University of Groningen

Master Thesis Mathematics

Classifying abelian threefolds of p-rank 0, 1, 2 and 3

July 20, 2021

Author:
Floor Dogger

First supervisor:
Pınar Kılıçer

Second assessor:
Jaap Top

Abstract

The aim of the thesis is to find relations between the endomorphism algebra, the p-rank and the factorization of the rational prime p into prime ideals in the number field generated by the Frobenius endomorphism for abelian threefolds over finite fields of characteristic p. For elliptic curves and abelian surfaces, these relations are discussed in Chapter 1 and Chapter 2. The main theorem follows in Chapter 3 and gives a complete classification of the p-rank in terms of the splitting behaviour of the rational prime p in the maximal order of the number field generated by the Frobenius endomorphism of an absolutely simple abelian threefold over a finite field of characteristic p. In Chapter 4, the reduction of absolutely simple CM abelian threefolds is studied. Only abelian threefolds with CM by a CM field of which the Galois group of the normal closure is cyclic or isomorphic to the dihedral group D_6 are considered. For both options, the endomorphism algebra and the p-rank of the reduced CM abelian threefold is determined from the prime factorization of a rational prime p in the ring of integers of the CM field.

Contents

List of Notation

k	a field
E/k	an elliptic curve defined over k
S/k	an abelian surface defined over k
A/k	an abelian threefold/variety defined over k
$\overline{k}$	an algebraic closure of k
$\mathrm{End}_k(A)$	the endomorphism ring of A over k
$\mathrm{End}(A)$	the endomorphism ring of A over the algebraic closure
$\mathrm{End}_k^0(A)$	the endomorpism algebra over k
$\mathrm{End}^0(A)$	the endomorphism algebra over the algebraic closure
$B_{p,\infty}$	a quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞
$A(k)[p]$	the group of p-torsion points of A over the field k
Tr	the trace on $\mathrm{End}(E)$
f_A	the characteristic polynomial of the Frobenius endomorphism of A
π_A	a root of the characteristic polynomial of the Frobenius endomorphism of A or the Frobenius endomorphism of A
$\overline{\pi}_A$	the complex conjugate of π_A

$\widehat{\phi}$	the dual isogeny to ϕ
ϕ^*	a map of function fields induced by the rational map of curves
$r(A)$	the p-rank of A
$e(\mathfrak{p})$	the ramification index of $\mathfrak{p}$
$f(\mathfrak{p})$	the residual degree of $\mathfrak{p}$
$A_1 \sim A_2$	A_1 and A_2 are isogenous
$\mathcal{Z}(\mathrm{End}^0(A))$	the center of $\mathrm{End}^0(A)$
$\mathcal{D}_A$	a central simple algebra over $\mathbb{Q}(\pi_A)$ which splits at all finite primes of $\mathbb{Q}(\pi_A)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_A)$
K	a number field
$\mathcal{O}_K$	the ring of integers of K
K_+	the subfield of K fixed by complex conjugation
K'	the Galois closure of K
$\mathrm{Np}_p(f)$	the Newton polygon of a polynomial f with respect to a prime p
$i_{\mathfrak{p}}$	the invariant of $\mathrm{End}^0_{\mathbb{F}_q}(A)$ at the prime $\mathfrak{p}$
$N_{K/\mathbb{Q}}$	the norm from K to $\mathbb{Q}$
D_6	the dihedral group with 12 elements
(K, Φ)	a CM type
(K^r, Φ^r)	the reflex CM type of a CM type (K, Φ)
N_Φ	the type norm of a CM type (K, Φ)
N_{Φ^r}	the type norm of a reflex CM pair (K^r, Φ^r)

Introduction

An elliptic curve is a nonsingular projective curve (variety of dimension $g = 1$) together with a group structure defined by regular maps. A rational map $\phi : E_1 \to E_2$ between two elliptic curves E_1 and E_2 that is regular at every point is called a *morphism*. If ϕ satisfies $\phi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ denotes the point at infinity, then ϕ is an *isogeny*. Isogenies from an elliptic curve to itself are called *endomorphisms*. If E is an elliptic curve over a field k, then the set $\mathrm{End}_k(E)$ of all endomorphisms of E defined over k forms a ring called the *endomorphism ring* of E. The set of all endomorphisms of E defined over the algebraic closure $\overline{k}$ is also a ring and is denoted by $\mathrm{End}(E)$. The *endomorphism algebra* of an elliptic curve E over k or $\overline{k}$ is defined as $\mathrm{End}_k^0(E) \coloneqq \mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ or $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ respectively.

We are interested in elliptic curves over finite fields. An important endomorphism of an elliptic curve E defined over a finite field $\mathbb{F}_q$ is the *Frobenius endomorphism* $\pi_E : E \to E$ given by $(x, y, z) \mapsto (x^q, y^q, z^q)$. The Frobenius endomorphism satisfies

$$\pi_E^2 - t\pi_E + q = 0$$

in $\mathrm{End}(E)$, see Silverman [19, Theorem V.2.3.1(b)], where t is the trace of the Frobenius endomorphism π_E. The polynomial

$$f_E = X^2 - tX + q \in \mathbb{Z}[X]$$

is called the *characteristic polynomial of the Frobenius endomorphism*. By abuse of notation, we let $\pi_E \in \mathbb{C}$ also denote a root of f_E. By Hasse's theorem [19, Theorem V.1.1], the number field $\mathbb{Q}(\pi_E)$ satisfies $\mathbb{Q}(\pi_E) = \mathbb{Q}$ or $\mathbb{Q}(\pi_E)$ is an imaginary quadratic field. If $\mathbb{Q}(\pi_E^r)$ is an imaginary quadratic field for all integers $r > 0$, then we call E ordinary. Otherwise, we say that E is supersingular. We will see in Chapter 1 that $E/\mathbb{F}_q$ is supersingular if and only if the endomorphism algebra $\mathrm{End}^0(E)$ is isomorphic to a quaternion algebra, and ordinary if and only if $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $\mathbb{Q}(\pi_E)$, see [19, Theorem V.3.1].

The *m-torsion subgroup* $E(\overline{\mathbb{F}_q})[m]$ of an elliptic curve $E/\mathbb{F}_q$ is the set of points of E of order m. The *p-rank* of $E/\mathbb{F}_q$, with $q = p^n$, is the integer $r = r(E)$ such that $E(\overline{\mathbb{F}_q})[p]$ has order p^r. As $E(\overline{\mathbb{F}_q})[p]$ is isomorphic to $\{\mathcal{O}\}$ or $\mathbb{Z}/p\mathbb{Z}$ by Silverman [19, Corollary III.6.4(c)], the p-rank of E is 0 or 1 respectively. In Chapter 1 we will see that $r(E) = 0$ if and only if $E/\mathbb{F}_q$ is supersingular and $r(E) = 1$ if and only if $E/\mathbb{F}_q$ is ordinary [19, Theorem V.3.1]. If $E/\mathbb{F}_q$, where $q = p^n$, is ordinary, then $\mathbb{Q}(\pi_E)$ is an imaginary quadratic field. If in addition $\mathrm{End}(E)$ is isomorphic to the ring of integers of the field $\mathbb{Q}(\pi_E)$, then the ideal (p) splits in $\mathcal{O}_{\mathbb{Q}(\pi_E)}$. This will be the subject of Section 1.3.

Similar to what we did for elliptic curves, the aim of the thesis is to find relations between the endomorphism algebra, the p-rank and the factorization of the rational prime p into prime ideals in the number field generated by the Frobenius endomorphism for abelian threefolds $A/\mathbb{F}_q$. An abelian threefold is an *abelian variety*, a nonsingular connected projective variety with a group structure defined by regular maps, of dimension $g = 3$. Many notions we know for elliptic curves transfer to abelian varieties. A rational map $\phi : A_1 \to A_2$ between two abelian varieties of dimension g that is regular at every point is called a *morphism*. A surjective homomorphism with a finite kernel between two abelian varieties with the same dimension is called an *isogeny*. If A is an abelian variety over a field k, then the set $\mathrm{End}_k(A)$ of all endomorphisms of A defined over k forms a ring called the *endomorphism ring* of A. The set of all endomorphisms of A defined over the algebraic closure $\overline{k}$ is also a ring and is denoted by $\mathrm{End}(A)$. The *endomorphism algebra* of A over k or $\overline{k}$ is defined as $\mathrm{End}_k^0(A) \coloneqq \mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ or $\mathrm{End}^0(A) \coloneqq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ respectively.

Again, we are interested in abelian varieties over finite fields. An important endomorphism of an abelian variety A defined over a finite field $\mathbb{F}_q$ is the *Frobenius endomorphism* $\pi_A : A \to A$ induced by the q-th power Frobenius automorphism of the field $\overline{\mathbb{F}_q}$. By Milne [14, Theorem 10.9], there is a unique polynomial $f_A \in \mathbb{Z}[X]$ of degree $2g$, where g is the dimension of A, such that $f_A(t) = \deg(\pi_A - t)$ for all $t \in \mathbb{Z}$. This polynomial f_A is called the *characteristic polynomial of the Frobenius endomorphism*. In dimension $g = 1$, this definition coincides with the definition of the characteristic polynomial of the Frobenius endomorphism of an elliptic curve. If f_A is a power of an irreducible polynomial, we let $\pi_A \in \mathbb{C}$ also denote a root of f_A. We can therefore talk about the number field $\mathbb{Q}(\pi_A)$ generated by the Frobenius endomorphism. The *p-rank* of an abelian variety $A/\mathbb{F}_{p^n}$ is the integer $r = r(A)$ such that the group $A(\overline{\mathbb{F}_{p^n}})[p]$ has order p^r. The p-rank satisfies $0 \leq r(A) \leq g$.

An abelian variety $A/\mathbb{F}_q$ can be isogenous (either over $\mathbb{F}_q$ or $\overline{\mathbb{F}_q}$) to a product of lower dimensional abelian varieties. If A is not $\mathbb{F}_q$-isogenous to a product of lower dimensional abelian varieties, we call A *simple*. If A is simple over the algebraic closure $\overline{\mathbb{F}_q}$, then A is called *absolutely simple*. If an abelian variety is not absolutely simple, then the

endomorphism algebra and the p-rank can be deduced from the endomorphism algebras and p-ranks of the lower dimensional abelian varieties, see Milne [14, p.43]. Therefore, we are mostly interested in absolutely simple abelian varieties.

In Section 2.1, we discuss abelian surfaces over finite fields, which are abelian varieties of dimension $g = 2$. We summarize the relations between the endomorphism algebra, the p-rank and the factorization of the rational prime p into prime ideals in $\mathbb{Q}(\pi_S)$ for an abelian surface $S/\mathbb{F}_{p^n}$, see Gonzalez [7, Theorem 3.7(ii)] and Bradford [2, Example 3.9]. After this short intermezzo we move on to abelian threefolds in Chapter 3.

Chapter 3 starts by describing the possible characteristic polynomials of the Frobenius endomorphism and endomorphism algebras of abelian threefolds. Then we discuss the relation between Newton polygons and the p-rank of an abelian threefold in Section 3.2. The main result follows in Section 3.3.1 and gives a complete classification of the p-rank in terms of the splitting behaviour of the rational prime p in the maximal order of the number field $\mathbb{Q}(\pi_A)$ of an absolutely simple abelian threefold $A/\mathbb{F}_{p^n}$.

The final chapter is about reductions of CM abelian threefolds over a number field k modulo prime ideals in k. An abelian threefold A has *complex multiplication* (CM) by a CM field K if K has degree six and there is an embedding $\theta : K \hookrightarrow \mathrm{End}^0(A)$. Furthermore, if $\theta^{-1}(\mathrm{End}(A)) = \mathcal{O}$ for an order $\mathcal{O} \subset K$, then we say that A has CM by the order $\mathcal{O}$. A *CM field* is a totally imaginary quadratic extension of a totally real number field. Up to isomorphisms, there are four different options for the Galois group of the normal closure of a sextic CM field, see Dodson [5]. We restrict to sextic CM fields of which the Galois group of the normal closure is cyclic or isomorphic to the dihedral group D_6. For any CM abelian variety A over a number field k, there exists a cyclic extension of k over which A acquires good reduction everywhere by Serre-Tate [16, Theorem 7]. We can therefore assume without loss of generality, that a CM abelian threefold A/k has good reduction everywhere. By reducing a CM abelian threefold A over a number field k modulo a prime $\wp$ in the ring of integers of k, we obtain the reduction $\overline{A} = A \mod \wp$ defined over the finite field $\mathbb{F}_q$, where $q = |\mathcal{O}_k/\wp|$. Assuming that A has good reduction at $\wp$, the reduction $\overline{A}$ defines an abelian threefold over a finite field. If an absolutely simple abelian threefold A over a number field k has CM by $\mathcal{O}_K$ for a sextic cyclic CM field K and $\wp \in \mathcal{O}_k$ is a prime lying over a rational prime p, then the splitting behaviour of p in $\mathcal{O}_K$ completely determines the endomorphism algebra and p-rank of $\overline{A} = A \mod \wp$, see Kılıçer, Labrande, Lercier, Ritzenthaler, Sijsling and Streng [12, Proposition 4.1]. Chapter 4 ends with an example of an abelian threefold A over a number field k with CM by a sextic CM field of which the Galois group of the normal closure is isomorphic to D_6. We look at the reduction $\overline{A} = A \mod \wp$ for primes $\wp \subset \mathcal{O}_k$ lying over small rational primes p, and compute the endomorphism algebra $\mathrm{End}^0(\overline{A})$ and the p-rank $r(\overline{A})$ using the factorization of $p\mathcal{O}_K$ into prime ideals.

Chapter 1

Elliptic curves

In this chapter, we describe the relations between the endomorphism algebra, the p-rank and the factorization of the rational prime p into prime ideals in $\mathbb{Q}(\pi_E)$ for an elliptic curve $E/\mathbb{F}_{p^n}$. These relations are well-known and can be found in Silverman [19]. We start in the next section by providing the necessary background of elliptic curves.

1.1 Background

An *elliptic curve* E is a nonsingular projective curve together with a group structure defined by regular maps. We consider elliptic curves over a field k. Such an elliptic curve is denoted by E/k. The maps between elliptic curves that we are interested in are called isogenies. Isogenies are a special type of morphisms. A *morphism* $\phi : E_1 \to E_2$ between two elliptic curves E_1 and E_2 is a rational map that is regular at every point. The set of morphisms between two elliptic curves coincides with the rational maps between those curves.

Definition 1.1. Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a surjective morphism

$$\phi : E_1 \to E_2 \quad \text{satisfying} \quad \phi(\mathcal{O}) = \mathcal{O},$$

where $\mathcal{O}$ denotes the identity element under the elliptic curve group law (the point at infinity). We call E_1 and E_2 *isogenous* if there exists an isogeny between E_1 and E_2.

Definition 1.2. Let $\phi : E_1 \to E_2$ be an isogeny between two elliptic curves E_1 and E_2 of degree m. Then the *dual isogeny* of ϕ is the unique isogeny $\widehat{\phi} : E_2 \to E_1$ satisfying $\widehat{\phi} \circ \phi = [m]$.

It follows from Silverman [19, Theorem II.2.3] that a morphism ϕ from E_1 to E_2 satisfies either $\phi(E_1) = \{\mathcal{O}\}$ or $\phi(E_1) = E_2$. In the first case, the morphism ϕ sends every point on E_1 to the identity element $\mathcal{O}$ of E_2. This morphism is called the *zero morphism* and is denoted by $[0]$. In the second case, the morphism ϕ is surjective and hence an isogeny from E_1 to E_2. Thus, every morphism between two elliptic curves is an isogeny, except the zero morphism.

Let E_1/k and E_2/k be two elliptic curves. We can distinguish between isogenies defined over k and isogenies defined over the algebraic closure $\overline{k}$. If there exists an isogeny defined over k from E_1 to E_2, then the elliptic curves E_1 and E_2 are called *k-isogenous*. If the isogeny from E_1 to E_2 is defined over the algebraic closure $\overline{k}$, then E_1 and E_2 are called *$\overline{k}$-isogenous*.

The points on an elliptic curve form an abelian group. Isogenies are group homomorphisms acting on this abelian group, see Silverman [19, Theorem III.4.8]. We will be mostly interested in morphisms from an elliptic curve E/k to itself. These maps are called *endomorphisms*. The set of all endomorphisms of E defined over k is an abelian group with the zero morphism as the unit element. The sum of two endomorphisms is defined pointwise

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

The multiplication law is given by composition

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

The zero morphism is also the multiplicative unit element. As endomorphisms are group homomorphisms acting on the points of an elliptic curve, distributivity follows

$$\begin{aligned}\phi \circ (\psi + \varphi)(P) &= \phi(\psi(P) + \varphi(P)) \\ &= \phi(\psi(P)) + \phi(\varphi(P)) \\ &= (\phi \circ \psi)(P) + (\phi \circ \varphi)(P) \\ &= (\phi \circ \psi + \phi \circ \varphi)(P).\end{aligned}$$

In a similar way, right distributivity can be proven.

Definition 1.3. Let E/k be an elliptic curve. The set of all endomorphisms of E defined over k is called the *endomorphism ring* of E and is denoted by $\mathrm{End}_k(E)$.

The endomorphisms of E defined over the algebraic closure $\overline{k}$ form a ring as well, which we denote by $\mathrm{End}(E)$. This ring will also be called the endomorphism ring of E.

A particular subring of $\mathrm{End}_k(E)$ is given by the multiplication-by-n maps $[n]$, for any integer n. Such an endomorphism $[n] : E \to E$ is given by

$$[n](P) = \underbrace{P + \cdots + P}_{n \text{ terms}}.$$

Note that the zero morphism [0], sending everything to the identity element, is an endomorphism of this form. The set $\{[n] : n \in \mathbb{Z}\}$ forms a subring of $\mathrm{End}_k(E)$ isomorphic to $\mathbb{Z}$. We identify $\{[n] : n \in \mathbb{Z}\}$ with $\mathbb{Z}$ and say that $\mathbb{Z} \subseteq \mathrm{End}_k(E)$.

Definition 1.4. The *endomorphism algebra* of E/k over the base field k is $\mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ and is denoted by $\mathrm{End}_k^0(E)$. Over the algebraic closure $\overline{k}$, the endomorphism algebra is $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ and is denoted by $\mathrm{End}^0(E)$.

We will see that up to isomorphism there are only three options for the endomorphism algebra $\mathrm{End}^0(E)$ of an elliptic curve E over an arbitrary field k. One of the options is that $\mathrm{End}^0(E)$ is isomorphic to a quaternion algebra.

Definition 1.5. A *quaternion algebra* B over $\mathbb{Q}$ is a $\mathbb{Q}$-algebra that has a basis of the form $\{1, \alpha, \beta, \alpha\beta\}$, with

$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \beta\alpha = -\alpha\beta.$$

A quaternion algebra B is *ramified at* p if $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra. If $B \otimes_{\mathbb{Q}} \mathbb{R}$ is a division algebra, we say B is *ramified at* ∞.

We define $B_{p,\infty}$ to be the quaternion algebra over $\mathbb{Q}$ ramifying only at p and ∞.

The complete set of options for the endomorphism algebra of an elliptic curve is described in the following theorem by Silverman.

Theorem 1.6 ([19, Corollary III.9.4])**.** Let E be an elliptic curve over an arbitrary field k. Then $\mathrm{End}^0(E)$ is isomorphic to one of

(i) the field of rational numbers $\mathbb{Q}$,

(ii) an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}_{<0}$,

(iii) the quaternion algebra $B_{p,\infty}$.

The endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E/k is a full rank $\mathbb{Z}$-module contained in the endomorphism algebra $\mathrm{End}^0(E)$. Explicitly, if $\mathrm{End}^0(E) \cong \mathbb{Q}$, then we have $\mathrm{End}(E) \cong \mathbb{Z}$, if $\mathrm{End}^0(E) \cong \mathbb{Q}(\sqrt{-d})$, then $\mathrm{End}(E)$ is isomorphic to an order in $\mathbb{Q}(\sqrt{-d})$, and if $\mathrm{End}^0(E) \cong B_{p,\infty}$, then $\mathrm{End}(E)$ is a $\mathbb{Z}$-module of rank 4 in $B_{p,\infty}$.

