we get that

$$\operatorname{ord}_p(\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])) = (1/e)\operatorname{ord}_{\mathscr{P}}(\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])) \geq \frac{(g-r(A))(g-r(A)-1)}{e_{\max}}.$$

Thus we see that the power of p dividing $\Delta_{K/\mathbb{Q}}(\mathbb{Z}[\beta])$ is at least the left hand side of (4.2). Therefore, if (4.2) holds, then p divides $[\mathcal{O}_K : \mathbb{Z}[\beta]]$. □

Theorem 4.10. *Let A be an absolutely simple abelian variety of dimension $g \geq 3$ defined over the finite field $k = \mathbb{F}_p$ with $p > g$. Let $r(A)$ denote the p-rank of the abelian group $A(\bar{k})[p]$. Let $f \in \mathbb{Z}[x]$ be the characteristic polynomial of the Frobenius endomorphism of A and suppose that f is irreducible. Let π be a root of f, $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, and $K = \mathbb{Q}(\beta)$. Let $P_1, P_2, \ldots, P_s$ be the primes in K over p and $f_1, \ldots, f_s$ the degrees of the extensions of the finite fields corresponding to these primes. If*

$$r(A) < g - \frac{1}{2}\left(1 + \sqrt{1 + 4\left(g - \sum_{i=1}^{s} f_i\right)}\right) \tag{4.3}$$

then p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$.

Proof. First let us assume that A is not ordinary. Let e_i be the ramification index of P_i over p. If β is in some P_i and $e_i > 1$, then p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$ by Proposition 4.6. Therefore without loss of generality we may assume that if $\beta \in P_i$, then $e_i = 1$. Because A is not ordinary, we must have $\beta \in P_i$ for some $1 \leq i \leq s$. Thus $e_{\max} = 1$, where $e_{\max}$ is defined in Proposition 4.9. Therefore (4.2) becomes

$$(g - r(A))(g - r(A) - 1) > g - \sum_{i=1}^{s} f_i. \tag{4.4}$$

Solving for $r(A)$ by using the quadratic formula gives two roots:

$$\gamma_1 = g - \frac{1}{2}\left(1 + \sqrt{1 + 4\left(g - \sum_{i=1}^{s} f_i\right)}\right), \gamma_2 = g + \frac{1}{2}\left(1 + \sqrt{1 + 4\left(g - \sum_{i=1}^{s} f_i\right)}\right)$$

But we know that $r(A) \leq g$, so $r(A) > \gamma_2$ is impossible. Therefore, if (4.3) holds, then Proposition 4.9 applies and we get that p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$. The case

where A is ordinary is vacuous because, if $r(A) = g$, then (4.3) will never hold. This completes the proof. □

Corollary 4.11. *If $K/\mathbb{Q}$ is such that p is unramified in K and $r(A) < g - 1$, then p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$.*

Proof. In this case $\sum_{i=1}^{s} f_i = g$ so (4.3) becomes $r(A) < g - 1$. □

Example 4.12. Let $p = 5$, $k = \mathbb{F}_p$, $f(x) = x^8 - 8x^7 + 30x^6 - 75x^5 + 165x^4 - 375x^3 + 750x^2 - 1000x + 625$, and let A be an abelian variety in the isogeny class of f. Then $g = 4$ and K is a degree 4 totally real field. By Corollary 2.13, $r(A) = 1$. Alternatively we look at the splitting behavior of 5 in K and see that (p) factors as $P_1 P_2^3$ and $e_1 = 1$, $f_1 = 1$, $e_2 = 3$, $f_2 = 1$. We also see that $\beta \notin P_1$, $\beta \in P_2$ and thus by (3.7) we get $r(A) = 1$. The right hand side of (4.3) is 2 and thus Theorem 4.10 implies that $\mathbb{Z}[\pi, \bar{\pi}]$ is not maximal at 5. We can check this by directly calculating the index and get $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]] = 5$.

Example 4.13. It is possible to get some other interesting corollaries if one picks lower bounds on s. For example, if we let $r := R(A)$ and assume that $s \geq r + 2$, then $r + 2$ becomes a lower bound on the sum $\sum_{i=1}^{s} f_i$. Solving (4.4) leads to the inequality

$$0 < (g - r)(g - r - 1) - g + r + 2 = (g - (r + 1))^2 + 1$$

which is always true. Therefore, if $s \geq r + 2$, then p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$.

Chapter 5

Subrings of CM Fields of Degree 6 Corresponding to Abelian 3-folds of p-rank 1

This section explores what possible subrings could lie between $\mathbb{Z}[\pi, \bar{\pi}]$ and $\mathcal{O}_E$. As already mentioned, subrings R containing $\mathbb{Z}[\pi, \bar{\pi}]$ such that $[R : \mathbb{Z}[\pi, \bar{\pi}]]$ is a power of p are the more interesting cases. Theorem 4.10 suggests that it will be easier to find examples where p divides $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]]$ if $r(A)$ is small. The case $r(A) = 0$ is somewhat special, so instead we will work with abelian varieties with $r(A) = 1$.

Throughout this section we let p be a prime and $f(x) = x^6 + ax^5 + bx^4 + cx^3 + pbx^2 + p^2ax + p^3$ be an irreducible Weil polynomial corresponding to an abelian variety A defined over $k = \mathbb{F}_p$ with $g = 3$ and $r(A) = 1$. Thus $(a, p) = 1$ and p divides b and c, so there are integers b_1, c_1 such that $b = pb_1$ and $c = pc_1$. Let π be a root of f and let $E := \mathbb{Q}(\pi) \simeq \mathrm{End}_k^0(A)$. Then E is a CM field of degree 6, and let $\mathcal{O}_E$ be the ring of integers of E and let $T = \mathbb{Z}[\pi, \bar{\pi}] \subset O_E$.