Definition 1.7. An elliptic curve E has *complex multiplication* (CM) if $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field.

An important endomorphism of an elliptic curve E defined over a finite field $\mathbb{F}_q$ is the Frobenius endomorphism.

Definition 1.8. Let $E/\mathbb{F}_q$ be an elliptic curve. The endomorphism given by

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

is called the *Frobenius endomorphism* of E.

Definition 1.9. The *trace* of an endomorphism $\phi \in \mathrm{End}(E)$ is $\mathrm{Tr}(\phi) = \phi + \widehat{\phi}$.

The Frobenius endomorphism π_E satisfies

$$\pi_E^2 - \mathrm{Tr}(\pi_E)\pi_E + q = 0,$$

see Silverman [19, Theorem V.2.3.1(b)], where $\mathrm{Tr}(\pi_E)$ (see Definition 1.9), and q and 0 are seen as elements in $\mathbb{Z} \subset \mathrm{End}(E)$. This leads to the following definition.

Definition 1.10. The polynomial $f_E = X^2 - tX + q$ is called the *characteristic polynomial of Frobenius*. Here t is the trace of the Frobenius endomorphism π_E.

By abuse of notation, we let $\pi_E \in \mathbb{C}$ also denote a root of f_E, so

$$\pi_E = \frac{t \pm \sqrt{t^2 - 4q}}{2}.$$

Let $m \in \mathbb{Z}_{>0}$. The *m-torsion subgroup* of an elliptic curve $E/\overline{\mathbb{F}_q}$ is the set of points of E of order m and is denoted by $E(\overline{\mathbb{F}_q})[m]$. The m-torsion subgroup is equal to the kernel of the multiplication-by-m map $[m]$. The structure of the m-torsion group is given in the following theorem by Silverman.

Theorem 1.11. ([19, Corollary III.6.4(b),(c)]) Let $E/\mathbb{F}_q$, with $q = p^n$, be an elliptic curve and let $m \in \mathbb{Z}$, $m \neq 0$.

(i) If m and p are coprime, then $E(\overline{\mathbb{F}_q})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(ii) Otherwise $E(\overline{\mathbb{F}_q})[p^e] \cong \begin{cases} \{\mathcal{O}\} & \text{for all } e = 1, 2, 3, \ldots \quad \text{or} \\ \mathbb{Z}/p^e\mathbb{Z} & \text{for all } e = 1, 2, 3, \ldots \end{cases}$

Definition 1.12. The *p-rank* of an elliptic curve E over a finite field $\mathbb{F}_q$, with $q = p^n$, is the integer $r = r(E)$ such that the group $E(\overline{\mathbb{F}_q})[p]$ has order p^r.

Remark 1.13. If E is an elliptic curve over the field $\mathbb{F}_q$ with $q = p^n$, then

$$E(\overline{\mathbb{F}_q})[p] = \begin{cases} \{\mathcal{O}\} & \text{or} \\ \mathbb{Z}/p\mathbb{Z}, \end{cases}$$

by Theorem 1.11. Hence, $E(\overline{\mathbb{F}_q})[p]$ has order $1 = p^0$ or order $p = p^1$. Thus, the p-rank of E is either 0 or 1.

Proposition 1.14. Let $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ be elliptic curves and let $\phi : E_1 \to E_2$ be an isogeny defined over $\overline{\mathbb{F}_q}$. Then $r(E_1) = r(E_2)$.

Proof. Let $Q \in E_1(\overline{\mathbb{F}_q})[p]$ be arbitrary. Then we have $pQ = \mathcal{O}_1$, where $\mathcal{O}_1$ denotes the identity element of E_1. Since ϕ is an isogeny, and thus a homomorphism, it holds that

$$\mathcal{O}_2 = \phi(\mathcal{O}_1) = \phi(pQ) = p\phi(Q),$$

where $\mathcal{O}_2$ is the identity element of E_2. This implies that $\phi(Q) \in E_2(\overline{\mathbb{F}_q})[p]$. Hence, we have

$$p^{r(E_1)} = |E_1(\overline{\mathbb{F}_q})[p]| \geq |E_2(\overline{\mathbb{F}_q})[p]| = p^{r(E_2)},$$

because ϕ is surjective. It follows that $r(E_1) \geq r(E_2)$.

Let $\widehat{\phi} : E_2 \to E_1$ be the dual isogeny of ϕ. Let $Q \in E_2(\overline{\mathbb{F}_q})[p]$ be arbitrary. Then we have $pQ = \mathcal{O}_2$. Since $\widehat{\phi}$ is an isogeny, and thus a homomorphism, it holds that

$$\mathcal{O}_1 = \widehat{\phi}(\mathcal{O}_2) = \widehat{\phi}(pQ) = p\widehat{\phi}(Q).$$

This implies that $\widehat{\phi}(Q) \in E_1(\overline{\mathbb{F}_q})[p]$. Hence, we have

$$p^{r(E_2)} = |E_2(\overline{\mathbb{F}_q})[p]| \geq |E_1(\overline{\mathbb{F}_q})[p]| = p^{r(E_1)},$$

because $\widehat{\phi}$ is surjective. It follows that $r(E_2) \geq r(E_1)$. This proves $r(E_1) = r(E_2)$. □

In the remaining of this chapter, elliptic curves over finite fields of characteristic p are studied. We will specify and prove under which conditions the endomorphism algebra of an elliptic curve over a finite field is isomorphic to an imaginary quadratic field or a quaternion algebra. Furthermore, the endomorphism algebra will be related to the p-rank and the splitting of the prime p in the field $\mathbb{Q}(\pi_E)$, where π_E is a root of f_E.

1.2 Relation between p-rank and endomorphism algebras

In this section based on Silverman [19], we will study the relation between the endomorphism algebra and the p-rank of an elliptic curve $E/\mathbb{F}_q$.

Lemma 1.15. ([19, Exercise 5.10(a)]) The p-rank of $E/\mathbb{F}_q$, with $q = p^n$, satisfies $r(E) = 0$ if and only if $t = \operatorname{Tr} \pi_E \equiv 0 \mod p$.

Proof. Assume $r(E) = 0$. For $i \in \{1, \dots, n\}$, define the isogenies

$$\begin{aligned} \phi_i : E^{(p^{i-1})} &\to E^{(p^i)}, \\ Q &\mapsto Q^p, \end{aligned}$$

where Q^p is obtained from the point $Q \in E$ by raising all coordinates to the power p, and $E^{(p^i)} = \{Q^p : Q \in E^{(p^{i-1})}\}$. Let $i \in \{1, \dots, n\}$ be arbitrary. The degree of ϕ_i is p and therefore $\phi_i \circ \widehat{\phi_i} = [p]$, where $[p]$ is the multiplication-by-p map on $E^{(p^i)}$. As $E^{(p^i)}$ is isogenous to E, the p-rank of $E^{(p^i)}$ is 1 for all $i \in \{1, \dots, n\}$ by Proposition 1.14. Therefore, we have $\#E^{(p^i)}(\overline{\mathbb{F}_q})[p] = 1$, so there is only one point $Q \in E^{(p^i)}(\overline{\mathbb{F}_q})$ such that $pQ = \mathcal{O}$. Since clearly $p\mathcal{O} = \mathcal{O}$, it follows that $E^{(p^i)}(\overline{\mathbb{F}_q})[p] = \{\mathcal{O}\}$. Hence, the kernel of the map $[p]$ on $E^{(p^i)}$ is trivial. Since $\phi_i \circ \widehat{\phi_i} = [p]$, the kernel of $\widehat{\phi_i}$ is also trivial. Suppose that $\widehat{\phi_i}$ is separable. Then by Silverman [19, Theorem III.4.10(c)] and [19, Theorem III.6.2(e)], we have

$$\#\ker \widehat{\phi_i} = \deg \widehat{\phi_i} = \deg \phi_i = p.$$

However, it holds that $\#\ker \widehat{\phi_i} = 1$, so $\widehat{\phi_i}$ must be inseparable for all $i \in \{1, \dots, n\}$.

Let $\pi_E : E \to E$ be the Frobenius endomorphism of E. Note that

$$\pi_E(Q) = Q^q = Q^{p^n} = \phi_n \circ \cdots \circ \phi_1(Q)$$

for all $Q \in E$ and hence $\pi_E = \phi_n \circ \cdots \circ \phi_1$. Then by Silverman [19, Theorem III.6.2(b)], it holds that $\widehat{\pi_E} = \widehat{\phi_n \circ \cdots \circ \phi_1} = \widehat{\phi_1} \circ \cdots \circ \widehat{\phi_n}$. We know that $\ker \widehat{\phi_i} = \{\mathcal{O}\}$ for all $i \in \{1, \dots, n\}$. Therefore, the kernel of $\widehat{\pi_E}$ satisfies

$$\ker \widehat{\pi_E} = \ker \widehat{\phi_1} \circ \cdots \circ \widehat{\phi_n} = \{\mathcal{O}\},$$

which implies that $\deg_s \widehat{\pi_E} = \#\ker \widehat{\pi_E} = 1$ (Silverman [19, Theorem III.4.10(a)]). This shows that $\widehat{\pi_E}$ is inseparable. Moreover, the map π_E is the Frobenius endomorphism and therefore purely inseparable by Silverman [19, Proposition II.2.11(b)]. Let ω be an invariant differential on E. Silverman [19, Proposition II.4.2(c)] states that $[t] = \pi_E + \widehat{\pi_E}$

is inseparable if and only if $(\pi_E + \widehat{\pi_E})^*\omega = 0$. By Silverman [19, Theorem III.5.2], we have

$$(\pi_E + \widehat{\pi_E})^*\omega = \pi_E^*\omega + \widehat{\pi_E}^*\omega.$$

The isogenies π_E and $\widehat{\pi_E}$ are inseparable, so by Silverman [19, Proposition II.4.2(c)], we have $\pi_E^*\omega = 0$ and $\widehat{\pi_E}^*\omega = 0$. Hence,

$$(\pi_E + \widehat{\pi_E})^*\omega = \pi_E^*\omega + \widehat{\pi_E}^*\omega = 0,$$

which shows that $[t] = \pi_E + \widehat{\pi_E}$ is inseparable. It is implied by Silverman [19, Corollary III.5.5] that the isogeny $[t]$ is inseparable if and only if $p|t$. Hence, we have $p|t$.

Next, assume that $p|t$. Then [19, Corollary III.5.5] implies that $\widehat{\pi_E} = [t] - \pi_E$ is inseparable. We have $\widehat{\pi_E} = \widehat{\phi_1} \circ \cdots \circ \widehat{\phi_n}$. Suppose that $\widehat{\phi_i}$ is separable for all $i \in \{1, \ldots, n\}$. Then Silverman [19, Proposition II.4.2(c)] implies that $\widehat{\phi_i}^*$ is injective. By Silverman [19, Proposition II.3.6(f)], we have

$$\widehat{\pi_E}^* = (\widehat{\phi_1} \circ \cdots \circ \widehat{\phi_n})^* = \widehat{\phi_n}^* \circ \cdots \circ \widehat{\phi_1}^*.$$

It follows that $\widehat{\pi_E}^*$ is also injective and hence $\widehat{\pi_E}$ is separable by Silverman [19, Proposition II.4.2(c)]. But this is a contradiction. Hence, there exists $j \in \{1, \ldots, n\}$ such that $\widehat{\phi_j}$ is inseparable.

Note that $\deg \widehat{\phi_j} = \deg_i \widehat{\phi_j} \cdot \deg_s \widehat{\phi_j} = p$. It holds that $\widehat{\phi_j}$ is inseparable, so $\deg_s \widehat{\phi_j} \neq p$. Hence, we have $\deg_s \widehat{\phi_j} = 1$ and $\deg_i \widehat{\phi_j} = p$. By Silverman [19, Theorem III.4.10(a)], it follows that $\#\ker \widehat{\phi_j} = \deg_s \widehat{\phi_j} = 1$ and hence $\widehat{\phi_j}$ has a trivial kernel. Moreover, the isogeny ϕ_j is the p^{th}-power Frobenius morphism and therefore purely inseparable by Silverman [19, Proposition II.2.11(c)]. Therefore, also ϕ_j has a trivial kernel. This implies that

$$\ker \phi_j \circ \widehat{\phi_j} = \ker[p] = \{O\}.$$

Hence, we have $\#E^{(p^j)}(\overline{\mathbb{F}_q})[p] = \#\ker[p] = 1$. This shows that the p-rank of $E^{(p^i)}$ is 1. Since all $E^{(p^i)}$ are isogenous, it follows that $r(E) = 1$ by Proposition 1.14. □

Lemma 1.16. [19, Theorem V.3.1(a)] The endomorphism algebra $\text{End}^0(E)$ of $E/\mathbb{F}_q$ is isomorphic to the quaternion algebra $B_{p,\infty}$ if and only if $r(E) = 0$.

Lemma 1.15 and Lemma 1.16 lead to the following theorem.

Theorem 1.17. Let $E/\mathbb{F}_q$, with $q = p^n$, be an elliptic curve. Then the following statements are equivalent

(i) $\text{Tr}\, \pi_E \equiv 0 \mod p$,

(ii) $r(E) = 0$

(iii) $\mathrm{End}^0(E)$ is isomorphic to the quaternion algebra $B_{p,\infty}$.

Definition 1.18. We call an elliptic curve $E/\mathbb{F}_q$ *supersingular* if E satisfies one of the equivalent statements in Theorem 1.17. Otherwise $E/\mathbb{F}_q$ is called *ordinary*.

The next lemma plays a role in the proof of the fact that an elliptic curve $E/\mathbb{F}_q$ is ordinary if and only if $\mathrm{End}^0(E)$ is isomorphic to an imaginary quadratic field.

Lemma 1.19. If $\alpha, \beta \in \mathrm{End}^0(E)$ commute and $\alpha \notin \mathbb{Q}$, then $\beta \in \mathbb{Q}(\alpha)$.

Proof. We can extend the trace Tr on $\mathrm{End}(E)$ to $\mathrm{End}^0(E)$ by defining $\widehat{r\alpha} = r\widehat{\alpha}$ for $r \in \mathbb{Q}$ and $\alpha \in \mathrm{End}(E)$.

Replace α by $\alpha' = \alpha - \frac{1}{2}\operatorname{Tr}\alpha$. Then

$$\begin{aligned}\operatorname{Tr}\alpha' &= \operatorname{Tr}\left(\alpha - \frac{1}{2}\operatorname{Tr}\alpha\right) = \operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}(\operatorname{Tr}\alpha) = \operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}(\alpha + \widehat{\alpha}) \\ &= \operatorname{Tr}\alpha - \frac{1}{2}(\operatorname{Tr}\alpha + \operatorname{Tr}\widehat{\alpha}) = \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}(\widehat{\alpha} + \widehat{\widehat{\alpha}}) \\ &= \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}(\widehat{\alpha} + \alpha) = \frac{1}{2}(\operatorname{Tr}\alpha - \operatorname{Tr}\alpha) = 0.\end{aligned}$$

Replace β by $\beta' = \beta - \frac{1}{2}\operatorname{Tr}\beta - \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\alpha'$. Then

$$\operatorname{Tr}\beta' = \operatorname{Tr}\left(\beta - \frac{1}{2}\operatorname{Tr}\beta\right) - \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\operatorname{Tr}\alpha' = 0,$$

and

$$\begin{aligned}\operatorname{Tr}\big(\alpha'\beta'\big) &= \operatorname{Tr}\left(\alpha'\left(\beta - \frac{1}{2}\operatorname{Tr}\beta - \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\alpha'\right)\right) \\ &= \operatorname{Tr}\left(\alpha'\beta - \frac{1}{2}\operatorname{Tr}(\beta)\alpha' - \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\alpha'^2\right) \\ &= \operatorname{Tr}\big(\alpha'\beta\big) - \frac{1}{2}\operatorname{Tr}(\beta)\operatorname{Tr}\big(\alpha'\big) - \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\operatorname{Tr}\alpha'^2 \\ &= \operatorname{Tr}\big(\alpha'\beta\big) - \operatorname{Tr}\big(\alpha'\beta\big) \\ &= 0.\end{aligned}$$

Moreover, it holds that

$$\begin{aligned}\operatorname{Tr}\alpha' &= \alpha' + \widehat{\alpha'} = 0, \\ \operatorname{Tr}\beta' &= \beta' + \widehat{\beta'} = 0, \\ \operatorname{Tr}\big(\alpha'\beta'\big) &= \alpha'\beta' + \widehat{\alpha'\beta'} = \alpha'\beta' + \widehat{\beta'}\widehat{\alpha'} = 0,\end{aligned}$$

so $\alpha'\beta' = -\widehat{\beta}'\widehat{\alpha}' = -(-\beta')(-\alpha') = -\beta'\alpha'$. By assumption α and β commute. Since α' and β' are $\mathbb{Q}$-linear combinations of α and β, also α' and β' commute. Hence,

$$\alpha'\beta' = -\beta'\alpha' = -\alpha'\beta',$$

so $2\alpha'\beta' = 0$. The endomorphism algebra $\mathrm{End}^0(E)$ has no zero divisors, so $\alpha' = 0$ or $\beta' = 0$. As $\alpha \notin \mathbb{Q}$ by assumption, it holds that $\alpha' \neq 0$ and hence $\beta' = 0$. This implies that

$$\begin{aligned}\beta &= \frac{1}{2}\operatorname{Tr}\beta + \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\alpha' = \frac{1}{2}\operatorname{Tr}\beta + \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\left(\alpha - \frac{1}{2}\operatorname{Tr}\alpha\right)\\ &= \left(\frac{1}{2}\operatorname{Tr}\beta - \frac{\operatorname{Tr}(\alpha'\beta)\operatorname{Tr}\alpha}{2\operatorname{Tr}\alpha'^2}\right) + \frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}\cdot\alpha.\end{aligned}$$

Since $\frac{1}{2}\operatorname{Tr}\beta - \frac{\operatorname{Tr}(\alpha'\beta)\operatorname{Tr}\alpha}{2\operatorname{Tr}\alpha'^2}$ and $\frac{\operatorname{Tr}(\alpha'\beta)}{\operatorname{Tr}\alpha'^2}$ are rational numbers, this shows that $\beta \in \mathbb{Q}(\alpha)$. □

The following theorem by Silverman gives the endomorphism algebra of an ordinary elliptic curve.

Theorem 1.20 ([19, Theorem V.3.1])**.** Let $E/\mathbb{F}_q$, with $q = p^n$, be an elliptic curve. Then $r(E) = 1$ if and only if $\mathrm{End}^0(E)$ is isomorphic to $\mathbb{Q}(\pi_E) = \mathbb{Q}(\sqrt{t^2 - 4q})$, which is an imaginary quadratic field.

Proof. Assume $r(E) = 1$. Suppose $\pi_E \in \mathbb{Z} \subset \mathrm{End}(E)$, say $\pi_E = r \in \mathbb{Z}$. Then

$$p^n = q = \deg(\pi_E) = \deg([r]) = r^2,$$

so n is even and $r = p^{\frac{n}{2}}$. Since $\pi_E = r$ is a root of $X^2 - tX + q = X^2 - tX + r^2$, where $t = \operatorname{Tr}(\pi_E) = \operatorname{Tr}([r])$, we find $\operatorname{Tr}([r]) = 2r$. Hence,

$$\operatorname{Tr}([r]) = 2r = 2p^{\frac{n}{2}} \equiv 0 \mod p,$$

which implies that $r(E) = 0$ by Theorem 1.17. However, $r(E) = 1$ by assumption, so $\pi_E \notin \mathbb{Z}$. Since π_E is a root of a monic quadratic polynomial with integer coefficients, the number π_E is an algebraic integer. It follows that $\pi_E \notin \mathbb{Q}$. The following claim will imply that also $\pi_E^m \notin \mathbb{Q}$ for any integer $m \geq 1$.