Theorem 5.1. *Let $f(x) = x^6 + ax^5 + bx^4 + cx^3 + pbx^2 + p^2ax + p^3$ be an irreducible Weil polynomial corresponding to a simple abelian variety of dimension 3 defined over $\mathbb{F}_p$. Assume further that $r(A) = 1$, hence $(a, p) = 1$, $b = b_1p$, and $c = c_1p$ for some $b_1, c_1 \in \mathbb{Z}$. Let π be a root of f, $E = \mathbb{Q}(\pi)$, $T = \mathbb{Z}[\pi, \bar{\pi}]$, and $\mathcal{O}_E$ be the ring of integers of E. If $c_1 \equiv 2a \pmod{p}$, then there are subrings R_1, R_2 such that $T \subsetneq R_1 \subsetneq R_2 \subset \mathcal{O}_E$ and $p = [R_1 : T] = [R_2 : R_1]$. In particular, $p^2 \mid [\mathcal{O}_E : T]$.*

Proof. We can give the structure of T, R_1, and R_2 explicitly. We make the following definitions:

$$\begin{aligned} v_1 &= 1 \\ v_2 &= \pi \\ v_3 &= \pi^2 \\ v_4 &= \tfrac{1}{p^2}(\pi^5 + a\pi^4 + b\pi^3 + c\pi^2) \\ v_5 &= \tfrac{1}{p^2}(\pi^4 + a\pi^3 + py\pi^2 + pa\pi) \\ v_6 &= \tfrac{1}{p}(\pi^3 + a\pi^2) \end{aligned}$$

where $y \equiv 1 + b_1 - a_1c_1 \pmod{p}$ and where $a_1 \in \mathbb{Z}$ is a multiplicative inverse of a modulo p. We then define $R_2 := \mathbb{Z}\langle v_1, v_2, v_3, v_4, v_5, v_6\rangle$ to be the $\mathbb{Z}$-span of these elements, $R_1 := \mathbb{Z}\langle v_1, v_2, v_3, v_4, pv_5, v_6\rangle$, and $R_0 := \mathbb{Z}\langle v_1, v_2, v_3, v_4, pv_5, pv_6\rangle$. We now claim the following:

(a) R_0, R_1, and R_2 are rings, and since they are also finitely generated $\mathbb{Z}$-modules they are therefore subrings of $\mathcal{O}_E$.

(b) $T = R_0$.

We prove (a) by explicitly calculating the multiplication table for R_2 which will be produced below. We define k_1, k_2 to be the integers such that $y = 1+b_1-a_1c_1+k_1p$ and $c_1 = 2a+k_2p$. Before stating the results we will briefly describe how the table was computed. Let M be the change of basis matrix from the basis $\{1, \pi, \pi^2, \pi^3, \pi^4, \pi^5\}$ to $\{v_1, v_2, v_3, v_4, v_5, v_6\}$. M may be calculated by a computer algebra system. The products v_iv_j are calculated directly and then the higher powers of π are reduced using the relation given by $f(\pi) = 0$. Then M is applied to change coordinates.

Doing this gives the following table:

$$
\begin{aligned}
v_2^2 &= v_3 \\
v_2v_3 &= -av_3 + pv_6 \\
v_2v_4 &= -pv_1 - av_2 - b_1v_3 \\
v_2v_5 &= \left(-ak_1 + k_2(aa_1 - 1) + \tfrac{2a(aa_1-1)}{p}\right) v_3 \\
&\quad + v_4 + (1 - 2aa_1 + k_1p - a_1k_2p)v_6 \\
v_2v_6 &= -av_2 + (-1 + 2aa_1 - b_1 - k_1p + a_1k_2p)v_3 + pv_5 \\
v_4^2 &= b_1pv_1 + (a(-1 + b_1) - k_2p)v_2 + (1 - 2aa_1 + b_1^2 + k_1p - a_1k_2p)v_3 \\
&\quad - av_4 - pv_5 \\
v_4v_5 &= -av_1 + (-1 + 2aa_1 - b_1 + p(-k_1 + a_1k_2))v_2 \\
&\quad + \left(b_1(ak_1 + k_2 - aa_1k_2) + \tfrac{2ab_1(1-aa_1)}{p}\right) v_3 \\
&\quad - b_1v_4 - av_5 + (-1 - b_1 + 2aa_1b_1 + pb_1(a_1k_2 - k_1))v_6 \\
v_4v_6 &= a(-1 + b_1)v_2 + (-1 + b_1(1 - 2aa_1 + b_1 + k_1p - a_1k_2p))v_3 \\
&\quad - b_1pv_5 - av_6 \\
v_5^2 &= \text{see below} \\
v_5v_6 &= -av_1 + (-1 + ak_2)v_2 \\
&\quad + \left(a(-1 + b_1)\left(k_1 - a_1k_2 + \tfrac{2(1-aa_1)}{p}\right) + b_1k_2\right) v_3 \\
&\quad + (1 - 2aa_1 + p(k_1 - a_1k_2))v_4 + (-a - k_2p)v_5 \\
&\quad + b_1(2(aa_1 - 1) + p(-k_1 + a_1k_2))v_6 \\
v_6^2 &= -pv_1 + a(-1 + b_1)v_2 + b_1((-2aa_1 + b_1) + p(k_1 - a_1k_2))v_3 \\
&\quad + av_4 - b_1pv_5 + (-2a - k_2p)v_6
\end{aligned}
$$

The product v_5^2 is somewhat more complicated than the other products. We

get that $v_5^2 = \sum_{i=1}^{6} \lambda_i v_i$ where

$$\begin{aligned}
\lambda_1 &= -2 + 4aa_1 - b_1 + 2p(-k_1 + a_1k_2) \\
\lambda_2 &= -4a\left((k_1 - a_1k_2)(1 - aa_1) + \tfrac{(1-aa_1)^2}{p}\right) - ap(k_1 - a_1k_2)^2 \\
\lambda_3 &= -3k_1 + 12aa_1k_1 - 12a^2(a_1)^2k_1 - 3b_1k_1 + 4aa_1b_1k_1 \\
&\quad + b_1^2k_1 + a^2k_1^2 + 3a_1k_2 - 12a(a_1)^2k_2 + 12a^2(a_1)^3k_2 \\
&\quad + 3a_1b_1k_2 - 4a(a_1)^2b_1k_2 - a_1b_1^2k_2 + 2ak_1k_2 \\
&\quad - 2a^2a_1k_1k_2 + k_2^2 - 2aa_1k_2^2 + a^2(a_1)^2k_2^2 - b_1^2(k_1 - a_1k_2) \\
&\quad + \tfrac{4a^2(1-aa_1)^2}{p^2} \\
&\quad + \tfrac{(1-aa_1)(-2(1+b_1)+4a(a_1+a_1b_1+k_2)+4a^2(k_1-a_1(2a_1+k_2)))}{p} \\
&\quad + p(-3 + 6aa_1 - b_1)(k_1 - a_1k_2)^2 - p^2(k_1 - a_1k_2)^3 \\
\lambda_4 &= -k_2 \\
\lambda_5 &= 1 + 4aa_1(-1 + aa_1) - b_1 + 2p(k_1 - a_1k_2)(1 - 2aa_1) \\
&\quad + p^2(k_1 - a_1k_2)^2 \\
\lambda_6 &= -4ak_1 + 4a^2a_1k_1 - 2k_2 + 8aa_1k_2 - 4a^2(a_1)^2k_2 - \tfrac{4a(1-aa_1)^2}{p} \\
&\quad + p(-ak_1^2 - 2k_1k_2 + 2aa_1k_1k_2 + 2a_1k_2^2 - a(a_1)^2k_2^2)
\end{aligned}$$

By examining the multiplication table we see that all terms with a power of p in the denominator evaluate to an integer because an appropriate power of $(1 - aa_1)$ appears as a factor of the numerator. Note also that once we have that all products $v_2v_i \in R_2$, then it follows that all products $v_3v_i \in R_2$ because $v_3 = v_2^2$ so there is no need to compute the products of v_3. Thus we see that $v_iv_j \in R_2$ for all $1 \leq i, j \leq 6$. Furthermore, the multiplication tables for R_0 and R_1 are easily deduced from the multiplication table for R_2. Examining those multiplication tables reveals that R_0 and R_1 are also both rings, proving (a).

To prove (b), we first note that $v_1, v_2, v_3, pv_6 \in T$ trivially. Thus to show $R_0 \subseteq T$ we just have to write v_4 and pv_5 as polynomials in π and $\bar{\pi}$ with coefficients in $\mathbb{Z}$. The relations $f(\pi) = f(\bar{\pi}) = 0$ and $\pi\bar{\pi} = p$ allow us to write $\bar{\pi}^k$ as a polynomial in $\{1, \pi, \pi^2, \pi^3, \pi^4, \pi^5\}$ with $\mathbb{Q}$-coefficients for $1 \leq k \leq 5$. For v_4 we can easily get that $v_4 = -a - b_1\pi - \bar{\pi}$. For pv_5 we have to solve the linear algebra problem

$$pv_5 = \sum_{i=0}^{5} x_i\pi^i + \sum_{j=1}^{5} y_i\bar{\pi}^j, \qquad x_i, y_j \in \mathbb{Z}.$$

Numerical evidence suggested that x_5, y_2, y_3, y_4 can all be set to 0. This leaves a system of seven variables and six equations. Using the Solve function of a computer algebra system we can solve for all variables in terms of y_5, and then to make the solutions integers we may take $y_5 = (a_1)^3$. This yields the following solution:

$$\begin{aligned}
x_0 &= (a_1)^3 p(-a^3(-2+b_1) + a(1+b_1(-5+2b_1)+ak_2)p - 2b_1k_2p^2) \\
x_1 &= a - 2a^4(a_1)^3 - a^2(a_1)^3(5-5b_1+ak_2)p \\
&\quad -(a_1)^3(-1+b_1^2-2a(-2+b_1)k_2)p^2 - (a_1)^3k_2^2p^3 \\
x_2 &= 1 - (aa_1)^3(-1+b_1) + b_1 + aa_1(-2+(a_1)^2(-1+b_1(-3+2b_1))p) \\
&\quad +p(k_1 - a_1k_2(1+(a_1)^2b_1p)) \\
x_3 &= a^2(a_1)^3(-1+2b_1) + \tfrac{a(1-(aa_1)^3)}{p} - (a_1)^3(b_1+ak_2)p \\
x_4 &= -2a(a_1)^3 + 2a(a_1)^3b_1 + \tfrac{1-(aa_1)^3}{p} - (a_1)^3k_2p \\
y_1 &= -(a_1)^3(a^4 + a^2(4-3b_1)p + (-1+b_1)b_1p^2 + 2ak_2p^2) \\
y_5 &= (a_1)^3
\end{aligned}$$

Thus $R_0 \subseteq T$. To show $T \subseteq R_0$ we note that since R_0 is a ring containing π, it also contains all powers of the π. Thus it suffices to show that $\bar{\pi} \in R_0$. We do this by the simple observation that $\bar{\pi} = -av_1 - b_1v_2 - v_4 \in R_0$. Therefore $T = R_0$. $\square$