Claim. For all integers $m \geq 1$, we have $\pi_E^m = a\pi_E + b$ for some integers a and b satisfying $a \not\equiv 0 \mod p$ and $b \equiv 0 \mod p$.

Proof of the claim. We will prove the claim by induction. For $m = 1$, we have $\pi_E = 1 \cdot \pi_E + 0$ with $1 \not\equiv 0 \mod p$ and $0 \equiv 0 \mod p$.

Let $m > 1$ be an integer and assume the claim holds for all integers n with $1 \leq n < m$. Then

$$\begin{aligned}\pi_E^m &= \pi_E \cdot \pi_E^{m-1} = \pi_E(a\pi_E + b) = a\pi_E^2 + b\pi_E \\ &= a(\mathrm{Tr}(\pi_E)\pi_E - q) + b\pi_E = (a\,\mathrm{Tr}(\pi_E) + b)\pi_E - aq,\end{aligned}$$

where we used the induction hypothesis in the second equality (with $a \not\equiv 0 \mod p$ and $b \equiv 0 \mod p$) and the fact that $\pi_E^2 - t\pi_E + q = 0$ in the fourth equality. We have

$$a\,\mathrm{Tr}(\pi_E) + b \mod p = a\,\mathrm{Tr}(\pi_E) \mod p.$$

Note that $a \not\equiv 0 \mod p$ and also $\mathrm{Tr}(\pi_E) \not\equiv 0 \mod p$, since $r(E) = 1$ (Theorem 1.17). Therefore $a\,\mathrm{Tr}(\pi_E) \not\equiv 0 \mod p$. Moreover, $-aq = -ap^n \equiv 0 \mod p$. This proves the claim. □

Let r be any positive integer and consider E over the field extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. The Frobenius endomorphism of $E/\mathbb{F}_{q^r}$ is π_E^r, see Section 2.2. By the claim we have $\pi_E^r = a\pi_E + b$ with $a \neq 0$. It follows that $\pi_E^r \notin \mathbb{Q}$. This implies that the endomorphism ring $\mathrm{End}_{\mathbb{F}_{q^r}}(E)$, containing the Frobenius endomorphism π_E^r, is not isomorphic to $\mathbb{Z}$ and hence $\mathrm{End}^0_{\mathbb{F}_{q^r}}(E)$ is not isomorphic to $\mathbb{Q}$. Since this holds for all integers $r > 1$, it follows that $\mathrm{End}^0(E)$ is not isomorphic to $\mathbb{Q}$. Moreover, the endomorphism algebra $\mathrm{End}^0(E)$ is not isomorphic to $B_{p,\infty}$ by Theorem 1.17, because $r(E) = 1$. Hence, it holds that $\mathrm{End}^0(E)$ is isomorphic to an imaginary quadratic field by Theorem 1.6, so $\mathrm{End}^0(E)$ is commutative.

Consider any $\alpha \in \mathrm{End}^0(E)$. Since $\mathrm{End}^0(E)$ is commutative, it follows that α commutes with $\pi_E \in \mathrm{End}^0(E)$. Then Lemma 1.19 implies that $\alpha \in \mathbb{Q}(\pi_E)$. Therefore, we have $\mathrm{End}^0(E) \subset \mathbb{Q}(\pi_E)$. Since clearly $\mathbb{Q}(\pi_E) \subset \mathrm{End}^0(E)$, we conclude that

$$\mathrm{End}^0(E) = \mathbb{Q}(\pi_E) = \mathbb{Q}(\sqrt{t^2 - 4q}).$$

On the other hand, if $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $\mathbb{Q}(\pi_E)$, then $r(E) \neq 0$ by Theorem 1.17. Hence, $r(E) = 1$. □

Remark 1.21. Let t be the trace of the Frobenius endomorphism π_E of $E/\mathbb{F}_q$. By Hasse's theorem (Silverman [19, Theorem V.1.1]), we have $|t| \leq 2\sqrt{q}$. This implies that $t^2 - 4q \leq 0$. Hence, $\mathbb{Q}(\pi_E) = \mathbb{Q}(\sqrt{t^2 - 4q})$ is an imaginary quadratic field, unless $t^2 - 4q = 0$.

Remark 1.22. Theorem 1.20 also holds if $\mathrm{End}^0(E)$ is replaced with $\mathrm{End}^0_{\mathbb{F}_q}(E)$. Hence, for an ordinary elliptic curve we have $\mathrm{End}^0_{\mathbb{F}_q}(E) = \mathrm{End}^0(E)$.

1.3 Relation between p-rank and decomposition of p

In the previous section we have seen that the endomorphism algebra $\mathrm{End}^0(E)$ determines the p-rank $r(E)$ of an elliptic curve $E/\mathbb{F}_q$ and vice versa. Let $E/\mathbb{F}_q$, with $q = p^n$, be an ordinary elliptic curve, f_E be the characteristic polynomial of the Frobenius endomorphism of E, π_E a root of f_E and K the field $\mathbb{Q}(\pi_E)$. In this section, we will give the prime factorization of $p\mathcal{O}_K$ in the field $K = \mathbb{Q}(\pi_E) \cong \mathrm{End}^0(E)$. We assume that $\mathrm{End}(E) \cong \mathcal{O}_K$.

Lemma 1.23. (Cox, [4, Exercise 5.9(b)]) Let K be an imaginary quadratic field. Then

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } K = \mathbb{Q}(i), \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } K = \mathbb{Q}(\omega) \text{ with } \omega = \frac{-1+\sqrt{-3}}{2}, \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

Theorem 1.24. Let $E/\mathbb{F}_q$, with $q = p^n$, be an ordinary elliptic curve. Then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $K = \mathbb{Q}(\pi_E)$ and p splits in K, so $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$.

Proof. If E is ordinary, then Theorem 1.20 states that $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $K = \mathbb{Q}(\pi_E)$. Thus $p\mathcal{O}_K$ factors as one of

1. $p\mathcal{O}_K$ (p is inert),
2. $\mathfrak{p}^2$,
3. $\mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$.

The norm of π_E in K can be computed as $\mathrm{N}_{K/\mathbb{Q}}(\pi_E) = \pi_E\overline{\pi_E} = p^n$, so $(\pi_E)(\overline{\pi_E}) = (p)^n$. Hence, each prime ideal in the prime factorization of (π_E) lies above p. In other words, the prime factorization of (π_E) in K is built from the same primes that appear in the prime factorization of $p\mathcal{O}_K$.

Suppose we are in case one or two, so there is only one prime ideal $\mathfrak{p}$ lying above p. If p is inert, then $\mathfrak{p}$ has norm p^2 and if p ramifies, then $\mathfrak{p}$ has norm p. Since $\mathrm{N}_{K/\mathbb{Q}}(\pi_E) = p^n$, it follows that $(\pi_E) = \mathfrak{p}^s$, where $s = \frac{n}{2}$ if p is inert and $s = n$ if $p\mathcal{O}_K = \mathfrak{p}^2$. Furthermore, the only prime ideal lying above p is $\mathfrak{p}$, so $\mathfrak{p} = \overline{\mathfrak{p}}$. Hence, we have

$$\overline{(\pi_E)} = \overline{\mathfrak{p}^s} = \overline{\mathfrak{p}}^s = \mathfrak{p}^s = (\pi_E).$$

Thus, there is a unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\overline{\pi_E} = \varepsilon\pi_E$.

As $f_E = X^2 - tX + q$ and π_E is a root of f_E, without loss of generality it holds that

$$\pi_E = \frac{t + \sqrt{t^2 - 4q}}{2} \qquad \text{and} \qquad \overline{\pi_E} = \frac{t - \sqrt{t^2 - 4q}}{2},$$

where $t \neq 0$ by Theorem 1.17 and $t^2 - 4q < 0$. By Lemma 1.23, we have $\mathcal{O}_K^\times = \{\pm 1\}$ unless $K = \mathbb{Q}(i)$ or $\mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)$. If $\overline{\pi_E} = \pi_E$, then π_E is real and hence K is a real field. If $\overline{\pi_E} = -\pi_E$, then $t = \overline{\pi_E} + \pi_E = 0$, implying that $r(E) = 0$ by Lemma 1.9. So both $\varepsilon = 1$ and $\varepsilon = -1$ lead to a contradiction. It remains to check the equation $\overline{\pi_E} = \varepsilon \pi_E$ when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\omega)$ with $\omega = \frac{-1+\sqrt{-3}}{2}$.

If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ by Lemma 1.23. By the same reasoning as above, the equation $\overline{\pi_E} = \varepsilon \pi_E$ does not hold for $\varepsilon \in \{\pm 1\}$. The equation $\overline{\pi_E} = \varepsilon \pi_E$ translates to

$$\varepsilon = \frac{\overline{\pi_E}}{\pi_E} = \frac{t^2 - 2q - t\sqrt{t^2 - 4q}}{2q}. \tag{1.1}$$

If $\varepsilon = \pm i$, then comparing the real parts of both sides of (1.1) gives

$$0 = \frac{t^2 - 2q}{2q}$$

and hence $t^2 = 2q = 2p^n$. This is possible only if $p = 2$ and n is odd. But then $t \equiv 0 \mod 2$ and $r(E) = 0$ by Lemma 1.9. Hence, $\overline{\pi_E} \neq \varepsilon \pi_E$ for all $\varepsilon \in \mathcal{O}_K^\times$.

If $K = \mathbb{Q}(\omega)$ with $\omega = \frac{-1+\sqrt{-3}}{2}$, then $\mathcal{O}_K^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ by Lemma 1.23. Again, by the same reasoning as above, the equation $\overline{\pi_E} = \varepsilon \pi_E$ does not hold for $\varepsilon \in \{\pm 1\}$. We have

$$\omega = \frac{-1 + \sqrt{-3}}{2}, \qquad -\omega = \frac{1 - \sqrt{-3}}{2}, \qquad \omega^2 = \frac{-1 - \sqrt{-3}}{2}, \qquad -\omega^2 = \frac{1 + \sqrt{-3}}{2},$$

so $\mathrm{Re}(\omega) = \mathrm{Re}(\omega^2) = -\frac{1}{2}$ and $\mathrm{Re}(-\omega) = \mathrm{Re}(-\omega^2) = \frac{1}{2}$. If $\varepsilon \in \{\omega, \omega^2\}$, then comparing the real parts of both sides of (1.1) gives

$$-\frac{1}{2} = \frac{t^2 - 2q}{2q},$$

which can be solved to $t^2 = q = p^n$, so n is even. But then $t \equiv 0 \mod p$ and $r(E) = 0$ by Lemma 1.9. If $\varepsilon \in \{-\omega, -\omega^2\}$, then comparing the real parts of both sides of (1.1) gives

$$\frac{1}{2} = \frac{t^2 - 2q}{2q},$$

which can be solved to $t^2 = 3q = 3p^n$. This is possible only if $p = 3$ and n is odd. But then $t \equiv 0 \mod 3$ and $r(E) = 0$ by Lemma 1.9. Hence, $\overline{\pi_E} \neq \varepsilon\pi_E$ for all $\varepsilon \in \mathcal{O}_K^\times$.

This shows that for all imaginary quadratic fields K, there is no $\varepsilon \in \mathcal{O}_K^\times$ such that $\overline{\pi_E} = \varepsilon\pi_E$. Therefore, the only remaining possibility for the factorization of $p\mathcal{O}_K$ is $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. □

Remark 1.25. Theorem 1.24 can also be achieved using Theorem 3.13.

Chapter 2

Abelian varieties over finite fields

The main goal of this chapter is to provide the necessary background on abelian varieties. This will be done in Section 2.1, which is mainly based on Milne [14] and Tate [20], [21], and Section 2.2, which is based on Howe and Zhu [9]. Besides, we summarize the relations between the endomorphism algebra, the p-rank and the prime factorization of the rational prime p in $\mathbb{Q}(\pi_S)$ for an abelian surface $S/\mathbb{F}_{p^n}$. These relations are known and can be found in Gonzalez [7] and Bradford [2]. This chapter forms the preparation for Chapter 3.

2.1 Background

An elliptic curve is a nonsingular projective curve together with a group structure defined by regular maps. This definition of an elliptic curve can be generalized to higher dimensional varieties.

Definition 2.1. An *abelian variety* is a nonsingular (geometrically irreducible) projective variety with a group structure defined by regular maps.

In general, an abelian variety over a field k of dimension g is denoted by A/k. Later we will slightly change notation, but for now we keep the notation A for an arbitrary abelian variety of dimension g.

Let A_1 and A_2 be two abelian varieties of dimension g. A rational map $\phi : A_1 \to A_2$ that is regular at every point is called a *morphism*. The maps between abelian varieties that

will be studied, form a subset of the set of morphisms and are again called isogenies. The definition is similar to the definition of an isogeny between elliptic curves (Definition 1.1).

Definition 2.2. Let A_1 and A_2 be abelian varieties of dimension g. An *isogeny* from A_1 to A_2 is a surjective morphism $\phi : A_1 \to A_2$ which defines a homomorphism of the underlying groups, with a finite kernel. We call A_1 and A_2 *isogenous* if there exists an isogeny between A_1 and A_2.

Definition 2.3. Let $\phi : A_1 \to A_2$ be an isogeny between two abelian varieties A_1 and A_2 of degree m. Then the *dual isogeny* of ϕ is the unique isogeny $\widehat{\phi} : A_2 \to A_1$ satisfying $\widehat{\phi} \circ \phi = [m]$.

Remark 2.4. If there exists an isogeny between two abelian varieties A_1 and A_2, then the dimension of A_1 is equal to the dimension of A_2, see Milne [14, Proposition I.7.1].

In addition to the isogenies defined above, there is one more important map between abelian varieties. This is the *zero morphism* $[0] : A_1 \to A_2$, where A_1 and A_2 are two abelian varieties of dimension g, and is given by sending all points on A_1 to the identity element on A_2.

Let A_1/k and A_2/k be two abelian varieties of dimension g. We can distinguish between isogenies defined over k and isogenies defined over the algebraic closure $\overline{k}$. If there exists an isogeny defined over k from A_1 to A_2, then the abelian varieties A_1 and A_2 are called *k-isogenous*. If the isogeny from A_1 to A_2 is defined over the algebraic closure $\overline{k}$, then A_1 and A_2 are called *$\overline{k}$-isogenous*.

Definition 2.5. Let A/k be an abelian variety. An *endomorphism* of A is a morphism from A to itself that is a homomorphism of the underlying group. The set of all endomorphisms defined over k from A to itself is called the *endomorphism ring* of A and is denoted by $\mathrm{End}_k(A)$.

Under pointwise addition and composition, $\mathrm{End}_k(A)$ becomes a ring. The additive and multiplicative unit element of the endomorphism ring is given by the zero morphism. The set of all endomorphisms of A defined over the algebraic closure $\overline{k}$ is denoted by $\mathrm{End}(A)$ and is also a ring under pointwise addition and composition.

Example 2.6. Let A/k be an abelian variety. The multiplication-by-n map $[n] : A \to A$, where n is any integer, given by

$$[n](P) = \underbrace{P + \cdots + P}_{n \text{ terms}}$$

is an endomorphism (and even an isogeny) of A defined over k. Therefore, $\{[n] : n \in \mathbb{Z}\}$ forms a subring of $\mathrm{End}_k(A)$ isomorphic to $\mathbb{Z}$ and we say that $\mathbb{Z} \subseteq \mathrm{End}_k(A) \subseteq \mathrm{End}(A)$.

From the endomorphism ring, the endomorphism algebra can be constructed.

Definition 2.7. The *endomorphism algebra* of A/k over the base field k is $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and is denoted by $\mathrm{End}_k^0(A)$. Over the algebraic closure $\overline{k}$, the endomorphism algebra is $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and is denoted by $\mathrm{End}^0(A)$.

From now on, we restrict to abelian varieties defined over finite fields. A special endomorphism of an abelian variety $A/\mathbb{F}_q$ is the Frobenius endomorphism.

Definition 2.8. The endomorphism $\pi_A : A \to A$ induced by the embedding of function fields $\mathbb{F}_q(A)^q \subset \mathbb{F}_q(A)$, is called the *Frobenius endomorphism* of A.

The next theorem by Milne is used to define the characteristic polynomial of the Frobenius endomorphism.

Theorem 2.9. ([14, Theorem 10.9]) Let $A/\mathbb{F}_q$ be an abelian variety of dimension g. For every $\alpha \in \mathrm{End}_{\mathbb{F}_q}(A)$, there is a unique polynomial $P_\alpha \in \mathbb{Z}[x]$ of degree $2g$ such that $P_\alpha(t) = \deg(\alpha - t)$ for almost all $t \in \mathbb{Z}$.

We define $f_A \coloneqq P_{\pi_A}$ to be the *characteristic polynomial of the Frobenius endomorphism* of A. If f_A is irreducible, we identify a root of f_A with the Frobenius endomorphism π_A. By abuse of language, we use the notation π_A to refer to both the Frobenius endomorphism and a root of f_A.

The Frobenius endomorphism of an abelian variety $A/\mathbb{F}_q$ determines the center of the endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}^0(A)$ as is stated in the following theorem by Tate.

Theorem 2.10. ([20, Theorem 2(a)]) Let $A/\mathbb{F}_q$ be an abelian variety and let π_A be the Frobenius endomorphism of A. Then the center of the endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}^0(A)$ is isomorphic to $\mathbb{Q}(\pi_A)$.

An abelian variety A/k of dimension $g > 1$ can be isogenous, either over k or $\overline{k}$, to a product $A_1 \times \cdots \times A_n$ of lower dimensional abelian varieties. As explained in Remark 2.4, the dimensions of $A_1, \ldots, A_n$ should add up to the dimension g of A in order for A and $A_1 \times \cdots \times A_n$ to be isogenous.

Definition 2.11. An abelian variety over a field k is called *simple* if it is not k-isogenous to a product of lower dimensional abelian varieties. An abelian variety is called *absolutely simple* if it is simple over the algebraic closure of k.

An alternative definition of a simple abelian variety A/k is an abelian variety of which the endomorphism ring $\mathrm{End}_k(A)$ contains no zero divisors.

Definition 2.12. An abelian variety A/k is called *isotypic over* k if it is k-isogenous to B^d, where B is a simple abelian variety and d a positive integer. An abelian variety A/k is called *isotypic over* $\overline{k}$ if it is $\overline{k}$-isogenous to B^d, where B is an absolutely simple abelian variety and d a positive integer.

In particular, every simple abelian variety A/k is isotypic over k and every absolutely simple abelian variety A/k is isotypic over $\overline{k}$.

If an abelian variety $A/\mathbb{F}_q$ is not (absolutely) simple, then there is a relation between the endomorphism algebra $\mathrm{End}^0(A)$ and the endomorphism algebras of the abelian subvarieties of A.

Proposition 2.13. ([14, p.43]) Let $A/\mathbb{F}_q$ be an abelian variety.

(i) If A is $\mathbb{F}_q$-isogenous to a product $\prod A_i^{n_i}$ of simple abelian varieties $A_i/\mathbb{F}_q$ that are not $\mathbb{F}_q$-isogenous to each other, then

$$\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \oplus M_{n_i}(\mathrm{End}^0_{\mathbb{F}_q}(A_i)),$$

where M_{n_i} denotes the ring of $(n_i \times n_i)$-matrices.

(ii) If A is $\overline{\mathbb{F}_q}$-isogenous to a product $\prod A_i^{n_i}$ of absolutely simple abelian varieties $A_i/\overline{\mathbb{F}_q}$ that are not $\overline{\mathbb{F}_q}$-isogenous to each other, then

$$\mathrm{End}^0(A) \cong \oplus M_{n_i}(\mathrm{End}^0(A_i)).$$

The following two theorems by Tate explain the relation between the characteristic polynomial of Frobenius of an abelian variety $A/\mathbb{F}_q$ and its abelian subvarieties over $\mathbb{F}_q$.

Theorem 2.14. ([20, Theorem 1(b),(c)]) Let $A/\mathbb{F}_q$ and $B/\mathbb{F}_q$ be abelian varieties. Then

(i) A and B are $\mathbb{F}_q$-isogenous if and only if $f_A = f_B$,

(ii) B is $\mathbb{F}_q$-isogenous to an abelian subvariety of A defined over $\mathbb{F}_q$ if and only if f_B divides f_A.