Example 5.2. It is not too difficult to find Weil polynomials that satisfy the hypotheses of Theorem 5.1. The following are examples of such polynomials:

$$x^6 + 3x^5 + 5x^4 + 5x^3 + 25x^2 + 75x + 125$$

$$x^6 + 2x^5 - 5x^3 + 50x + 125$$

$$x^6 + x^5 - 15x^3 + 25x + 125$$

$$x^6 + 4x^5 + 7x^4 + 7x^3 + 49x^2 + 196x + 343$$

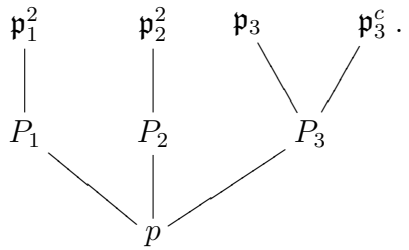
$$x^6 + 6x^5 + 11x^4 + 11x^3 + 121x^2 + 726 + 1331$$

$$x^6 - 4x^5 + 33x^3 - 484 + 1331$$

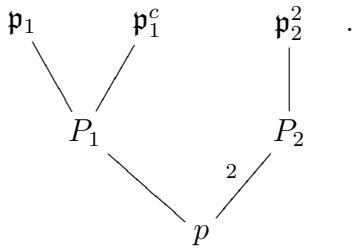
$$x^6 - 5x^5 + 39x^3 - 845 + 2197$$

$$x^6 - 4x^5 + 65x^3 - 676x + 2197$$

Remark 5.3. A natural question is whether p has the same splitting behavior in all these examples. The answer is no, which we can see by examining the first two polynomials in the above example. Let $f_1(x) = x^6+3x^5+5x^4+5x^3+25x^2+75x+125$ and $f_2(x) = x^6+2x^5-5x^3+50x+125$. For $i = 1, 2$, let π_i be a root of f_i, $E_i = \mathbb{Q}(\pi_i)$, and $K_i = \mathbb{Q}(\pi_i + 5/\pi_i)$. Then the splitting of 5 in the tower $E_i - K_i - \mathbb{Q}$ for $i = 1$ is



On the other hand, for $i = 2$ the splitting of 5 is



Example 5.4. It need not be the case that $R_2 = \mathcal{O}_E$. For example, if $p = 7$ and $f(x) = x^6 - 3x^5 + 7x^3 - 147x + 343$, then the hypotheses of Theorem 5.1 are satisfied. However, in this case we get that $[\mathcal{O}_E : \mathbb{Z}[\pi, \bar{\pi}]] = 7^3$ and so R_2 is properly contained in $\mathcal{O}_E$.

Conjecture 5.5. *Let f, T, R_1, and R_2 be as in Theorem 5.1. Then R_1 is the only ring that lies properly between T and R_2.*

This conjecture is based upon numerical evidence. Using the notation of Theorem 5.1 and its proof, let us ask what are the possible subrings that lie between T and R_2. We have that $T = \mathbb{Z}\langle v_1, v_2, v_3, v_4, pv_5, pv_6\rangle$ and $R_2 = \mathbb{Z}\langle v_1, v_2, v_3, v_4, v_5, v_6\rangle$ as $\mathbb{Z}$-modules. Thus the intermediate $\mathbb{Z}$-modules may be enumerated as follows:

$$\begin{aligned} M_i &= \mathbb{Z}\langle v_1, v_2, v_3, v_4, pv_5, iv_5 + v_6\rangle \qquad \text{for } 0 \le i \le p-1 \\ M_p &= \mathbb{Z}\langle v_1, v_2, v_3, v_4, v_5, pv_6\rangle \end{aligned}$$

We want to know which of these $\mathbb{Z}$-modules are actually closed under multiplication. What we will actually do is let S_i be the ring generated by the generators of M_i for $0 \le i \le p$. We then look to see which S_i have the property that $S_i \neq R_2$. This can be done easily with Magma. All of the polynomials listed in Example 5.2 have the property that $S_0 \neq R_2$ and $S_i = R_2$ for $1 \le i \le p$. Evidence like this is the basis for the conjecture.

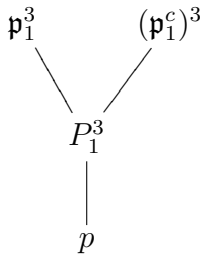
If this conjecture holds, then it may find applications in computing endomorphism rings. If A is an abelian variety satisfying the hypotheses of the conjecture and $[\mathcal{O}_E : T] = p^2$, then $\mathrm{End}_k(A)$ is either T, R_1, or R_2. One might pick an element $r \in R_1$ such that $r \notin T$ and then try to see if r is an endomorphism of A. If it is not, then $\mathrm{End}_k(A) = T$. Otherwise, pick a new r such that $r \in R_2$, $r \notin R_1$ and then test to see if r is an endomorphism of A. If it is not, then $\mathrm{End}_k(A) = R_1$, otherwise $\mathrm{End}_k(A) = R_2$.

Appendix A

Splitting of p

Let A be an absolutely simple abelian variety defined over $k = \mathbb{F}_p$ with commutative endomorphism ring. Let f be the characteristic polynomial of Frobenius, π a root of f, $\beta = \pi + \bar{\pi}$, $E = \mathbb{Q}(\pi)$, and $K = \mathbb{Q}(\beta)$. In this appendix we work out all possible cases for the splitting behavior of p in the tower of fields $\mathbb{Q} \subset K \subset E$ for abelian 3- and 4-folds. For each type of splitting, we give the possible factorizations of the principal ideal (π). It is then possible to apply Theorem 3.6 to find $r(A)$.

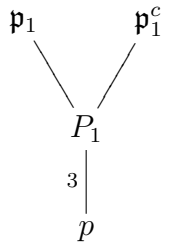
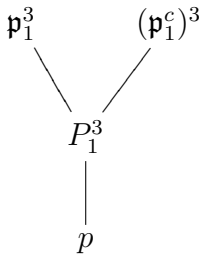
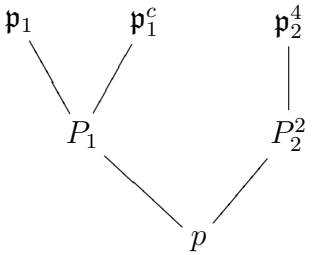
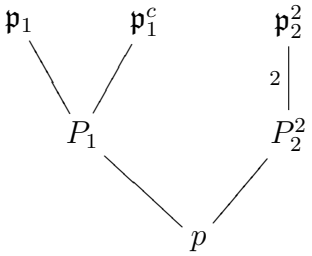
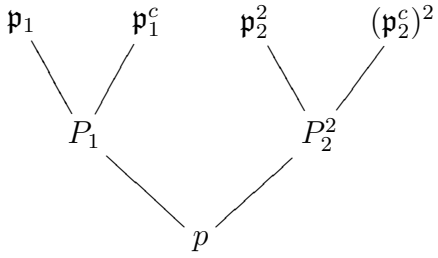
The tables are organized into three columns. The first column is a diagram showing the way that p splits in the tower of fields. The second column contains all possible factorizations of (π) for that particular diagram, and the last column gives the value of $r(A)$ for the given factorization of (π). For example, one row of the table reads

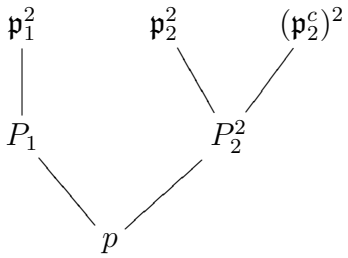
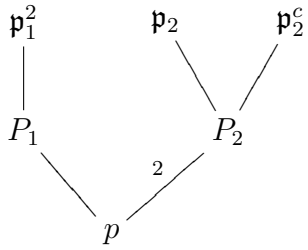
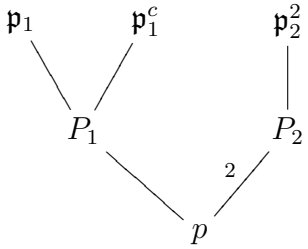
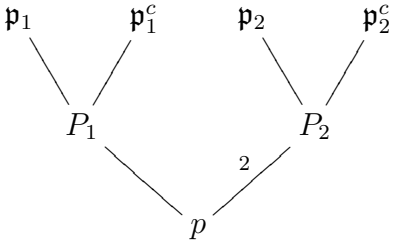
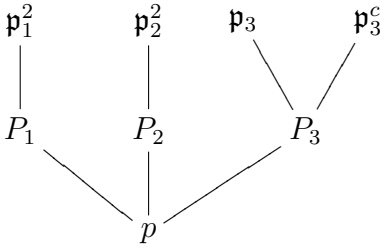
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^3$	3
	$\mathfrak{p}_1^2\mathfrak{p}_1^c$	0

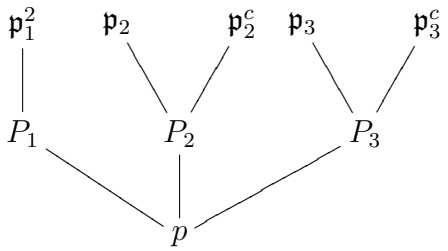
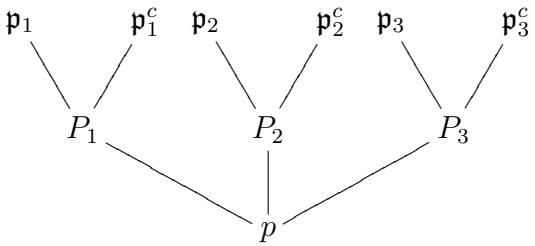
The diagram tells us that $p\mathcal{O}_K = P_1^3$, so p is totally ramified in K. We then get that $P_1\mathcal{O}_E = \mathfrak{p}_1\mathfrak{p}_1^c$, hence P_1 splits in E. There are two possible ways that (π)

might factor in E. One possibility is that $(\pi) = \mathfrak{p}_1^3$. By using Theorem 3.6 we then get that $r(A) = 3$ hence A is ordinary. The other possibility is that $(\pi) = \mathfrak{p}_1^2\mathfrak{p}_1^c$. In this case, we get that $r(A) = 0$. However, we also see that $(\pi) \neq (\bar{\pi})$ hence A is not supersingular.

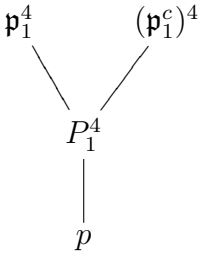
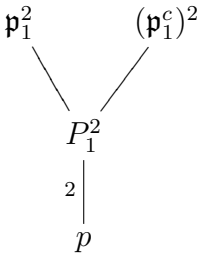
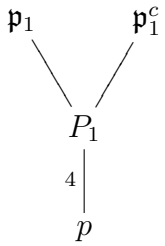
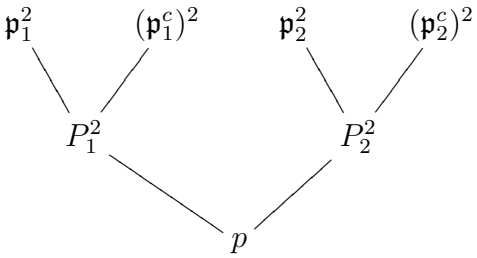
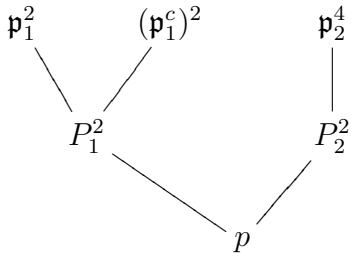
1.1 3-folds