Theorem 2.15. ([20, Theorem 2(d)]) Let $A/\mathbb{F}_q$ be an abelian variety of dimension g. Then the following statements are equivalent.

(i) f_A is a power of a linear polynomial,

(ii) $\mathbb{Q}(\pi_A) = \mathbb{Q}$,

(iii) A is $\mathbb{F}_q$-isogenous to the g-th power of a supersingular elliptic curve, all of whose endomorphisms are defined over $\mathbb{F}_q$.

Definition 2.16. A complex number $\pi \in \mathbb{C}$ is called a *Weil q-number* if $|\phi(\pi)| = q^{\frac{1}{2}}$ for all embeddings $\phi : \mathbb{Q}(\pi) \to \mathbb{C}$.

The above definition implies that Weil q-numbers are algebraic over $\mathbb{Q}$.

Definition 2.17. A polynomial in $\mathbb{Z}[x]$ is called a *Weil polynomial* if all its roots are Weil q-numbers.

Two Weil q-numbers π_1 and π_2 are called equivalent if they have the same minimal polynomial. In other words, if there is an isomorphism $\phi : \mathbb{Q}(\pi_1) \to \mathbb{Q}(\pi_2)$ such that $\phi(\pi_1) = \pi_2$. The relation between Weil q-numbers and abelian varieties over $\mathbb{F}_q$ is due to Honda and Tate and is given by the next two theorems.

Theorem 2.18. ([14, Theorem II.1.1]) Let $A/\mathbb{F}_q$ be an abelian variety of dimension g with f_A the characteristic polynomial of Frobenius. Write $f_A(X) = \prod_{i=1}^{2g}(X - a_i)$ for $a_i \in \mathbb{C}$. Then the Riemann hypothesis implies $|a_i| = q^{\frac{1}{2}}$.

Corollary 2.19. The characteristic polynomial of the Frobenius endomorphism of an abelian variety over a finite field is a Weil polynomial.

Theorem 2.20. ([21, Theorem 1]) There is a bijection between the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the equivalence classes of Weil q-numbers. The bijection is given by associating to a simple abelian variety $A/\mathbb{F}_q$ a root of the characteristic polynomial of Frobenius.

Corollary 2.21. Let $A/\mathbb{F}_q$ be a simple abelian variety of dimension g. Then $f_A = h^e$, where h is an irreducible Weil polynomial and e a positive integer dividing $2g$.

Proof. Let $A/\mathbb{F}_q$ be a simple abelian variety of dimension g. Consider the set of abelian varieties

$$\mathcal{S} = \{A'/\mathbb{F}_q : A' \text{ is simple and } \mathbb{F}_q\text{-isogenous to } A\}.$$

By Theorem 2.14(i), every abelian variety in the set $\mathcal{S}$ has the same characteristic polynomial of Frobenius f_A. Any root of f_A is a representative of the equivalence class of Weil q-numbers corresponding to the set $\mathcal{S}$ by Theorem 2.20. Therefore, all roots of f_A are equivalent Weil q-numbers. Since these equivalent Weil q-numbers have the same minimal polynomial h, it follows that $f_A = h^e$. Here e is a positive integer dividing $2g$, because the degree of f_A is $2g$. □

If $A/\mathbb{F}_q$ is a simple abelian variety, then the characteristic polynomial of Frobenius determines the endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A)$, as is stated in the following theorem by Tate.

Theorem 2.22. ([20, Theorem 2(c),(e)]) Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian variety. Then

(i) $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathbb{Q}(\pi_A)$ if and only if f_A is irreducible;

(ii) $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathcal{D}_A$, where $\mathcal{D}_A$ is a central simple algebra over $\mathbb{Q}(\pi_A)$ which splits at all finite primes $\mathfrak{p}$ of $\mathbb{Q}(\pi_A)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_A)$, if $f_A = h^e$, with h an irreducible polynomial and $e > 1$.

Remark 2.23. If for an abelian variety A/F_q of dimension g it holds that f_A is a power of a linear polynomial, then part (ii) of Theorem 2.22 applies. Moreover, it follows from Theorem 2.15 that in this case A is $\mathbb{F}_q$-isogenous to the g-th power of a supersingular elliptic curve $E/\mathbb{F}_q$, all of whose endomorphisms are defined over $\mathbb{F}_q$. Thus by Proposition 2.13, we have

$$\mathrm{End}^0_{\mathbb{F}_q}(A) \cong M_g(\mathrm{End}^0_{\mathbb{F}_q}(E)) = M_g(\mathrm{End}^0(E)) \cong M_g(B_{p,\infty}),$$

where $B_{p,\infty}$ is a quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞, and $M_g(B_{p,\infty})$ is a central simple algebra over $\mathbb{Q}(\pi_A) = \mathbb{Q}$ which does not split at any prime of $\mathbb{Q}$ by part (ii) of Theorem 2.22.

Let $A/\mathbb{F}_q$, with $q = p^n$, be a simple abelian variety. Let π_A be a root of f_A and let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\pi_A)$. Then the invariant $i_\mathfrak{p}$ of $\mathrm{End}^0_{\mathbb{F}_q}(A)$ at $\mathfrak{p}$ is defined as

$$i_\mathfrak{p} = \begin{cases} \frac{1}{2} & \text{if } \mathfrak{p} \text{ is real,} \\ 0 & \text{if } \mathfrak{p} \text{ lies over a prime } l \neq p \text{ in } \mathbb{Q}, \\ f(\mathfrak{p}) \cdot \frac{\mathrm{ord}_\mathfrak{p}(\pi_A)}{n} & \text{if } \mathfrak{p} \text{ lies over } p, \end{cases}$$

where $f(\mathfrak{p})$ denotes the residual degree at $\mathfrak{p}$ with respect to p. More information about the invariants can be found in Waterhouse and Milne [22, Theorem 8].

If $A/\mathbb{F}_q$ is a simple abelian variety of dimension g, then the characteristic polynomial of Frobenius f_A is of the form h^e, where h is an irreducible Weil polynomial and e is a positive integer dividing $2g$ by Corollary 2.21. There is a relation between the integer e and the invariants of $\mathrm{End}^0_{\mathbb{F}_q}(A)$. This relation will become apparent after the next two theorems by Tate and Milne respectively.

Theorem 2.24. ([21, Theorem 1]) Let $A/\mathbb{F}_q$ be a simple abelian variety of dimension g. Then

$$2g = [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}} [\mathbb{Q}(\pi_A) : \mathbb{Q}].$$

Let A be a simple abelian variety of dimension g with $f_A = h^e$ and let π_A be a root of f_A. Then $[\mathbb{Q}(\pi_A) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial h of π_A. Since the degree of f_A is $2g$, by Theorem 2.24 it holds that

$$\begin{aligned} e \deg(h) &= \deg(f_A) = 2g \\ &= [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}} [\mathbb{Q}(\pi_A) : \mathbb{Q}] \\ &= [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}} \deg(h), \end{aligned}$$

so $e = [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}$.

Theorem 2.25. ([14, Theorem II.2.8]) If $A/\mathbb{F}_q$ is a simple abelian variety, then the least common denominator of the invariants $i_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\pi_A)$, is equal to $[\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}$.

By Theorem 2.25, the integer $e = [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}$ is equal to the least common denominator of the invariants $i_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\pi_A)$. In particular, we have the following corollary.

Corollary 2.26. If an abelian threefold $A/\mathbb{F}_q$ is such that f_A is irreducible, then its invariants are integers.

Proof. If f_A is irreducible, then Theorem 2.14(ii) implies that A is simple. Thus $f_A = h^e$, where h is an irreducible Weil polynomial and e a positive integer dividing $2g$ by Corollary 2.21. But f_A is irreducible, so $e = 1$. Now by Theorem 2.25, it holds that $e = [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}$ equals the least common denominator of the invariants $i_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\pi_A)$. It follows that the least common denominator of the invariants $i_{\mathfrak{p}}$ is 1 and hence the invariants are integers. □

Let $A/\overline{\mathbb{F}_q}$, with $q = p^n$, be an abelian variety of dimension g. Let $m \in \mathbb{Z}_{>0}$. The *m-torsion subgroup* of A is the set of points of A of order m and is denoted by $A(\overline{\mathbb{F}_q})[m]$. The m-torsion subgroup is equal to the kernel of the multiplication-by-m map $[m]$. If m and p are coprime, then $A(\overline{\mathbb{F}_q})[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g}$ by Milne [14, p.4]. However, this does not always hold when $m = p$.

Definition 2.27. The p-rank of an abelian variety $A/\mathbb{F}_q$, with $q = p^n$, is the integer $r = r(A)$ such that the group $A(\overline{\mathbb{F}_q})[p]$ has order p^r.

The p-rank of an abelian variety $A/\mathbb{F}_q$ of dimension g is nonnegative and bounded by g

$$0 \leq r(A) \leq g.$$

In the next proposition, we will show that abelian varieties that are $\overline{\mathbb{F}_q}$-isogenous to each other have the same p-rank. Moreover, if an abelian variety $A/\mathbb{F}_q$ is not absolutely simple, the p-rank of A can be deduced from the p-rank of the abelian subvarieties of A.

Proposition 2.28. Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian variety $\overline{\mathbb{F}_q}$-isogenous to a product $A_1 \times \cdots \times A_m$ of absolutely simple abelian varieties defined over $\mathbb{F}_q$. Then

$$r(A) = r(A_1) + \cdots + r(A_m).$$

Proof. Let $\phi : A \to A_1 \times \cdots \times A_m$ be an isogeny defined over $\overline{\mathbb{F}_q}$. Let $Q \in A(\overline{\mathbb{F}_q})[p]$ be arbitrary. Then we have $pQ = \mathcal{O}_A$, where $\mathcal{O}_A$ denotes the identity element of A. Since ϕ is an isogeny, and thus a homomorphism, it holds that

$$(\mathcal{O}_{A_1}, \ldots, \mathcal{O}_{A_m}) = \phi(\mathcal{O}_A) = \phi(pQ) = p\phi(Q),$$

where $\mathcal{O}_{A_i}$ is the identity element of A_i for $i \in \{1, \ldots, m\}$. This implies that $\phi(Q) \in A_1 \times \cdots \times A_m(\overline{\mathbb{F}_q})[p]$. Hence, we have

$$\begin{aligned} p^{r(A)} &= |A(\overline{\mathbb{F}_q})[p]| \geq |A_1 \times \cdots \times A_m(\overline{\mathbb{F}_q})[p]| = |A_1(\overline{\mathbb{F}_q})[p] \times \cdots \times A_m(\overline{\mathbb{F}_q})[p]| \\ &= |A_1(\overline{\mathbb{F}_q})[p]| \cdot \ldots \cdot |A_m(\overline{\mathbb{F}_q})[p]| = p^{r(A_1)} \cdot \ldots \cdot p^{r(A_m)} = p^{r(A_1)+\cdots+r(A_m)}, \end{aligned}$$

because ϕ is surjective. It follows that $r(A) \geq r(A_1) + \cdots + r(A_m)$.

Let $\widehat{\phi} : A_1 \times \cdots \times A_m \to A$ be the dual isogeny of ϕ. Let $Q \in |A_1 \times \cdots \times A_m(\overline{\mathbb{F}_q})[p]|$ be arbitrary. Then we have $pQ = (\mathcal{O}_{A_1}, \ldots, \mathcal{O}_{A_m})$. Since $\widehat{\phi}$ is an isogeny, and thus a homomorphism, it holds that

$$\mathcal{O}_A = \widehat{\phi}((\mathcal{O}_{A_1}, \ldots, \mathcal{O}_{A_m})) = \widehat{\phi}(pQ) = p\widehat{\phi}(Q).$$

This implies that $\widehat{\phi}(Q) \in A(\overline{\mathbb{F}_q})[p]$. Hence, we have

$$p^{r(A_1)+\cdots+r(A_m)} = |A_1 \times \cdots \times A_m(\overline{\mathbb{F}_q})[p]| \geq |A(\overline{\mathbb{F}_q})[p]| = p^{r(A)},$$

because $\widehat{\phi}$ is surjective. It follows that $r(A_1) + \cdots + r(A_m) \geq r(A)$. This shows that $r(A) = r(A_1) + \cdots + r(A_m)$. □

If $r(A) = g$, then A is called *ordinary*. If A is $\overline{\mathbb{F}_q}$-isogenous to the product of g supersingular elliptic curves, then A is called *supersingular*. It follows from Proposition 2.28 that a supersingular abelian variety $A/\mathbb{F}_q$ satisfies $r(A) = 0$. In Chapter 1, we have seen that the converse holds for elliptic curves. If an elliptic curve E satisfies $r(E) = 0$, then E is supersingular. We will see in Section 2.3 that the same holds for an abelian variety of dimension $g = 2$.

2.2 Base extensions

In this section, we discuss what happens with the Frobenius endomorphism, the endomorphism algebra and the p-rank if we define an abelian variety $A/\mathbb{F}_q$ over a finite field extension $\mathbb{F}_{q^r}$. Extending the base of abelian varieties over finite fields proves to be a helpful tool that will turn up in Chapter 3.

Let $A/\mathbb{F}_q$ be an abelian variety of dimension g with Frobenius endomorphism π_A. Let r be a positive integer and consider $A/\mathbb{F}_{q^r}$. The field $\mathbb{F}_{q^r}$ is a finite field extension of $\mathbb{F}_q$ of degree r. The endomorphisms of A defined over $\mathbb{F}_q$ are also defined over the field extension $\mathbb{F}_{q^r}$, so $\mathrm{End}^0_{\mathbb{F}_q}(A) \subseteq \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$. The Frobenius π_A of $A/\mathbb{F}_q$ is induced by the q-th power Frobenius automorphism of $\overline{\mathbb{F}_q}$ and the Frobenius of $A/\mathbb{F}_{q^r}$ is induced by the q^r-th power Frobenius automorphism of $\overline{\mathbb{F}_{q^r}}$. Composing r times the q-th power Frobenius automorphism of $\overline{\mathbb{F}_q}$ gives the q^r-th power Frobenius automorphism of $\overline{\mathbb{F}_q}$. Since $\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}$, the composition of r times the q-th power Frobenius automorphism of $\overline{\mathbb{F}_q}$ coincides with the q^r-th power Frobenius automorphism of $\overline{\mathbb{F}_{q^r}}$. Hence, the Frobenius endomorphism of $A/\mathbb{F}_{q^r}$ is π_A^r. It follows that if the characteristic polynomial of Frobenius of $A/\mathbb{F}_q$ is

$$f_A = (x - \pi_{A,1}) \cdots (x - \pi_{A,2g}),$$

then the characteristic polynomial of Frobenius of $A/\mathbb{F}_{q^r}$ is

$$f'_A = (x - (\pi_{A,1})^r) \cdots (x - (\pi_{A,2g})^r).$$

Suppose A is $\overline{\mathbb{F}_q}$-isogenous to a product $\prod A_1^{n_i}$ of absolutely simple abelian varieties $A_i/\overline{\mathbb{F}_q}$ that are not $\overline{\mathbb{F}_q}$-isogenous to each other. As

$$\mathrm{End}^0_{\mathbb{F}_q}(A) \subseteq \mathrm{End}^0_{\mathbb{F}_{q^2}}(A) \subseteq \cdots \subseteq \mathrm{End}^0_{\mathbb{F}_{q^r}} \subseteq \cdots \subseteq \mathrm{End}^0 A,$$

there exists a positive integer s such that over the field extension $\mathbb{F}_{q^s}$, the abelian variety A is $\mathbb{F}_{q^s}$-isogenous to $\prod A_i^{n_i}$. On the other hand, if there exists a positive integer s such that $A/\mathbb{F}_{q^s}$ is $\mathbb{F}_{q^s}$-isogenous to a product $\prod A_i^{n_i}$ of absolutely simple abelian varieties A_i, then $A/\mathbb{F}_q$ is $\overline{\mathbb{F}_q}$-isogenous to $\prod A_i^{n_i}$. Furthermore, there always exists a positive integer t such that $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^t}}(A)$.

Recall that the p-rank of an abelian variety $A/\mathbb{F}_q$, with $q = p^n$, is the integer $r(A)$ such that the group $A(\overline{\mathbb{F}_q})[p]$ has order $p^{r(A)}$. Since $\overline{\mathbb{F}_q} = \overline{\mathbb{F}_{q^2}} = \cdots = \overline{\mathbb{F}_{q^r}} = \ldots$, it holds that

$$\left|A(\overline{\mathbb{F}_q})[p]\right| = \left|A(\overline{\mathbb{F}_{q^2}})[p]\right| = \cdots = \left|A(\overline{\mathbb{F}_{q^r}})[p]\right| = \ldots$$

and hence

$$r(A/\mathbb{F}_q) = r(A/\mathbb{F}_{q^2}) = \cdots = r(A/\mathbb{F}_{q^r}) = \ldots. \tag{2.1}$$

The following proposition by Howe and Zhu gives a sufficient condition for a simple abelian variety $A/\mathbb{F}_q$ to be absolutely simple.

Proposition 2.29. ([9, Proposition 3]) Let $A/\mathbb{F}_q$ be a simple abelian variety with Frobenius π_A. If $\mathbb{Q}(\pi_A^r) = \mathbb{Q}(\pi_A)$ for all integers $r > 0$, then A is absolutely simple.

Proof. Let f_A be the characteristic polynomial of the Frobenius endomorphism π_A. The abelian variety A is simple, so $f_A = h^e$, where $h = (x - \pi_{A,1}) \cdots (x - \pi_{A,\frac{2g}{e}})$ is an irreducible Weil polynomial and e a positive integer dividing $2g$ by Corollary 2.21. Let r be an arbitrary positive integer and consider $A/\mathbb{F}_{q^r}$. Let f'_A be the characteristic polynomial of the Frobenius endomorhism π_A^r of $A/\mathbb{F}_{q^r}$. Then

$$f'_A = ((x - (\pi_{A,1})^r) \cdots (x - (\pi_{A,\frac{2g}{e}})^r))^e = (h')^e.$$

Since $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_A^r)$, the polynomial h' is irreducible.

If $e = 1$, then f_A and f'_A are both irreducible. It follows that $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathbb{Q}(\pi_A)$ and $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A) \cong \mathbb{Q}(\pi_A^r)$ by Theorem 2.22. Hence, we have $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$, because $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_A^r)$.

If $e > 1$, then $\mathrm{End}^0_{\mathbb{F}_q}$ is isomorphic to a central simple algebra over $\mathbb{Q}(\pi_A)$ which splits at all finite primes $\mathfrak{p}$ of $\mathbb{Q}(\pi_A)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_A)$, and $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ is isomorphic to a central simple algebra over $\mathbb{Q}(\pi_A^r)$ which splits at all finite primes $\mathfrak{p}$ of $\mathbb{Q}(\pi_A^r)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_A^r)$. Since $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_A^r)$, it follows that $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$.

Suppose that the abelian variety $A/\mathbb{F}_{q^r}$ is not simple. Then at least one zero divisor is contained in the endomorphism ring $\mathrm{End}_{\mathbb{F}_{q^r}}(A)$. The abelian variety $A/\mathbb{F}_q$ is simple by assumption, so the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$ contains no zero divisors. Hence, there exists an element in $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ that does not come from $\mathrm{End}^0_{\mathbb{F}_q}(A)$. But we proved that $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$. This shows that $A/\mathbb{F}_{q^r}$ must be simple. Hence, the abelian variety $A/\mathbb{F}_q$ is absolutely simple. □

Corollary 2.30. Let $A/\mathbb{F}_q$ be a simple abelian variety. If $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ for all integers $r > 0$, then A is absolutely simple.

Proof. If $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ for all integers $r > 0$, then in particular it holds that $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ for all integers $r > 0$. Let r be any positive integer and consider $A/\mathbb{F}_{q^r}$. The Frobenius endomorphism of $A/\mathbb{F}_{q^r}$ is π_A^r. By Theorem 2.10, the center of $\mathrm{End}^0_{\mathbb{F}_q}(A)$ is isomorphic to $\mathbb{Q}(\pi_A)$ and the center of $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ is isomorphic to $\mathbb{Q}(\pi_A^r)$. Since $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$, their centers are also equal. Therefore, it holds

that $\mathbb{Q}(\pi_A^r) = \mathbb{Q}(\pi_A)$. Since r is taken arbitrary, $\mathbb{Q}(\pi_A^r) = \mathbb{Q}(\pi_A)$ for all integers $r > 0$. Then Proposition 2.29 implies that A is absolutely simple. □

2.3 Classifying abelian surfaces over finite fields

In this section, we summarize the relations between the endomorphism algebra, the p-rank and the prime factorization of the rational prime p in $\mathbb{Q}(\pi_S)$ for an abelian surface $S/\mathbb{F}_{p^n}$ with Frobenius π_S. These relations are known and can be found in Gonzalez [7] and Bradford [2].

An abelian variety of dimension $g = 2$ is called an *abelian surface*. The notation S is used for an abelian surface. Let $S/\mathbb{F}_q$ be an abelian surface defined over the finite field $\mathbb{F}_q$. If $S/\mathbb{F}_q$ is not simple, then S is $\mathbb{F}_q$-isogenous to the product of two elliptic curves E_1 and E_2. Theorem 2.14(ii) implies that in this case the characteristic polynomial of Frobenius of S is given by $f_S = f_{E_1} f_{E_2}$. The p-rank of S can be deduced from the p-rank of E_1 and E_2 via the formula $r(S) = r(E_1) + r(E_2)$, see Proposition 2.28. Furthermore, the endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_q}(A)$ is isomorphic to the direct sum of $\mathrm{End}^0_{\mathbb{F}_q}(E_1)$ and $\mathrm{End}^0_{\mathbb{F}_q}(E_2)$ by Proposition 2.13(i).

Now assume that $S/\mathbb{F}_q$, with $q = p^n$, is simple. Then $f_S = h^e$, where h is an irreducible Weil polynomial and $e|4$ by Corollary 2.14. Also $e \neq 4$ by Theorem 2.15. Therefore, the polynomial f_S is either irreducible, or equal to the second power of an irreducible Weil polynomial. Theorem 2.22 implies that if f_S is irreducible, then $\mathrm{End}^0_{\mathbb{F}_q}(S) \cong \mathbb{Q}(\pi_S)$ with $[\mathbb{Q}(\pi_S) : \mathbb{Q}] = 4$. And if $f_S = h^2$, where h is an irreducible second degree Weil polynomial, then $\mathrm{End}^0_{\mathbb{F}_q}(S) \cong \mathcal{D}_S$. Here $\mathcal{D}_S$ is a central simple algebra over $\mathbb{Q}(\pi_S)$ which splits at all finite primes of $\mathbb{Q}(\pi_S)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_S)$.

Suppose $S/\mathbb{F}_q$ is supersingular. Then S is $\overline{\mathbb{F}_q}$-isogenous to the product of two supersingular elliptic curves and Proposition 2.28 implies that $r(S) = 0$. To prove the converse, assume that S is not supersingular. Then S is either $\overline{\mathbb{F}_q}$-isogenous to a product $E_1 \times E_2$ such that at least one elliptic curve is not supersingular, or S is absolutely simple. In the first case, at least one of E_1 and E_2 has p-rank 1 and it follows from Proposition 2.28 that $r(S) > 0$.

For the second case, let $S/\mathbb{F}_q$, with $q = p^n$, be absolutely simple and let f_S be the characteristic polynomial of Frobenius. Let π_S be a root of f_S and let $K = \mathbb{Q}(\pi_S)$. Gonzalez proved in [7, Theorem 3.7(ii)] that in this case $[K : \mathbb{Q}] = 4$ and $\mathrm{End}^0(S) \cong K$. Moreover, the factorization of $p\mathcal{O}_K$ into prime ideals, which only depends on $\mathrm{End}^0(S)$,

completely determines the p-rank $r(S)$. The possible factorizations of the ideal $p\mathcal{O}_K$ and the corresponding p-rank are summarized in Table 2.1. See [2, Example 3.9] by Bradford for a complete explanation.

Factorization of $p\mathcal{O}_K$	$r(S)$
$\mathfrak{p}^2\overline{\mathfrak{p}}^2$	2
$\mathfrak{p}\overline{\mathfrak{p}}$	2
$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$	1
$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$	1
$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$	2

Table 2.1: Factorizations of $p\mathcal{O}_K$ and corresponding p-ranks

For all possible factorizations of $p\mathcal{O}_K$ into prime ideals, it holds that $r(S) > 0$. Hence, if S is absolutely simple, then $r(S) > 0$. This shows that if S is not supersingular, then its p-rank is not zero. In other words, if $r(S) = 0$, then S is supersingular.

In the next chapter, we will study abelian varieties of dimension $g = 3$. If an abelian variety of dimension $g = 3$ is supersingular, then its p-rank is zero. But unlike as for elliptic curves and abelian surfaces, the converse does not hold. We will see in Table 3.2 that an abelian variety A of dimension $g = 3$ can satisfy $r(A) = 0$ without being supersingular. Moreover, for absolutely simple abelian varieties A of dimension $g = 3$, knowing the factorization of (p) in the maximal order of $\mathbb{Q}(\pi_A)$ is no longer sufficient to determine the p-rank $r(A)$. In addition, the factorization of the ideal (π_A) must be known. In Section 3.3.1 it will be shown that certain factorizations of the ideal (p) allow for multiple factorizations of the ideal (π_A), which correspond to different p-ranks.

Chapter 3

Abelian threefolds over finite fields

An abelian variety of dimension $g = 3$ is called an *abelian threefold*. The notation A is used for an abelian threefold. In this chapter, we will study abelian threefolds $A/\mathbb{F}_q$ defined over the finite field $\mathbb{F}_q$ of characteristic p. In Section 3.1, we first discuss the possible characteristic polynomials of the Frobenius endomorphism for a simple abelian threefold and the possible endomorphism algebras of an abelian threefold. Section 3.2 explains the relation between Newton polygons and the p-rank of an abelian threefold. Section 3.3 prepares for Theorem 3.17 which follows in Section 3.3.1. Theorem 3.17 is the main theorem of the thesis and gives a complete classification of the p-rank in terms of the splitting behaviour of the rational prime p in the maximal order of the number field $\mathbb{Q}(\pi_A)$ of an absolutely simple abelian threefold $A/\mathbb{F}_{p^n}$.

3.1 Characteristic polynomial and endomorphism algebras

Let $A/\mathbb{F}_q$ denote an arbitrary abelian threefold, let $S/\mathbb{F}_q$ denote an arbitrary simple abelian surface and let $E/\mathbb{F}_q, E_1/\mathbb{F}_q, E_2/\mathbb{F}_q$ and $E_3/\mathbb{F}_q$ denote arbitrary elliptic curves. Then we have the following possibilities:

- A is $\mathbb{F}_q$-isogenous to $E \times S$;
- A is $\mathbb{F}_q$-isogenous to $E_1 \times E_2 \times E_3$;
- A is simple, but not absolutely simple;

- A is absolutely simple.

If A is $\mathbb{F}_q$-isogenous to $E \times S$, then Theorem 2.14(ii) implies that the characteristic polynomial of Frobenius of A is given by $f_A = f_E f_S$. Furthermore, the p-rank of A can be deduced from the p-rank of E and S via the formula $r(A) = r(E) + r(S)$, see Proposition 2.28. In the same way, if A is $\mathbb{F}_q$-isogenous to $E_1 \times E_2 \times E_3$, then $f_A = f_{E_1} f_{E_2} f_{E_3}$ and the p-rank of A is given by $r(A) = r(E_1) + r(E_2) + r(E_3)$.

Proposition 3.1. Let $A/\mathbb{F}_q$, with $q = p^n$, be a simple abelian threefold and let f_A be the characteristic polynomial of Frobenius. Then f_A satisfies one of the following

(i) f_A is an irreducible Weil polynomial,

(ii) f_A is the third power of a second degree irreducible Weil polynomial.

Proof. Corollary 2.19 implies that $f_A = h^e$, where h is an irreducible Weil polynomial and e a positive integer dividing $2g = 6$. So a priori we have the following options for f_A:

(i) f_A is an irreducible Weil polynomial,

(ii) f_A is the second power of a third degree irreducible Weil polynomial,

(iii) f_A is the third power of a second degree irreducible Weil polynomial,

(iv) f_A is the sixth power of a linear Weil polynomial.

Theorem 2.15 states that in the last case, A is $\mathbb{F}_q$-isogenous to the third power of a supersingular elliptic curve. This contradicts with the assumption that A is simple. Therefore, the last option is not possible.

Suppose f_A is the second power of a third degree irreducible Weil polynomial. So $f_A = h^2$, where $\deg(h) = 3$ and h is an irreducible Weil polynomial. The polynomial h has three roots: a pair of complex conjugate roots and one real root. For all roots π_A of h it holds that $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 3$. Moreover, h is a Weil polynomial, so all the roots of h are Weil q-numbers. Let π_A be the real root of h. Then for all embeddings $\phi : \mathbb{Q}(\pi_A) \to \mathbb{C}$, it holds that $|\phi(\pi_A)| = q^{\frac{1}{2}}$. Let ϕ be the embedding given by $\phi(\pi_A) = \pi_A$. Then

$$|\phi(\pi_A)| = |\pi_A| = \pm\pi_A = q^{\frac{1}{2}}.$$

If $q = p^n$ with n even, then $q^{\frac{1}{2}} \in \mathbb{Q}$ and hence $\pi_A \in \mathbb{Q}$. If $q = p^n$ with n odd, then $q^{\frac{1}{2}} \in \mathbb{Q}(\sqrt{p})$ and hence $\pi_A \in \mathbb{Q}(\sqrt{p})$. Thus, if n is even, then $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 1$

and if n is odd, then $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 2$. This shows that the real root π_A of h does not satisfy $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 3$. Hence, f_A cannot be the second power of a third degree irreducible Weil polynomial.

The options for f_A that remain are

(i) f_A is irreducible,

(ii) f_A is the third power of a second degree irreducible polynomial. □

Next, we discuss the possible endomorphism algebras of an abelian threefold. We will first consider the possible endomorphism algebras over the finite field $\mathbb{F}_q$ of characteristic p of an abelian threefold $A/\mathbb{F}_q$. If A is $\mathbb{F}_q$-isogenous to a product of lower dimensional simple abelian varieties, then $\mathrm{End}^0_{\mathbb{F}_q}(A)$ is isomorphic to the direct sum of the endomorphism algebras of these lower dimensional simple abelian varieties by Proposition 2.13(i). Therefore, knowing the endomorphism algebras of elliptic curves, simple abelian surfaces and simple abelian threefolds is enough to determine the endomorphism algebra over $\mathbb{F}_q$ of any abelian threefold.

The endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(E)$ of an ordinary elliptic curve is isomorphic to the imaginary quadratic field $\mathbb{Q}(\pi_E)$ by Remark 1.22. For a supersingular elliptic curve, only the endomorphism algebra $\mathrm{End}^0(E)$ is known. In Section 2.3, we found that the endomorphism algebra of a simple abelian surface $S/\mathbb{F}_q$ depends on the characteristic polynomial of its Frobenius endomorphism. If f_S is irreducible, then $\mathrm{End}^0_{\mathbb{F}_q}(S)$ is isomorphic to $\mathbb{Q}(\pi_S)$ with $[\mathbb{Q}(\pi_S) : \mathbb{Q}] = 4$. If $f_S = h^2$, where h is an irreducible second degree Weil polynomial, then $\mathrm{End}^0_{\mathbb{F}_q}(S) \cong \mathcal{D}_S$.

The possible endomorphism algebras for a simple abelian threefold are very similar to those of a simple abelian surface. By Proposition 3.1, the characteristic polynomial of the Frobenius endomorphism of a simple abelian threefold $A/\mathbb{F}_q$ is either irreducible or the third power of a second degree irreducible Weil polynomial. Theorem 2.22 implies that if f_A is irreducible, then $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathbb{Q}(\pi_A)$ with $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 6$. And if $f_A = h^3$, where h is an irreducible second degree Weil polynomial, then $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathcal{D}_A$. Here $\mathcal{D}_A$ is a central simple algebra over $\mathbb{Q}(\pi_A)$ which splits at all finite primes of $\mathbb{Q}(\pi_A)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_A)$. The following example shows how the endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_q}(A)$ of an abelian variety $A/\mathbb{F}_q$ depends on the endomorphism algebras of the lower dimensional simple abelian varieties whose product is $\mathbb{F}_q$-isogenous to A.

Example 3.2. Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian threefold.

- If A is $\mathbb{F}_q$-isogenous to E^3, where $E/\mathbb{F}_q$ is an ordinary elliptic curve, then
$$\mathrm{End}^0_{\mathbb{F}_q}(A) \cong M_3(\mathrm{End}^0_{\mathbb{F}_q}(E)) \cong M_3(\mathbb{Q}(\pi_E)),$$
by Proposition 2.13(i).
- Assume A is $\mathbb{F}_q$-isogenous to $E \times S$, where $E/\mathbb{F}_q$ is an ordinary elliptic curve and $S/\mathbb{F}_q$ is a simple abelian surface with $f_S = h^2$, where h is a second degree irreducible Weil polynomial. Then $\mathrm{End}^0_{\mathbb{F}_q}(S) \cong \mathcal{D}_S$, where $\mathcal{D}_S$ is a central simple algebra over $\mathbb{Q}(\pi_S)$ which splits at all finite primes of $\mathbb{Q}(\pi_S)$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_S)$. Proposition 2.13(i) implies that
$$\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathrm{End}^0_{\mathbb{F}_q}(E) \oplus \mathrm{End}^0_{\mathbb{F}_q}(S) \cong \mathbb{Q}(\pi_E) \oplus \mathcal{D}_S.$$

We also determine the possible endomorphism algebras over the algebraic closure $\overline{\mathbb{F}_q}$ of $A/\mathbb{F}_q$ with $q = p^n$. If A is $\overline{\mathbb{F}_q}$-isogenous to a product of lower dimensional absolutely simple abelian varieties, then $\mathrm{End}^0(A)$ is isomorphic to the direct sum of the endomorphism algebras of these lower dimensional absolutely simple abelian varieties by Proposition 2.13(ii). Therefore, knowing the endomorphism algebras of elliptic curves, absolutely simple abelian surfaces and absolutely simple abelian threefolds is enough to determine the endomorphism algebra over $\overline{\mathbb{F}_q}$ of any abelian threefold.

The endomorphism algebra $\mathrm{End}^0(E)$ of a supersingular elliptic curve E is isomorphic to the quaternion algebra $B_{p,\infty}$ by Theorem 1.16. The endomorphism algebra $\mathrm{End}^0(E)$ of an ordinary elliptic curve E is isomorphic to the imaginary quadratic field $\mathbb{Q}(\pi_E)$ by Theorem 1.20. For an absolutely simple abelian surface $S/\mathbb{F}_q$, it holds that $\mathrm{End}^0(S) \cong \mathbb{Q}(\pi_S)$. The endomorphism algebra $\mathrm{End}^0(A)$ of an absolutely simple abelian threefold $A/\mathbb{F}_q$ can be isomorphic to $\mathbb{Q}(\pi_A)$ or to $\mathcal{D}_A$. If $A/\mathbb{F}_q$ is absolutely simple and ordinary, Gonzalez proved in [7, Theorem 3.6(i)] that $\mathrm{End}^0(A) \cong \mathbb{Q}(\pi_A)$ with $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 6$. This result will be proven in Section 3.2.

3.2 Newton polygons

In this section, we relate Newton polygons to the p-rank of an abelian threefold. The section is mainly based on Koblitz [10], Bradford [2] and Nart-Maisner [15].

We will be interested in the Newton polygon of a characteristic polynomial of the Frobenius of an abelian variety. Therefore, we start the construction of a Newton polygon

with a monic polynomial $f(x) = x^n + a_{n-1}x^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ and a prime p. We consider the set of points

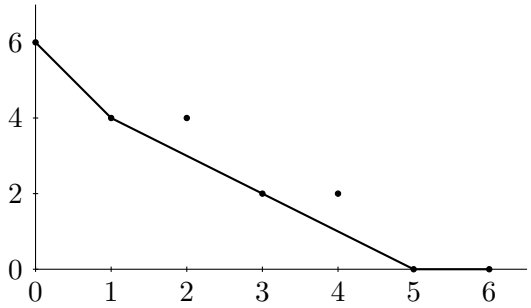
$$S_f = \{(0, \operatorname{ord}_p a_0), (1, \operatorname{ord}_p a_1), \ldots, (n-1, \operatorname{ord}_p a_{n-1}), (n, 0)\}.$$

The construction of the Newton polygon of f, denoted by $\mathrm{Np}_p(f)$, starts with drawing a vertical line l through the point $(0, \operatorname{ord}_p a_0)$. Then we rotate l counterclockwise until we hit another point in S_f for the first time. It can happen that at this point l touches multiple points in S_f at the same time. We then draw the line segment from $(0, \operatorname{ord}_p a_0)$ to the last point $(i_1, \operatorname{ord}_p a_{i_1})$ in S_f that l currently touches. This is the first line segment of $\mathrm{Np}_p(f)$. We continue rotating the line l counterclockwise until we hit another point in S_f for the first time. Again, it can happen that at this point l touches multiple points in S_f. We draw the line segment from $(i_1, \operatorname{ord}_p a_{i_1})$ to the last point $(i_2, \operatorname{ord}_p a_{i_2})$ in S_f that l currently touches. This is the second line segment of $\mathrm{Np}_p(f)$. This process is repeated until we have hit the point $(n, 0)$ and drawn the final line segment of $\mathrm{Np}_p(f)$.

Example 3.3. Let $f(x) = x^6+2x^5+50x^4+75x^3+1250x^2+1250x+15625$, an irreducible Weil polynomial for $q = 25$, and take the prime 5. Then

$$S_f = \{(0,6), (1,4), (2,4), (3,2), (4,2), (5,0), (6,0)\}$$

and the Newton polygon $\mathrm{Np}_5(f)$ is



The points where the slopes of a Newton polygon change are the vertices. If the points $(i, \operatorname{ord}_p a_i)$ and $(j, \operatorname{ord}_p a_j)$ are two vertices of a Newton polygon connected by a single line segment, then the slope of this segment is $(\operatorname{ord}_p a_j - \operatorname{ord}_p a_i)/(j - i)$. By the horizontal length, we mean the length of the projection of the segment onto the horizontal axis, so in this case $j - i$.

The following lemma by Koblitz is the first step in obtaining the relation between Newton polygons and the p-rank of an abelian threefold.

Lemma 3.4. ([10, IV Lemma 4]) Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian threefold with $f_A(x)$ the characteristic polynomial of Frobenius. Let K' be the splitting field

of f_A in $\mathbb{C}$ and let $f_A(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_6)$ be the factorization of f_A in K'. Assume that $\alpha_i \neq 0$ for $i = 1, \ldots, 6$. Let $\mathscr{P}$ be a prime ideal in K' lying above p. Let v be the extension of ord_p to K' induced by the prime $\mathscr{P}$ and let $\lambda_i = -v(\alpha_i)$. If λ is the slope of a segment of $\mathrm{Np}_p(f_A)$ having horizontal length m, then precisely m of the λ_i are equal to λ.

Proof. We can write

$$f_A(x) = \alpha_1\alpha_2\cdots\alpha_6\left(1-\frac{x}{\alpha_1}\right)\left(1-\frac{x}{\alpha_2}\right)\ldots\left(1-\frac{x}{\alpha_6}\right) = \alpha_1\alpha_2\cdots\alpha_6\tilde{f_A}(x).$$

Then $\tilde{f_A}(x) = 1 + \sum_{i=1}^{6} a_i x^i$ where the a_i's are expressed in terms of $\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \ldots, \frac{1}{\alpha_6}$ as $(-1)^i$ times the i-th symmetric polynomial

$$a_i = (-1)^i \sum_{k_1=1}^{6} \sum_{\substack{k_2=1 \\ k_2>k_1}}^{6} \cdots \sum_{\substack{k_i=1 \\ k_i>k_{i-1}}}^{6} \frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}.$$

Since $\tilde{f_A}$ is obtained by dividing f_A by the constant $\alpha_1\alpha_2\cdots\alpha_6 = q^3$, the Newton polygon $\mathrm{Np}_p(\tilde{f_A})$ differs from $\mathrm{Np}_p(f_A)$ by a horizontal shift. This does not change the slopes or lengths of the segments of the Newton polygon. Hence, it is sufficient to prove the lemma for $\mathrm{Np}_p(\tilde{f_A})$.