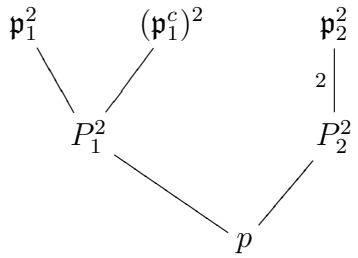
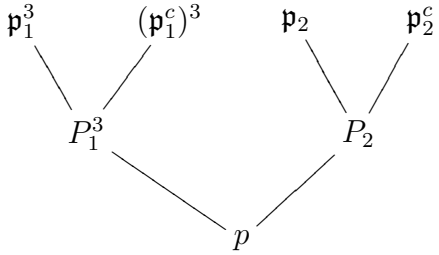
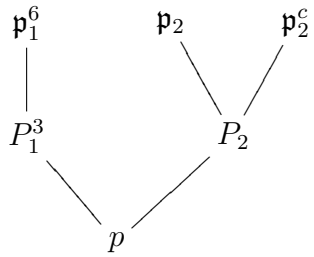
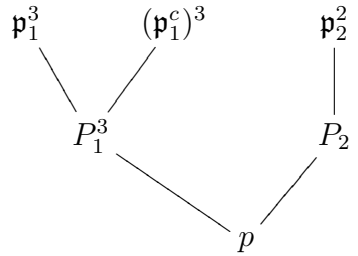
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1$	3
	$\mathfrak{p}_1^3$	3
	$\mathfrak{p}_1^2\mathfrak{p}_1^c$	0
	$\mathfrak{p}_1\mathfrak{p}_2^2$	1
	$\mathfrak{p}_1\mathfrak{p}_2$	1
	$\mathfrak{p}_1\mathfrak{p}_2^2$	3
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_2^c$	1

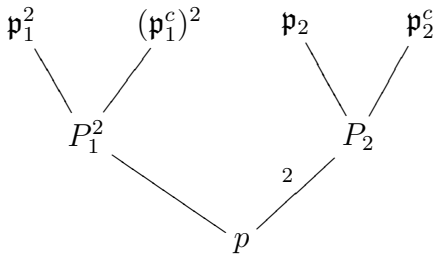
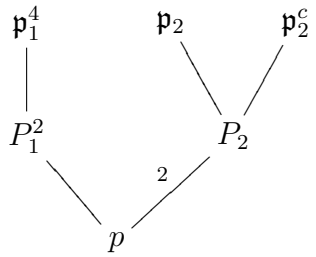
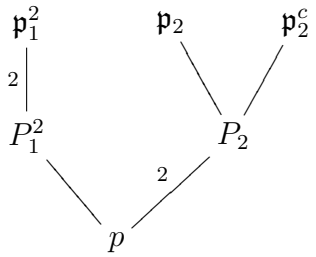
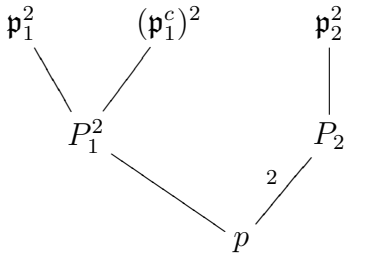
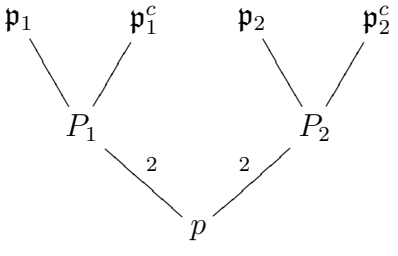
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1\mathfrak{p}_2^2$	2
	$\mathfrak{p}_1\mathfrak{p}_2$	2
	$\mathfrak{p}_1\mathfrak{p}_2$	1
	$\mathfrak{p}_1\mathfrak{p}_2$	3
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1

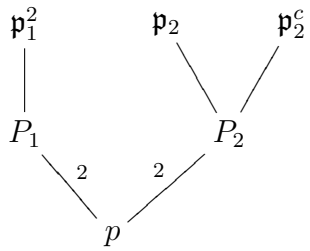
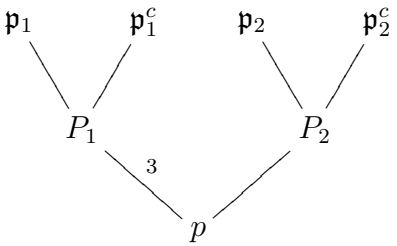
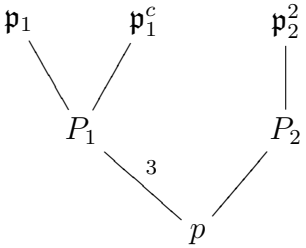
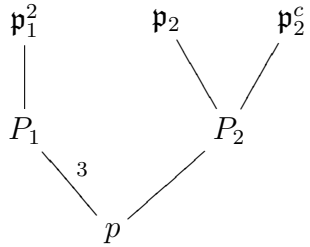
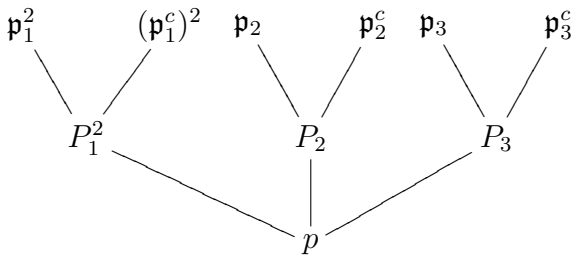
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	3