Without loss of generality, the α_i can be arranged such that $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_6$. Suppose $\lambda_1 = \lambda_2 = \ldots = \lambda_r$ and $\lambda_r < \lambda_{r+1}$ for some $r \in \{1, 2, \ldots, 6\}$. The Newton polygon $\mathrm{Np}_p(\tilde{f_A})$ is constructed from the set of points

$$S_{\tilde{f_A}} = \{(0,0), (1, \mathrm{ord}_p\, a_1), (2, \mathrm{ord}_p\, a_2), (3, \mathrm{ord}_p\, a_3), (4, \mathrm{ord}_p\, a_4), (5, \mathrm{ord}_p\, a_5), (6, \mathrm{ord}_p\, a_6)\}.$$

Claim. The first segment of $\mathrm{Np}_p(\tilde{f_A})$ is the segment joining $(0,0)$ and $(r, r\lambda_1)$.

Proof of the claim. Let $i \in \{1, 2, \ldots, 6\}$ and let $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}$ be any product appearing in the sum that forms a_i. Then

$$\begin{aligned} v\left(\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}\right) &= -v(\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}) \\ &= -v(\alpha_{k_1}) - v(\alpha_{k_2}) - \ldots - v(\alpha_{k_i}) \\ &= \lambda_{k_1} + \lambda_{k_2} + \ldots + \lambda_{k_i} \\ &\geq i\lambda_1. \end{aligned}$$

It follows that $\mathrm{ord}_p\, a_i \geq i\lambda_1$. This shows that every point $(i, \mathrm{ord}_p\, a_i)$ is on or above the point $(i, i\lambda_1)$ and hence lies either on or above the line joining $(0,0)$ and $(r, r\lambda_1)$.

Next, we will show that $\operatorname{ord}_p a_r = r\lambda_1$. This implies that the point $(r, \operatorname{ord}_p a_r)$ lies on the line joining $(0,0)$ and $(r, r\lambda_1)$. The term $\frac{1}{\alpha_1 \cdots \alpha_r}$ appears in a_r and

$$\begin{aligned} v\left(\frac{1}{\alpha_1 \cdots \alpha_r}\right) &= -v(\alpha_1 \cdots \alpha_r) \\ &= -v(\alpha_1) - \ldots - v(\alpha_r) \\ &= \lambda_1 + \ldots + \lambda_r = r\lambda_1. \end{aligned}$$

Every other term appearing in the sum that forms a_r has at least one α_j in the denominator with $j > r$ and the valuation of this term is therefore strictly larger than $r\lambda_1$. Since $\operatorname{ord}_p a_i$ is equal to the minimum of the valuations of each term in the sum, it follows that $\operatorname{ord}_p a_i = r\lambda_1$.

Consider a_i with $i > r$. Then every term in a_i is of the form $\frac{1}{\alpha_{k_1} \cdots \alpha_{k_i}}$ and hence contains at least one α_j in the denominator with $j > r$. Since $v\left(\frac{1}{\alpha_j}\right) = \lambda_j > \lambda_1$, the valuation of each term in a_i is strictly larger than $i\lambda_1$. Hence, $\operatorname{ord}_p a_i > i\lambda_1$ and the point $(i, \operatorname{ord}_p a_i)$ lies above the line joining $(0,0)$ and $(r, r\lambda_1)$. □

The claim states that the first segment of $\operatorname{Np}_p(\tilde{f_A})$ is the line segment joining $(0,0)$ and $(r, r\lambda_1)$, which has horizontal length r. The slope of this segment is λ_1 and precisely r of the λ_i are equal to λ_1.

If $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \ldots = \lambda_{s+r} < \lambda_{s+r+1}$ for some integers $1 \leq s \leq 5$ and $1 \leq r \leq 6-s$, then the line segment joining $(s, \lambda_1 + \lambda_2 + \ldots + \lambda_s)$ and $(s+r, \lambda_1 + \lambda_2 + \ldots + \lambda_s + r\lambda_{s+1})$ is a line segment of $\operatorname{Np}_p(\tilde{f_A})$. The proof of this is completely analogous to the proof of the claim. The segment joining $(s, \lambda_1 + \lambda_2 + \ldots + \lambda_s)$ and $(s + r, \lambda_1 + \lambda_2 + \ldots + \lambda_s + r\lambda_{s+1})$ has horizontal length r. Moreover, this segment has slope λ_{s+1} and precisely r of the λ_i are equal to λ_{s+1}. □

Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian threefold and let f_A be the characteristic polynomial of the Frobenius of A. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_6\}$ be the complete set of roots of f_A and let K' be the splitting field of f_A in $\mathbb{C}$. Let $\mathscr{P}$ be a prime ideal in K' lying above p. Let v be the extension of ord_p to K' induced by the prime $\mathscr{P}$ and let $\lambda_i = -v(\alpha_i)$ for $i = 1, \ldots, 6$. By Gonzalez [7, Proposition 3.1(ii)], it holds that

$$r(A) = \#\{\alpha_i \notin \mathscr{P} : 1 \leq i \leq 6\}. \tag{3.1}$$

For a root α_i of f_A, we have $\alpha_i \notin \mathscr{P}$ if and only if $\operatorname{ord}_{\mathscr{P}} \alpha_i = 0$. So $\alpha_i \notin \mathscr{P}$ if and only if $v(\alpha_i) = 0$ by definition of v. Hence, equation (3.1) is equivalent to

$$r(A) = \#\{v(\alpha_i) = 0 : 1 \leq i \leq 6\}.$$

Now consider the segment of $\mathrm{Np}_p(f_A)$ with slope equal to zero and let m be the horizontal length of this segment. Then we obtain

$$m = \#\{v(\alpha_i) = 0 : 1 \leq i \leq 6\}$$

by Lemma 3.4. This proves the following proposition.

Proposition 3.5. Let $A/\mathbb{F}_q$, with $q = p^n$, be an abelian threefold and let f_A be the characteristic polynomial of Frobenius. The horizontal length of the zero-slope segment of $\mathrm{Np}_p(f_A)$ is equal to the p-rank $r(A)$.

Let $A/\mathbb{F}_q$ be a simple abelian threefold with $f_A = h^3$, where h is a second degree irreducible Weil polynomial. Using the Newton polygon of f_A, we will prove that $r(A) = 0$. For this we need the following proposition by Maisner and Nart.

Proposition 3.6. ([15, Proposition 2.5]) Let $\beta \in \mathbb{Z}$ with $|\beta| < 2\sqrt{q}$, and let $b = v_p(\beta)$. Let $h(x) = x^2 - \beta x + q$ and let $D = \beta^2 - 4q$ be the discriminant of $h(x)$. Let $A/\mathbb{F}_q$, with $q = p^n$, be a simple abelian variety with $f_A = h^e$. Then

$$\dim(A) = \begin{cases} \frac{n}{\gcd(n,b)} & \text{if } b < \frac{n}{2}, \\ 2 & \text{if } b \geq \frac{n}{2},\ D \in \mathbb{Q}_p^{*2}, \\ 1 & \text{if } b \geq \frac{n}{2},\ D \notin \mathbb{Q}_p^{*2}. \end{cases}$$

Proof. The degree of f_A is $2e$. Since the characteristic polynomial of Frobenius of an abelian variety of dimension g has degree $2g$, the dimension of A is equal to e. Moreover, the integer e is the least common denominator of the invariants of $\mathrm{End}^0_{\mathbb{F}_q}(A)$ by Theorem 2.24 and Theorem 2.25. The invariants at the finite places lying above p are $\frac{v_p(h_\nu(0))}{n}$, where ν runs among the finite places of $\mathbb{Q}(\pi_A)$ lying above p and $h_\nu(x)$ denotes the corresponding factor of $h(x)$ in $\mathbb{Q}_p[x]$.

Assume $D \notin \mathbb{Q}_p^{*2}$, so D is not a square in $\mathbb{Q}_p$. Then the roots of $h(x)$ are not in $\mathbb{Q}_p$ and hence $h(x)$ is irreducible in $\mathbb{Q}_p[x]$. It holds that $v_p(h(0)) = v_p(q) = v_p(p^n) = n$. Hence, the integer e is equal to the denominator of $\frac{n}{n} = 1$, so $e = 1$.

Next, assume $D \in \mathbb{Q}_p^{*2}$, so D is a nonzero square in $\mathbb{Q}_p$. Then the roots of $h(x)$ are in $\mathbb{Q}_p$ and hence $h(x)$ factors in $\mathbb{Q}_p[x]$ as $h_1(x)h_2(x)$. Let $b_1 = v_p(h_1(0))$ and $b_2 = v_p(h_2(0))$. It holds that

$$h(x) = (x + h_1(0))(x + h_2(0)) = x^2 + (h_1(0) + h_2(0))x + h_1(0)h_2(0),$$

so $-\beta = h_1(0) + h_2(0)$ and $q = h_1(0)h_2(0)$. Thus

$$\begin{aligned} n &= v_p(q) = v_p(h_1(0)h_2(0)) = v_p(h_1(0)) + v_p(h_2(0)) = b_1 + b_2, \\ b &= v_p(\beta) = v_p(-\beta) = v_p(h_1(0) + h_2(0)) = \min\{v_p(h_1(0)), v_p(h_2(0))\} = \min\{b_1, b_2\}. \end{aligned}$$

Suppose $b \geq \frac{n}{2}$. Then $\min\{b_1, b_2\} \geq \frac{n}{2}$ while $b_1 + b_2 = n$. It follows that $b_1 = b_2 = \frac{n}{2}$. Hence, e is equal to the denominator of $\frac{b_1}{n} = \frac{b_2}{n} = \frac{1}{2}$, so $e = 2$.

Suppose $b < \frac{n}{2}$. Then $b = \min\{b_1, b_2\}$ and $b_1 + b_2 = n$. Without loss of generality it holds that $b_1 = b$ and $b_2 = n - b$. Hence, e is the least common denominator of $\frac{b_1}{n} = \frac{b}{n}$ and $\frac{b_2}{n} = \frac{n-b}{n}$, so $e = \frac{n}{\gcd(n,b)}$. □

Theorem 3.7. Let $A/\mathbb{F}_q$, with $q = p^n$, be a simple abelian threefold with $f_A = h^3$, where h is a second degree irreducible Weil polynomial. Then $r(A) = 0$.

Proof. The polynomial $f_A = h^3$ is the characteristic polynomial of Frobenius of the abelian threefold $A/\mathbb{F}_q$. Therefore, the constant term of f_A is equal to q^3. It follows that the constant term of h is q. Hence, we have $h(x) = x^2 - \beta x + q$ for some integer β.

Suppose $|\beta| \geq 2\sqrt{q}$. If $\beta = \pm 2\sqrt{q} \in \mathbb{Z}$, then

$$h(x) = x^2 \pm 2\sqrt{q}x + q = (x \pm \sqrt{q})^2,$$

so $h(x)$ is not irreducible. This is a contradiction. The roots of h are $\frac{\beta \pm \sqrt{\beta^2 - 4q}}{2}$. If $|\beta| > 2\sqrt{q}$, then the roots of h are real and one of the roots of h has absolute value equal to $\frac{|\beta| + \sqrt{\beta^2 - 4q}}{2}$. Since h is a Weil polynomial, the roots of h are Weil q-numbers. Therefore, it holds that

$$\frac{|\beta| + \sqrt{\beta^2 - 4q}}{2} = \sqrt{q}.$$

Since $\frac{1}{2}\sqrt{\beta^2 - 4q} > 0$, it follows that $\frac{|\beta|}{2} < \sqrt{q}$. Thus, we find $|\beta| < 2\sqrt{q}$, which is a contradiction. Hence, we have $|\beta| < 2\sqrt{q}$.

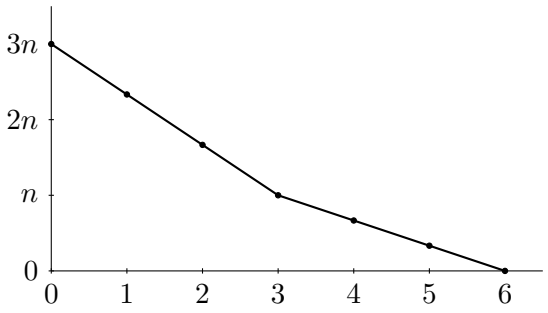
By Proposition 3.6, the simple abelian variety corresponding to h has dimension $g = 3$ only if $v_p(\beta) < \frac{n}{2}$ and $\frac{n}{\gcd(n, v_p(\beta))} = 3$. Thus, we have $3|n$ and $\gcd(n, v_p(\beta)) = \frac{n}{3}$, so $v_p(\beta) \geq \frac{n}{3} \geq 1$. Expanding the equation $f_A(x) = (x^2 - \beta x + q)^3$ gives

$$f_A(x) = x^6 - 3\beta x^5 + (3\beta^2 + 3q)x^4 - (\beta^3 + 6\beta q)x^3 + (3\beta^2 q + 3q^2)x^2 - 3\beta q^2 x + q^3. \quad (3.2)$$

Since $v_p(\beta) \geq 1$, each coefficient a_i of f_A satisfies $\mathrm{ord}_p a_i > 0$. Hence, the Newton polygon $\mathrm{Np}_p(f_A)$ has no zero-slope segment and therefore the p-rank of A is zero by Proposition 3.5. □

Remark 3.8. Xing [23] proved that a simple abelian threefold $A/\mathbb{F}_q$ satisfies $f_A = h^3$ if and only if $3|n$ and $\beta = aq^{\frac{1}{3}}$, where a is an integer coprime with p. The statement of this result can also be found in Haloui [8, Proposition 1.2]. Hence, if $A/\mathbb{F}_q$ is a simple

abelian threefold with $f_A = h^3$, where h is an irreducible second degree Weil polynomial, then the Newton polygon of f_A (given in (3.2)) is



In the next section, we will study the p-rank of simple abelian threefolds $A/\mathbb{F}_q$ for which the characteristic polynomial of Frobenius f_A is irreducible. We will relate the p-rank to the factorization of the ideals (p) and (π_A) into prime ideals in the maximal order of the field $K = \mathbb{Q}(\pi_A)$, where π_A is a root of f_A. Recall that in Section 3.1, we stated that if an abelian threefold $A/\mathbb{F}_q$ is ordinary and absolutely simple, then $\mathrm{End}^0(A) \cong \mathbb{Q}(\pi_A)$ with $[\mathbb{Q}(\pi_A) : \mathbb{Q}] = 6$. At this point, all the results needed to prove this statement are obtained. The statement is a direct consequence of the following theorem by Gonzalez.

Theorem 3.9. ([7, Theorem 3.6(i)]) Let $A/\mathbb{F}_q$ be an ordinary simple abelian threefold. Then $\mathrm{End}^0_{\mathbb{F}_q}(A)$ is commutative and $\mathrm{End}^0_{\mathbb{F}_q} \cong \mathbb{Q}(\pi_A)$. In particular, if A is ordinary and absolutely simple, then $\mathrm{End}^0(A)$ is commutative.

Proof. Since $A/\mathbb{F}_q$ is simple, the polynomial f_A is irreducible or $f_A = h^3$, where h is a second degree irreducible Weil polynomial by Proposition 3.1. If $f_A = h^3$, then Theorem 3.7 implies that the p-rank of $A/\mathbb{F}_q$ is zero, which is a contradiction. Therefore, the polynomial f_A is irreducible and $\mathrm{End}^0_{\mathbb{F}_q}(A) \cong \mathbb{Q}(\pi_A)$ by Theorem 2.22(i).

Let r be any positive integer and consider $A/\mathbb{F}_{q^r}$. Since $A/\mathbb{F}_q$ is absolutely simple and ordinary, the abelian threefold $A/\mathbb{F}_{q^r}$ is simple and ordinary. Let π_A be the Frobenius of $A/\mathbb{F}_q$. Then π_A^r is the Frobenius of $A/\mathbb{F}_{q^r}$. Let f'_A be the characteristic polynomial of π_A^r. Since $A/\mathbb{F}_{q^r}$ is simple, the polynomial f'_A is irreducible or $f'_A = h'^3$, where h' is a second degree irreducible Weil polynomial by Proposition 3.1. If $f'_A = h'^3$, then Theorem 3.7 implies that $r(A/\mathbb{F}_{q^r}) = r(A/\mathbb{F}_q) = 0$, which is a contradiction. Therefore, the polynomial f'_A is irreducible and $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A) \cong \mathbb{Q}(\pi_A^r)$ by Theorem 2.22(i). It follows that $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ is commutative for every integer $r > 0$. Hence, the endomorphism algebra $\mathrm{End}^0(A)$ is commutative. □

Remark 3.10. Let $A/\mathbb{F}_q$ be a simple abelian threefold. Theorem 3.9 implies that if $A/\mathbb{F}_q$ is ordinary, then the converse of Proposition 2.29 and Corollary 2.30 holds for abelian varieties of dimension $g = 3$. Namely, if $A/\mathbb{F}_q$ is absolutely simple and ordinary, then $\mathrm{End}^0_{\mathbb{F}_q}(A)$ and $\mathrm{End}^0(A)$ are commutative by Theorem 3.9. Therefore, we have $\mathrm{End}^0(A) \cong \mathbb{Q}(\pi_A) \cong \mathrm{End}^0_{\mathbb{F}_q}(A)$. Since $\mathrm{End}^0_{\mathbb{F}_q}(A) \subseteq \mathrm{End}^0_{\mathbb{F}_{q^r}}(A) \subseteq \mathrm{End}^0(A)$ for all integers $r > 0$ and $\mathrm{End}^0_{\mathbb{F}_q}(A) = \mathrm{End}^0(A)$, it follows that $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ for all integers $r > 0$. Moreover, we have $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A) = \mathrm{End}^0_{\mathbb{F}_q}(A)$ for all integers $r > 0$, so their centers are also equal for all integers $r > 0$. Since $\mathbb{Q}(\pi_A^r)$ is the center of $\mathrm{End}^0_{\mathbb{F}_{q^r}}(A)$ and $\mathbb{Q}(\pi_A)$ is the center of $\mathrm{End}^0_{\mathbb{F}_q}(A)$ by Theorem 2.10, it holds that $\mathbb{Q}(\pi_A^r) = \mathbb{Q}(\pi_A)$ for all integers $r > 0$.

3.3 Relation between p-rank and decomposition of p

Let $A/\mathbb{F}_q$ be a simple abelian variety with f_A the characteristic polynomial of Frobenius. Throughout this section, we assume f_A is irreducible. Let π_A be a root of f_A and let $K = \mathbb{Q}(\pi_A)$. In this section, we relate the p-rank of A to the factorization of the ideal $p\mathcal{O}_K$ into prime ideals and show that for an absolutely simple abelian threefold, there exists at least one prime ideal $\mathfrak{p}$ in K above p such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. The section is based on Bradford [2] and Gonzalez [7]. We first prove two lemmas by Bradford.

Lemma 3.11. ([2, Proposition 3.1]) Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ and let $K' = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$. 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 K', let $a \coloneqq \mathrm{ord}_{\mathscr{P}_0}(\alpha)$ and let N be the number of roots of f with $\mathscr{P}_0$-adic valuation equal to a. Then

$$N = d\left(\frac{\#\{\mathscr{P} : \mathscr{P}|p,\ \mathrm{ord}_{\mathscr{P}}(\alpha) = a\}}{\#\{\mathscr{P} : \mathscr{P}|p\}}\right),$$

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

Proof. The field $K' = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ is the splitting field of f, so K' is a Galois extension. Let $G = \mathrm{Gal}(K'/\mathbb{Q})$. Let $H \leq G$ denote the stabilizer of α and $D \leq G$ the stabilizer of $\mathscr{P}_0$. The group G acts transitively on the roots of f. Therefore, there exists an element $\tau \in G$ such that $\tau(\alpha_i) = \alpha_j$ for every two roots α_i and α_j of f. Hence, we can pick elements $\tau_i \in G$ satisfying $\tau_i(\alpha_i) = \alpha$ for all $i \in \{1, 2, \ldots, d\}$.

Suppose we take an element $\tau \in H\tau_i \cap H\tau_j$. Then $\tau \in H\tau_i$ and hence there exists $h \in H$ such that $\tau = h\tau_i$. We have

$$\tau(\alpha_i) = h(\tau_i(\alpha_i)) = h(\alpha) = \alpha,$$

since h is in the stabilizer group of α. Similarly, $\tau(\alpha_j) = \alpha$. Since τ is an isomorphism and f has distinct roots (f is irreducible), it must hold that $i = j$. This shows that the sets $H\tau_i$ with $i \in \{1, \dots, d\}$ are pairwise distinct. Moreover, the union of these sets is G. Hence, the sets $H\tau_i$, with $1 \leq i \leq d$, are the right cosets of H.

By relabeling the roots of f if necessary, we can assume without loss of generality that

- $\mathrm{ord}_{\mathscr{P}_0}(\alpha_1) = \mathrm{ord}_{\mathscr{P}_0}(\alpha_2) = \cdots = \mathrm{ord}_{\mathscr{P}_0}(\alpha_N) = a$,
- $\mathrm{ord}_{\mathscr{P}_0}(\alpha_i) \neq a$ if $i > N$,

for some integer N with $1 \leq N \leq d$.

For an element $\tau \in G$ and a prime $\mathscr{P}$ lying above p in K', it holds that $\tau(\mathscr{P})$ is also a prime lying above p in K'. Moreover, G acts transitively on the primes $\mathscr{P}$ lying above p in K'. It follows that $\{\mathscr{P} : \mathscr{P}|p\} \subset \{\tau(\mathscr{P}_0) : \tau \in G\}$. The set $\{\tau(\mathscr{P}_0) : \tau \in G\}$ has $|G|$ elements, which are not necessarily distinct. Let $\{\mathscr{P} : \mathscr{P}|p\} = \{\mathscr{P}_1, \dots, \mathscr{P}_m\}$. There exist $\tau_1, \dots, \tau_m \in G$ such that $\tau_i(\mathscr{P}_0) = \mathscr{P}_i$ for $i \in \{1, \dots, m\}$. For every $\tau \in D$, it holds that $\tau(\mathscr{P}_0) = \mathscr{P}_0$. Thus, we have $\tau_i(\tau(\mathscr{P}_0)) = \tau_i(\mathscr{P}_0) = \mathscr{P}_i$. This shows that

$$\{\mathscr{P} : \mathscr{P}|p\} = \frac{\{\tau(\mathscr{P}_0) : \tau \in G\}}{|D|} = \frac{|G|}{|D|} = [G : D]. \tag{3.3}$$

Moreover,

$$\begin{aligned} \{\mathscr{P} : \mathscr{P}|p,\ \mathrm{ord}_{\mathscr{P}}(\alpha) = a\} &= \frac{\{\tau(\mathscr{P}_0) : \mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = a,\ \tau \in G\}}{|D|} \\ &= \frac{\{\tau : \mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = a\}}{|D|}. \end{aligned} \tag{3.4}$$

Claim. It holds that $\mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = \mathrm{ord}_{\mathscr{P}_0}\left(\tau^{-1}(\alpha)\right)$.

Proof. Suppose $\mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = k$. Then the prime ideal $\tau(\mathscr{P}_0)$ appears precisely k times in the factorization of the ideal (α) into prime ideals in K'. As τ is an isomorphism, applying τ^{-1} to the ideal (α) gives $\tau^{-1}((\alpha)) = \left(\tau^{-1}(\alpha)\right)$. To find the factorization of $\left(\tau^{-1}(\alpha)\right)$ into prime ideals, we have to apply τ^{-1} to the prime factorization of (α). It follows that $\tau^{-1}(\tau(\mathscr{P}_0)) = \mathscr{P}_0$ appears precisely k times in the factorization of $(\tau^{-1}(\alpha))$ into prime ideals. Hence, $\mathrm{ord}_{\mathscr{P}_0}(\tau^{-1}(\alpha)) = k$.

Suppose $\mathrm{ord}_{\mathscr{P}_0}\left(\tau^{-1}(\alpha)\right) = k$. Then applying τ to the ideal $\left(\tau^{-1}(\alpha)\right)$ and to the factorization of this ideal into prime ideals in K' shows that $\mathrm{ord}_{\tau(\mathscr{P}_0)}(\alpha) = k$. □

Using equations (3.3), (3.4) and the claim, we find

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

where we used that $H\tau_i$, with $1 \leq i \leq d$, are the right cosets of H in the last line. □

Lemma 3.12. ([2, Proposition 3.4]) Let f, K' and α be as in Lemma 3.11. Let $K = \mathbb{Q}(\alpha)$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ the primes of K lying above p. For each $\mathfrak{p}_i$, denote the ramification index of $\mathfrak{p}_i$ over p by e_i, and the degree of the extension of residue fields for $\mathfrak{p}_i$ over p by f_i. Let e be the ramification index of p in K' and $\frac{a}{e}$ be a slope of a segment of $\mathrm{Np}_p(f)$ with length N. Let $S_a = \{i : \mathrm{ord}_{\mathfrak{p}_i}(\alpha) = \frac{ae_i}{e},\ 1 \leq i \leq s\}$. Then

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

Proof. Since K' is the Galois closure of K in $\mathbb{C}$, the field K' is also Galois over K. We denote the number of primes in K' that lie above $\mathfrak{p}_i$ by g_i. Since K' is Galois over K, it follows that every prime in K' lying above $\mathfrak{p}_i$ has the same ramification index and the same degree of the extension of residue fields with respect to $\mathfrak{p}_i$. Thus, if we let a_i be the ramification index and b_i the degree of the extension of residue fields of a prime in K' lying above $\mathfrak{p}_i$, then we get

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

Since K' is Galois over $\mathbb{Q}$, it also holds that every prime in K' lying above p has the same ramification index and degree of the extension of residue fields with respect to p. Define m to be the degree of the extension of residue fields with respect to p in K'.

Then $a_i e_i = e$ and $b_i f_i = m$ for all $1 \leq i \leq s$. Dividing equation (3.5) through by em gives

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

We will now use Lemma 3.11. We have $\#\{\mathscr{P} : \mathscr{P}|p\} = \sum_{i=1}^{s} g_i$. Suppose $\mathscr{P}$ is a prime in K' that lies above $\mathfrak{p}_i$. Then $\mathrm{ord}_{\mathscr{P}}(\alpha) = a$ if and only if $\mathrm{ord}_{\mathfrak{p}_i}(\alpha) = \frac{a}{a_i} = \frac{ae_i}{e}$. Define $S_i \coloneqq \{\mathscr{P} : \mathscr{P}|\mathfrak{p}_i\}$ for $1 \leq i \leq s$. Then $|S_i| = g_i$. By Lemma 3.11, we have

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

Now we have proved the two lemmas above, we are ready for the theorem that relates the p-rank of a simple abelian variety $A/\mathbb{F}_q$, with f_A irreducible, to the factorization of the ideal (p) in the maximal order of $\mathbb{Q}(\pi_A)$ into prime ideals.

Theorem 3.13. ([2, Theorem 3.6]) Let A be a simple abelian variety of dimension g over the finite field $\mathbb{F}_q$ with $q = p^n$. Let f_A be the characteristic polynomial of π_A and suppose f_A is irreducible. Let π_A be a root of f_A, let $K = \mathbb{Q}(\pi_A)$ and let $K_+ = \mathbb{Q}(\beta)$, where $\beta = \pi_A + \overline{\pi_A}$. For each prime $\mathfrak{p}$ in K lying above p and each prime $\mathfrak{P}$ in K_+ lying above p, let $e(\mathfrak{p})$ and $e(\mathfrak{P})$ be the ramification index of $\mathfrak{p}$ and $\mathfrak{P}$ with respect to p, and let $f(\mathfrak{p})$ and $f(\mathfrak{P})$ be the degree of the extension of $\mathbb{Z}/p\mathbb{Z}$ corresponding to $\mathfrak{p}$ and $\mathfrak{P}$. Then

$$r(A) = \sum_{\pi_A \notin \mathfrak{p},\ \mathfrak{p}|p} e(\mathfrak{p}) f(\mathfrak{p}), \tag{3.6}$$

and

$$r(A) = \sum_{\beta \notin \mathfrak{P},\ \mathfrak{P}|p} e(\mathfrak{P}) f(\mathfrak{P}). \tag{3.7}$$

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes of K lying above p and let

$$S_0 = \{i : \mathrm{ord}_{\mathfrak{p}_i}(\pi_A) = 0,\ 1 \leq i \leq s\}.$$

For each $\mathfrak{p}_i$, denote the ramification index over p by e_i, and the degree of the extension of residue fields over p by f_i. The p-rank $r(A)$ is the length of the zero-slope segment of $\mathrm{Np}_p(f_A)$ by Proposition 3.5. Thus, if we take $a = 0$ and $\alpha = \pi_A$ in Lemma 3.12, we obtain

$$r(A) = \sum_{i \in S_0} e_i f_i. \tag{3.8}$$

For the primes $\mathfrak{p}$ in S_0, we have $\mathrm{ord}_{\mathfrak{p}}(\pi_A) = 0$, which holds if and only if $\mathfrak{p}$ does not contain π_A. Thus the primes in S_0 are precisely the primes in K over p that do not contain π_A. Hence, equation (3.8) is equivalent to

$$r(A) = \sum_{\pi_A \notin \mathfrak{p},\ \mathfrak{p}|p} e(\mathfrak{p}) f(\mathfrak{p}).$$

The next step is to show the equivalence of (3.6) and (3.7). Let $\mathfrak{P}$ be a prime in K_+ lying above p that does not contain β. As $[K : K_+] = 2$, the prime $\mathfrak{P}$ can be inert, it can split as $\mathfrak{p}\overline{\mathfrak{p}}$ or it can ramify as $\mathfrak{p}^2$ in K. Suppose there is only one prime in K lying above $\mathfrak{P}$, so $\mathfrak{P}$ is inert or ramifies in K. The prime p is contained in all primes in K lying above p, so in particular in all primes in K lying above $\mathfrak{P}$, and $\pi_A\overline{\pi_A} = q = p^n$. Hence, $\pi_A\overline{\pi_A}$ is contained in all primes lying above $\mathfrak{P}$ in K. It follows that π_A and $\overline{\pi_A}$ are both contained in the unique prime in K lying above $\mathfrak{P}$. Therefore $\beta = \pi_A + \overline{\pi_A}$ is also contained in the unique prime in K lying above $\mathfrak{P}$ and hence in $\mathfrak{P}$, which is a contradiction. Therefore, $\mathfrak{P}$ splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$.

Since $\mathfrak{P}$ splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$ and K is a quadratic extension of K_+, it follows that

$$e(\mathfrak{P}) = e(\mathfrak{p}) = e(\overline{\mathfrak{p}}) \qquad \text{and} \qquad f(\mathfrak{P}) = f(\mathfrak{p}) = f(\overline{\mathfrak{p}}).$$

Moreover, as $\pi_A\overline{\pi_A} = q = p^n$ is contained in $\mathfrak{p}$ and in $\overline{\mathfrak{p}}$ and π_A cannot be contained in both (otherwise $\beta \in \mathfrak{P}$), exactly one of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ contains π_A. In other words, exactly one of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ does not contain π_A and hence appears in the sum of (3.6). This shows that every summand of (3.7) appears in (3.6).

Let $\mathfrak{p}$ be a prime in K that does not contain π_A. Since $\pi_A\overline{\pi_A} = p^n \in \mathfrak{p}$, it holds that $\overline{\pi_A} \in \mathfrak{p}$. It follows that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Let $\mathfrak{P} = \mathfrak{p} \cap \mathcal{O}_{K_+}$. Then $\mathfrak{P}$ splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$ and hence $e(\mathfrak{P}) = e(\mathfrak{p})$ and $f(\mathfrak{P}) = f(\mathfrak{p})$. Moreover, $\beta \notin \mathfrak{P}$ as $\overline{\pi_A} \in \mathfrak{p}$, but $\pi_A \notin \mathfrak{p}$. This shows that every summand of (3.6) appears in (3.7). □

Besides Theorem 3.13, the next proposition by Gonzalez will also be of great use in Section 3.3.1. We first prove a lemma.

Lemma 3.14. Let $K = \mathbb{Q}(\pi)$ be a number field of degree r. If $u \in \mathcal{O}_K^*$ and $|\phi(u)| = 1$ for all embeddings $\phi : K \to \mathbb{C}$, then u is a root of unity.

Proof. Since $u \in K$, there is a polynomial $g(x) \in \mathbb{Q}[x]$ such that $u = g(\pi)$. Let $\phi_1, \ldots, \phi_r$ be the embeddings of K. Let $f_n(x) = \prod_{i=1}^{r}(x - \phi_i(u)^n)$, where n is any positive integer. The coefficients of f_n are, up to sign, symmetric polynomials in $\phi_1(u), \ldots, \phi_r(u)$. For each embedding $\phi_i : K \to \mathbb{C}$, it holds that $\phi_i(u) = \phi_i(g(\pi)) = g(\phi_i(\pi))$. It follows that every symmetric polynomial in $\phi_1(u), \ldots, \phi_r(u)$ is a symmetric polynomial in $\phi_1(\pi), \ldots, \phi_r(\pi)$, which are precisely the roots of the minimal polynomial f of π. The fundamental theorem of symmetric polynomials states that any symmetric polynomial in the roots of a monic polynomial h can be expressed as a polynomial in the coefficients of h. This implies that any symmetric polynomial in $\phi_1(u), \ldots, \phi_r(u)$ can be expressed as a polynomial in the coefficients of f. Hence, f_n has integer coefficients for all positive integers n.

Let k be an integer satisfying $0 \leq k \leq r$. The coefficient of x^k in f_n is equal to $(-1)^{r-k}$ times the $(r-k)$-th symmetric polynomial in $\phi_1(u)^n, \ldots, \phi_r(u)^n$. Thus, the coefficient of x^k is a sum of $\binom{r}{k}$ terms. Since by assumption $|\phi_i(u)| = 1$ for $i = 1, \ldots, r$, the absolute value of the coefficient of x^k is $\binom{r}{k}$. Hence, all the coefficients of f_n are bounded by a value independent of n. Moreover, the coefficients of f_n are integers. Therefore, there are only finitely many possibilities for the coefficients of f_n, so only finitely many polynomials occur in the infinite sequence $\{f_n\}_{n\in\mathbb{N}}$. In particular, only finitely many polynomials occur in the infinite subsequence $\{f_{2^n}\}_{n\in\mathbb{N}}$. Thus, there exist integers k, l with $k \geq 0$ and $l > 0$ such that $f_{2^k} = f_{2^{k+l}}$. Then the set of roots of f_{2^k} is equal to the set of roots of $f_{2^{k+l}}$. This means that raising the roots of f_{2^k} to the power 2^l permutes the roots of f_{2^k}. There exists a positive integer m such that performing this permutation m times, results in the identity permutation. Hence, we have $\phi_i(u)^{2^k} = \phi_i(u)^{2^{k+lm}}$ for all $i \in \{1, \ldots, r\}$. It follows that every $\phi_i(u)$, specifically u itself, is a root of unity. □

Proposition 3.15. ([7, Proposition 3.2(iii)]) Let $A/\mathbb{F}_q$ be a simple abelian threefold with Frobenius π_A and let $K = \mathbb{Q}(\pi_A)$. Then A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve if and only if $(\pi_A) = (\overline{\pi_A})$ in K.

Proof. Assume $(\pi_A) = (\overline{\pi_A})$. Then

$$(\pi_A^2) = (\pi_A)^2 = (\pi_A)(\pi_A) = (\pi_A)(\overline{\pi_A}) = (\pi_A\overline{\pi_A}) = (q),$$

so there exists a unit $u \in \mathcal{O}_K$ such that $\pi_A^2 = qu$. Since π_A is a Weil q-number, see Theorem 2.18, it holds that $|\phi(\pi_A)| = q^{\frac{1}{2}}$ and therefore $|\phi(\pi_A^2)| = |\phi(\pi_A)|^2 = q$ for all

embeddings $\phi : K \to \mathbb{C}$. It follows that $|\phi(u)| = 1$ for all embeddings $\phi : K \to \mathbb{C}$. Hence, the element u is a root of unity by Lemma 3.14. Let s be the order of u. Then $\pi_A^{2s} = q^s$. Consider $A/\mathbb{F}_{q^{2s}}$ which has Frobenius $\pi_A^{2s} = q^s \in \mathbb{Q}$. By Theorem 2.15, the abelian variety $A/\mathbb{F}_{q^{2s}}$ is $\mathbb{F}_{q^{2s}}$-isogenous to the third power of a supersingular elliptic curve. Hence, the abelian threefold $A/\mathbb{F}_q$ is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve.

Assume $A/\mathbb{F}_q$ is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve. Then there exists an integer $s > 0$ such that $A/\mathbb{F}_{q^s}$ is $\mathbb{F}_{q^s}$-isogenous to the third power of a supersingular elliptic curve. Thus, the Frobenius π_A^s of $A/\mathbb{F}_{q^s}$ is a rational number by Theorem 2.15. Since $\pi_A^{2s} = \pi_A^s \overline{\pi_A^s} = q^s$, it holds that $\pi_A^2 = uq$, where $u^s = 1$. It follows that $(\pi_A^2) = (q) = (\pi_A)(\overline{\pi_A})$ and hence $(\pi_A) = (\overline{\pi_A})$. □

Corollary 3.16. Let A be an abelian threefold over $\mathbb{F}_q$, with $q = p^n$. Let π_A be the Frobenius of A and $K = \mathbb{Q}(\pi_A)$. If A is absolutely simple, then there exists at least one prime ideal $\mathfrak{p}$ above p in K such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. In particular, if f_A is irreducible, then $p\mathcal{O}_K$ cannot factor as in Table 3.1.

m	$p\mathcal{O}_K$				
1	$\mathfrak{p}_1$	$\mathfrak{p}_1^2$	$\mathfrak{p}_1^3$	$\mathfrak{p}_1^6$	
2	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	$\mathfrak{p}_1\mathfrak{p}_2^4$	$\mathfrak{p}_1^2\mathfrak{p}_2^4$
3	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$	$\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$	$\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^3$	

Table 3.1: The prime factorizations of $p\mathcal{O}_K$ satisfying $\mathfrak{p}_i = \overline{\mathfrak{p}_i}$ for all primes $\mathfrak{p}_i$ above p in K. The number m in the left column denotes the number of prime ideals lying above p in K.