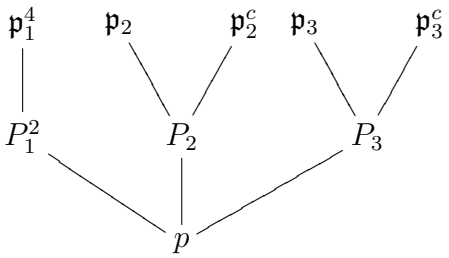
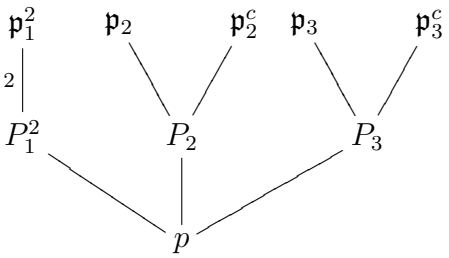
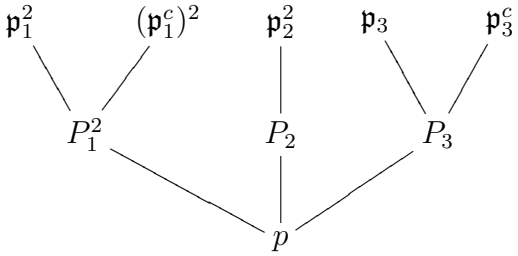
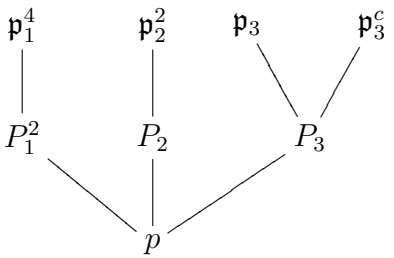
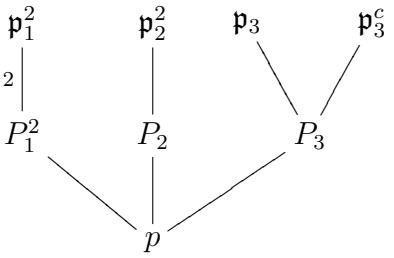
1.2 4-folds

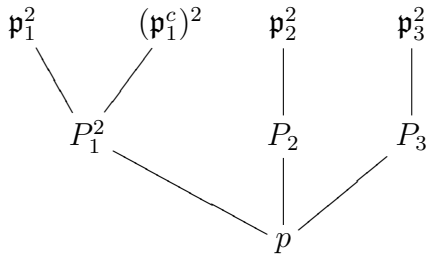
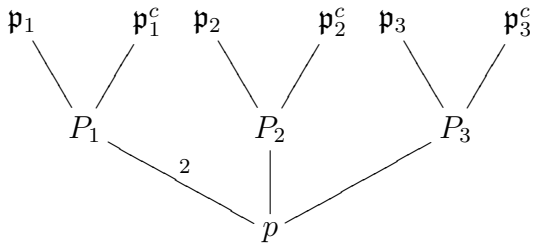
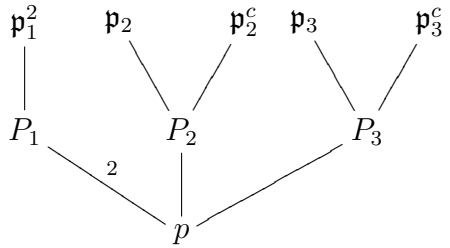
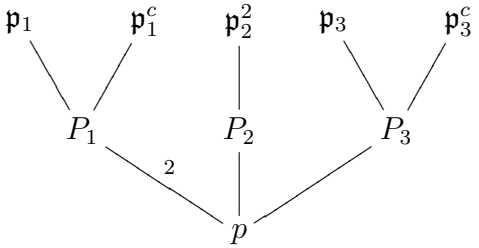
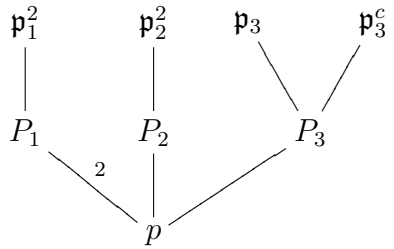
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^4$	4
	$\mathfrak{p}_1^3\mathfrak{p}_1^c$	0
	$\mathfrak{p}_1^2$	4
	$\mathfrak{p}_1$	0
	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	4
	$\mathfrak{p}_1\mathfrak{p}_1^c\mathfrak{p}_2^2$	2
	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	2

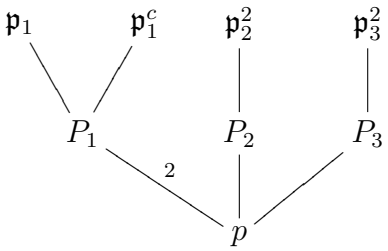
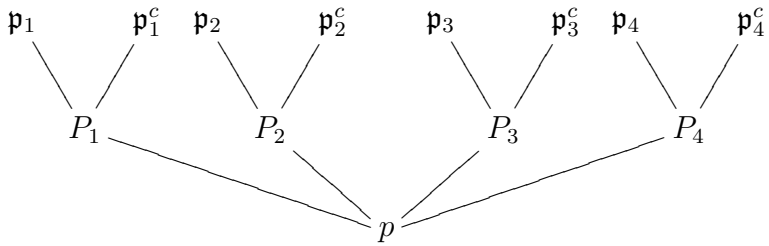
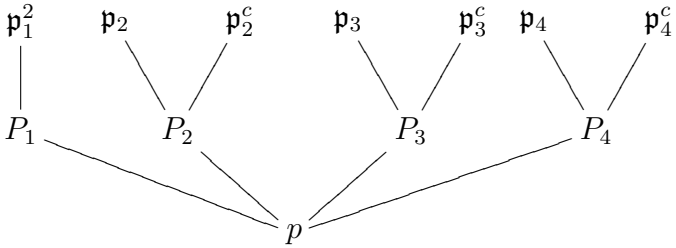
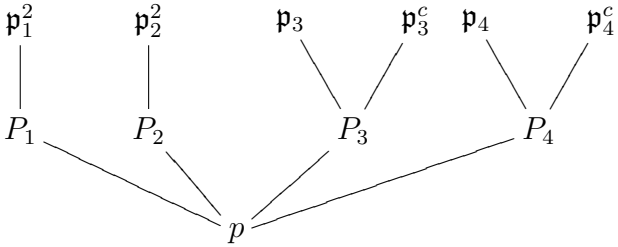
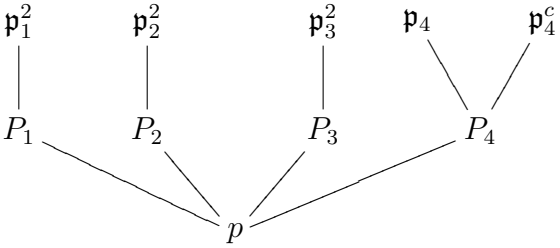
splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^2\mathfrak{p}_2$	2
	$\mathfrak{p}_1^3\mathfrak{p}_2$	4
	$\mathfrak{p}_1^2\mathfrak{p}_1^c\mathfrak{p}_2$	1
	$\mathfrak{p}_1^3\mathfrak{p}_2$	1
	$\mathfrak{p}_1^3\mathfrak{p}_2$	3
	$\mathfrak{p}_1^2\mathfrak{p}_1^c\mathfrak{p}_2$	0

splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^2\mathfrak{p}_2$	4
	$\mathfrak{p}_1\mathfrak{p}_1^c\mathfrak{p}_2$	2
	$\mathfrak{p}_1^2\mathfrak{p}_2$	2
	$\mathfrak{p}_1\mathfrak{p}_2$	2
	$\mathfrak{p}_1^2\mathfrak{p}_2$	2
	$\mathfrak{p}_1\mathfrak{p}_2$	4

splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1\mathfrak{p}_2$	2
	$\mathfrak{p}_1\mathfrak{p}_2$	4
	$\mathfrak{p}_1\mathfrak{p}_2$	3
	$\mathfrak{p}_1\mathfrak{p}_2$	1
	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ $\mathfrak{p}_1\mathfrak{p}_1^c\mathfrak{p}_2\mathfrak{p}_3$	4 2

splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	3
	$\mathfrak{p}_1\mathfrak{p}_1^c\mathfrak{p}_2\mathfrak{p}_3$	1
	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	1
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1

splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	4
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	3
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1

splitting of p	factorization of (π)	$r(A)$
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	4
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	3
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	2
	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	1

Bibliography

[1] Kristen Eisentrager and Kristin Lauter. A crt algorithm for construction genus 2 curves over finite fields. In *Arithmetic, Geometry, and Coding Theory (AGCT - 10)*, Séminaires et Congrès 21, pages 161–176. Société Mathématique de France, 2009.

[2] David Freeman and Kristin Lauter. Computing endomorphism rings of jacobians of genus 2 curves over finite fields. In *Algebraic Geometry and its Applications*, Ser. Number Theory Appl., 5, pages 29–66. World Sci. Publ., Hackensack, NJ, 2008.

[3] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkley, December 1996.

[4] Andrew V. Sutherland. On the evaluation of modular polynomials. arXiv: 1202.3985 [math.NT], 2012.

[5] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 113:815–831, 2011.

[6] William C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. Ec. Norm. Sup.*, pages 521–560, 1969.

[7] Alexey Zaytsev. Generalizations of deuring reduction theorem. arXiv: 1209.5207v1 [math.AG], 2012.

[8] Tetsuo Nakamura. A note on endomorphism rings of abelian varieties over finite fields. *Kodai Math. J.*, 2:123–129, 1979.

[9] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[10] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2:134–144, 1966.

[11] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini. In *Séminaire N. Bourbaki*, 352, pages 95–110, 1968-1969.

[12] J.S. Milne. Class field theory (v4.00), 2008. Available at www.jmilne.org/math/.

[13] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, New York, NY, 2 edition, 1984.

[14] Josep Gonzalez. On the p-rank of an abelian variety and its endomorphism algebra. *Publicacions Matematiques*, 42:119–130, 1998.

[15] F. Oort. Subvarieties of moduli spaces. *Invent. Math.*, 24:95–119, 1974.

[16] Serge Lang. *Algebraic Number Theory*. Springer-Verlag, New York, NY, 2 edition, 1994.

[17] Hans-Georg Rück. Abelian surfaces and jacobian varieties over finite fields. *Compositio Mathematica*, 76:351–366, 1990.

[18] Safia Haloui. The characteristic polynomial of abelian varieties of dimension 3 over finite fields. arXive: 1003.0374v2 [math.AG], 2010.

[19] C. P. Xing. The characteristic polynomial of abelian varieties of dimensions three and four over finite fields. *Science in China*, 37(2):147–150, 1994.

[20] Safia Haloui and Vijaykumar Sing. The characteristic polynomials of abelian varieties of dimenions 4 over finite fields. arXiv: 1101.5070v1 [math.AG], 2011.

[21] Jürgen Neukirch. *Algebraic Number Theory*. Springer, New York, NY, 1999.

[22] J. .W. S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Thompson Book Company Inc., Washington, D.C., 1967.