Proof. Suppose all prime ideals $\mathfrak{p}$ above p in K satisfy $\mathfrak{p} = \overline{\mathfrak{p}}$. If $\mathfrak{p}|p$, then $p \in \mathfrak{p}$ and hence $\pi_A\overline{\pi_A} = p^n \in \mathfrak{p}$. Therefore, we have $\pi_A \in \mathfrak{p}$ or $\overline{\pi_A} \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}|p$. Since $\mathfrak{p} = \overline{\mathfrak{p}}$ by assumption, it holds that $\pi_A, \overline{\pi_A} \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ in K dividing p. It follows that $(\pi_A) = (\overline{\pi_A})$. So A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve by Proposition 3.15, which contradicts with the assumption that A is absolutely simple. Hence, there exists at least one prime ideal $\mathfrak{p}$ in K dividing p such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. If f_A is irreducible, then $[K : \mathbb{Q}] = 6$ and Table 3.1 contains all prime factorizations of $p\mathcal{O}_K$ satisfying $\mathfrak{p} = \overline{\mathfrak{p}}$ for all primes $\mathfrak{p}$ above p in K. So if the factorization of $p\mathcal{O}_K$ occurs in Table 3.1, then $(\pi_A) = (\overline{\pi_A})$ and A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve. This contradicts with the fact that A is absolutely simple. □

3.3.1 The table

This section is based on the PhD thesis of Jeremy Bradford, [2, Example 3.10, Appendix A]. In his thesis, Bradford considers an absolutely simple abelian threefold $A/\mathbb{F}_p$ with commutative endomorphism ring. Let f_A be the characteristic polynomial of the Frobenius endomorphism and let π_A be a root of f_A. Bradford then defines the fields $K = \mathbb{Q}(\pi_A)$ and $K_+ = \mathbb{Q}(\pi_A + \overline{\pi_A})$. In [2, Appendix A], all possible cases for the splitting behaviour of p in the maximal order of the tower of fields $\mathbb{Q} \subset K_+ \subset K$ are worked out. In this section, we consider an absolutely simple abelian threefold defined over the finite field $\mathbb{F}_{p^n}$, for any positive integer n, such that $\mathrm{End}^0(A)$ is commutative. We assume that $\mathrm{End}(A) \cong \mathcal{O}_K$. We will follow a similar strategy as Bradford to work out all possible cases for the splitting behaviour of p in the maximal order of the tower of fields $\mathbb{Q} \subset K_+ \subset K$.

Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold such that $\mathrm{End}^0(A)$ is commutative. Let π_A be a root of f_A and let $K = \mathbb{Q}(\pi_A)$, which is a CM-field of degree 6. The field K is a second degree extension of the totally real subfield $K_+ = \mathbb{Q}(\pi_A + \overline{\pi_A})$. Thus, we have

$$[K : \mathbb{Q}] = [K : K_+][K_+ : \mathbb{Q}] = 2 \cdot 3 = 6.$$

The goal is to find all possible splitting behaviours of $p\mathcal{O}_K$ and the corresponding factorizations of the ideal (π_A) into prime ideals in K. From the prime factorization of (π_A) and the splitting behaviour of $p\mathcal{O}_K$, we can determine the p-rank $r(A)$ using Theorem 3.13.

We first look at the possible prime factorizations of $p\mathcal{O}_{K_+}$. Since $[K_+ : \mathbb{Q}] = 3$, we have $\sum_{\mathfrak{P}|p} e(\mathfrak{P})f(\mathfrak{P}) = 3$. This allows for the following possibilities of the prime factorization of $p\mathcal{O}_{K_+}$:

- $\mathfrak{P}_1$
- $\mathfrak{P}_1^3$
- $\mathfrak{P}_1\mathfrak{P}_2$
- $\mathfrak{P}_1\mathfrak{P}_2^2$
- $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$

Moreover, we have $[K : K_+] = 2$. Thus, for every prime ideal $\mathfrak{P}$ in K_+, it holds that $\sum_{\mathfrak{p}|\mathfrak{P}} e(\mathfrak{p}/\mathfrak{P})f(\mathfrak{p}/\mathfrak{P}) = 2$, where $e(\mathfrak{p}/\mathfrak{P})$ and $f(\mathfrak{p}/\mathfrak{P})$ denote the ramification index and residual degree of $\mathfrak{p}$ with respect to $\mathfrak{P}$. It follows that a prime $\mathfrak{P}$ in K_+ can have the following splitting types in K:

- $\mathfrak{p}$
- $\mathfrak{p}^2$
- $\mathfrak{p}\overline{\mathfrak{p}}$

By combining the possible splitting behaviours of $p\mathcal{O}_{K_+}$ and the possible splitting behaviours of $\mathfrak{P}\mathcal{O}_K$, where $\mathfrak{P}$ is a prime ideal in K, we can construct splitting diagrams. A *splitting diagram*, is a figure showing the splitting behaviour of p in the fields K_+ and K, like in the first column of Table 3.2. The middle row of a splitting diagram shows the prime factorization of p in the field K_+ and the top row shows the prime factorization of p in the field K. Two primes lying in different fields are connected by a line if the upper prime ideal lies above the lower prime ideal. Every prime ideal appearing in the diagram is connected via one or two lines with p, implying that every prime ideal in the diagram lies above p. If a prime divides a prime in the row below it and the corresponding residual degree is strictly greater than one, we put the residual degree in the splitting diagram next to the line connecting the two ideals.

Since A is absolutely simple, Corollary 3.16 states that at least one prime ideal $\mathfrak{p}$ above p in K satisfies $\mathfrak{p} \neq \overline{\mathfrak{p}}$. This implies that at least one prime ideal $\mathfrak{P}$ above p in K_+ splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$. In particular, the prime factorizations of $p\mathcal{O}_K$ in Table 3.1 cannot occur. Any splitting diagram that satisfies $\sum_{\mathfrak{p}|p} e(\mathfrak{p})f(\mathfrak{p}) = 6$, where $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification index and residual degree of $\mathfrak{p}$ with respect to p respectively, and has at least one prime ideal $\mathfrak{P}|p$ in K_+ that splits as $\mathfrak{p}\overline{\mathfrak{p}}$ in K, shows a possible splitting behaviour of p in the maximal order of K_+ and K and is listed in the first column of Table 3.2.

The prime factorization of the ideal (π_A) can be deduced from the prime factorization of $p\mathcal{O}_K$. It holds that

$$(\pi_A)(\overline{\pi_A}) = (\pi_A\overline{\pi_A}) = (p^n) = (p)^n,$$

and hence all prime ideals dividing (π_A), and also $(\overline{\pi_A})$, are lying above p. Furthermore, the norm of π_A in K is

$$\mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K_+/\mathbb{Q}}(\mathrm{N}_{K/K_+}(\pi_A)) = \mathrm{N}_{K_+/\mathbb{Q}}(\pi_A\overline{\pi_A}) = \mathrm{N}_{K_+/\mathbb{Q}}(p^n) = p^{3n}.$$

So if $(\pi_A) = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s}$, then

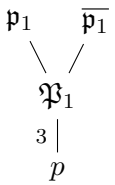
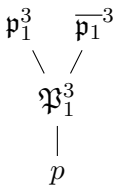
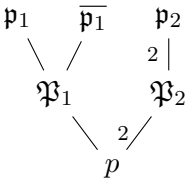
$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \cdots \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_s)^{c_s}.$$

Let $\mathfrak{p}$ be a prime ideal in K lying above p. Since $\pi_A\overline{\pi_A} = p^n$ and $p \in \mathfrak{p}$, it holds that $\pi_A\overline{\pi_A} \in \mathfrak{p}$. Thus, we have $\pi_A \in \mathfrak{p}$ or $\overline{\pi_A} \in \mathfrak{p}$, as $\mathfrak{p}$ is a prime ideal. In particular, if $\mathfrak{p} = \overline{\mathfrak{p}}$, then $\pi_A \in \mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\pi_A) > 0$. Furthermore, the abelian threefold A is absolutely simple, so Proposition 3.15 implies that $(\pi_A) \neq (\overline{\pi_A})$. Also, f_A is irreducible, so Corollary 2.26 implies that the invariants of A are integers. Hence, if $p\mathcal{O}_K = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$, then there exist integers $c_1, \ldots, c_s$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s}$ satisfies

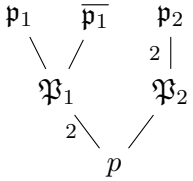
- $\mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \cdots \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_s)^{c_s} = p^{3n}$,
- $\mathrm{ord}_{\mathfrak{p}_i}(\pi_A) + \mathrm{ord}_{\overline{\mathfrak{p}_i}}(\pi_A) > 0$, in particular $\mathrm{ord}_{\mathfrak{p}_i}(\pi_A) > 0$ if $\mathfrak{p}_i = \overline{\mathfrak{p}_i}$,
- $\mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s} = (\pi_A) \neq (\overline{\pi_A}) = \overline{\mathfrak{p}_1}^{c_1} \cdots \overline{\mathfrak{p}_s}^{c_s}$,
- $i_{\mathfrak{p}_i} = f(\mathfrak{p}_i) \cdot \frac{\mathrm{ord}_{\mathfrak{p}_i}(\pi_A)}{n} = f(\mathfrak{p}_i) \cdot \frac{c_i}{n} \in \mathbb{Z}$ for all $i = 1, \ldots, s$.

The prime factorizations of (π_A) in K that satisfy the above conditions depend on the prime factorization of $p\mathcal{O}_K$ and appear in the second column of Table 3.2. The last column of the table contains the p-rank of A, which can be deduced from the splitting diagram and the prime factorization of (π_A) using Theorem 3.13.

Theorem 3.17. Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold such that $\mathrm{End}^0(A)$ is commutative and let π_A be a root of f_A. Then Table 3.2 gives the complete classification of p-rank in terms of the splitting behaviour of p in the maximal order of $\mathbb{Q}(\pi_A)$.

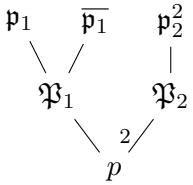
	Splitting of p	Factorization of (π_A)	$r(A)$
(I)		$\mathfrak{p}_1^n$	3
		$\mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}}$	0
(II)		$\mathfrak{p}_1^{3n}$	3
		$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^{2n}$	0
(III)		$\mathfrak{p}_1^n\mathfrak{p}_2^{\frac{n}{2}}$	1
		$\mathfrak{p}_1^{2n}\mathfrak{p}_2^{\frac{n}{4}}$	1

(IV)



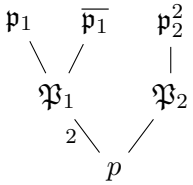
$\mathfrak{p}_1^n \mathfrak{p}_2^{\frac{n}{2}}$	2
$\mathfrak{p}_1^{\frac{n}{2}} \mathfrak{p}_2^n$	2

(V)



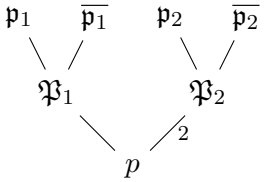
$\mathfrak{p}_1^n \mathfrak{p}_2^n$	1
$\mathfrak{p}_1^{2n} \mathfrak{p}_2^{\frac{n}{2}}$	1

(VI)



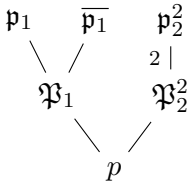
$\mathfrak{p}_1^n \mathfrak{p}_2^n$	2
$\mathfrak{p}_1^{\frac{n}{2}} \mathfrak{p}_2^{2n}$	2

(VII)



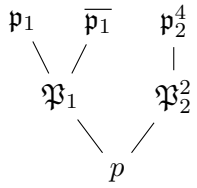
$\mathfrak{p}_1^n \mathfrak{p}_2^n$	3
$\mathfrak{p}_1^{2n} \mathfrak{p}_2^{\frac{n}{2}}$	3
$\mathfrak{p}_1^n \overline{\mathfrak{p}_1}^n \mathfrak{p}_2^{\frac{n}{2}}$	2
$\mathfrak{p}_1^n \mathfrak{p}_2^{\frac{n}{2}} \overline{\mathfrak{p}_2}^{\frac{n}{2}}$	1

(VIII)



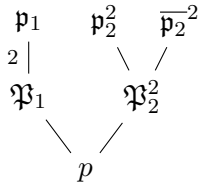
$\mathfrak{p}_1^n \mathfrak{p}_2^n$	1
$\mathfrak{p}_1^{2n} \mathfrak{p}_2^{\frac{n}{2}}$	1

(IX)



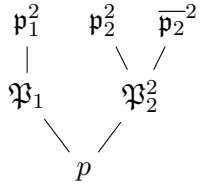
$\mathfrak{p}_1^n\mathfrak{p}_2^{2n}$	1
$\mathfrak{p}_1^{2n}\mathfrak{p}_2^n$	1

(X)



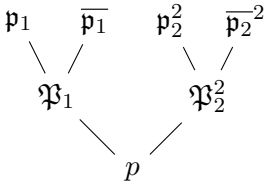
$\mathfrak{p}_1^n\mathfrak{p}_2^n$	2
$\mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^{2n}$	2

(XI)



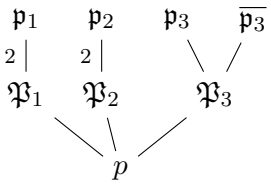
$\mathfrak{p}_1^n\mathfrak{p}_2^{2n}$	2
$\mathfrak{p}_1^{2n}\mathfrak{p}_2^n$	2

(XII)



$\mathfrak{p}_1^n\mathfrak{p}_2^{2n}$	3
$\mathfrak{p}_1^{2n}\mathfrak{p}_2^n$	3
$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^n$	2
$\mathfrak{p}_1^n\mathfrak{p}_2^n\overline{\mathfrak{p}_2}^n$	1

(XIII)



$\mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^{\frac{n}{2}}\mathfrak{p}_3^n$	1

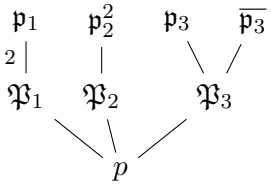
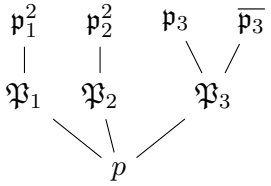
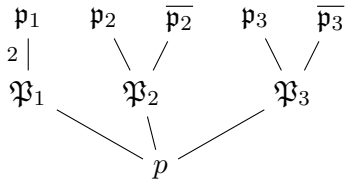
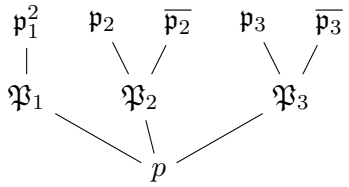
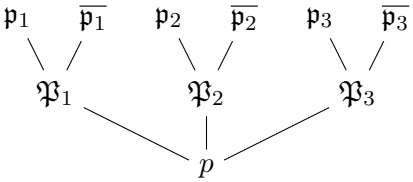
(XIV)		$\mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\mathfrak{p}_3^n$	1
(XV)		$\mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n$	1
(XVI)		$\mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\mathfrak{p}_3^n$	2
(XVII)		$\mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n$	2
(XVIII)		$\mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n$	3

Table 3.2: The splitting of p and the corresponding prime factorization of (π_A) and p-rank. In some prime factorizations of (π_A) appear prime ideals with exponents of the form $\frac{n}{2}$, $\frac{n}{3}$, $\frac{2n}{3}$ or $\frac{n}{4}$. These prime factorizations are only possible if n is even, if n is divisible by 3 or if n is divisible by 4 respectively. If n does not satisfy these conditions, then the corresponding prime factorization of (π_A) cannot occur.

Proof. We start the proof by explaining that the table contains all possible splitting behaviours of $p\mathcal{O}_K$ in the maximal order of K. Recall that Corollary 3.16 states that at least one prime ideal $\mathfrak{p}$ in K dividing p satisfies $\mathfrak{p} \neq \overline{\mathfrak{p}}$. This implies that at least one prime ideal $\mathfrak{P}$ in K_+ dividing p splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$. As explained in the beginning of this section, the possible prime factorizations of $p\mathcal{O}_{K_+}$ are

- $\mathfrak{P}_1$
- $\mathfrak{P}_1^3$
- $\mathfrak{P}_1\mathfrak{P}_2$
- $\mathfrak{P}_1\mathfrak{P}_2^2$
- $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$

and any prime $\mathfrak{P}$ in K_+ ramifies, splits or is inert in K. Starting from one of the prime factorizations of $p\mathcal{O}_{K_+}$ as listed above, all the possible splitting behaviours of $p\mathcal{O}_K$, under the restriction that at least one prime ideal $\mathfrak{P}$ in K_+ dividing p splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$, are listed in Table 3.3. Table 3.3 contains all possible prime factorizations of $p\mathcal{O}_K$ with the exception of the prime factorizations occuring in Table 3.1.

$p\mathcal{O}_{K_+}$	$p\mathcal{O}_K$		Case
$\mathfrak{P}_1$	$\mathfrak{p}_1\overline{\mathfrak{p}_1}$		(I)
$\mathfrak{P}_1^3$	$\mathfrak{p}_1^3\overline{\mathfrak{p}_1}^3$		(II)
$\mathfrak{P}_1\mathfrak{P}_2$	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$,	$f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1,\ f(\mathfrak{p}_2) = 4$	(III)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$,	$f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 2,\ f(\mathfrak{p}_2) = 2$	(IV)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$,	$f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1,\ f(\mathfrak{p}_2) = 2$	(V)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$,	$f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 2,\ f(\mathfrak{p}_2) = 1$	(VI)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$		(VII)
$\mathfrak{P}_1\mathfrak{P}_2^2$	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$		(VIII)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^4$		(IX)
	$\mathfrak{p}_1\mathfrak{p}_2^2\overline{\mathfrak{p}_2}^2$		(X)
	$\mathfrak{p}_1^2\mathfrak{p}_2^2\overline{\mathfrak{p}_2}^2$		(XI)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2\overline{\mathfrak{p}_2}^2$		(XII)
$\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XIII)
	$\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XIV)
	$\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XV)
	$\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XVI)
	$\mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XVII)
	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$		(XVIII)

Table 3.3: The possible prime factorizations of $p\mathcal{O}_{K_+}$ and $p\mathcal{O}_K$ and the corresponding case in Table 3.2.

Since every possible splitting behaviour of $p\mathcal{O}_K$ corresponds to a case in Table 3.2, it follows that Table 3.2 is complete.

The next step is to prove that for each splitting type of p in Table 3.2, the possible factorizations of (π_A) and the corresponding p-rank are correct. Recall that if $p\mathcal{O}_K = \mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$, then the possible factorizations of (π_A) are those for which there exist $c_1,\ldots,c_s \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\cdots\mathfrak{p}_s^{c_s}$ satisfies

- $\mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\cdots\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_s)^{c_s} = p^{3n}$,
- $\mathrm{ord}_{\mathfrak{p}_i}(\pi_A) + \mathrm{ord}_{\overline{\mathfrak{p}_i}}(\pi_A) > 0$, in particular $\mathrm{ord}_{\mathfrak{p}_i}(\pi_A) > 0$ if $\mathfrak{p}_i = \overline{\mathfrak{p}_i}$,
- $\mathfrak{p}_1^{c_1}\cdots\mathfrak{p}_s^{c_s} = (\pi_A) \neq (\overline{\pi_A}) = \overline{\mathfrak{p}_1}^{c_1}\cdots\overline{\mathfrak{p}_s}^{c_s}$,
- $i_{\mathfrak{p}_i} = f(\mathfrak{p}_i)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_i}(\pi_A)}{n} = f(\mathfrak{p}_i)\cdot\frac{c_i}{n} \in \mathbb{Z}$ for all $i = 1,\ldots,s$.

Case (I). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 3$. There exist $c_1, c_2 \in \mathbb{Z}$ such

that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2} = p^{3c_1}p^{3c_2} = p^{3c_1+3c_2},$$

so $3n = 3c_1 + 3c_2$. The invariants are

$$i_{\mathfrak{p}_1} = f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{3c_1}{n},$$
$$i_{\overline{\mathfrak{p}_1}} = f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{3c_2}{n}.$$

Thus, it holds that $c_1, c_2 \in \{0, \frac{n}{3}, \frac{2n}{3}, n\}$. Moreover, we have $c_1 \neq c_2$, otherwise we get $(\pi_A) = (\overline{\pi_A})$. Hence, the possibilities for the factorization of (π_A) are

$$(\pi_A) = \mathfrak{p}_1^n,$$
$$(\pi_A) = \overline{\mathfrak{p}_1}^n,$$
$$(\pi_A) = \mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}},$$
$$(\pi_A) = \mathfrak{p}_1^{\frac{2n}{3}}\overline{\mathfrak{p}_1}^{\frac{n}{3}}.$$

Note that $\overline{\mathfrak{p}_1}^n = \overline{\mathfrak{p}_1^n}$ and $\mathfrak{p}_1^{\frac{2n}{3}}\overline{\mathfrak{p}_1}^{\frac{n}{3}} = \overline{\mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}}}$. Without loss of generality, we can set $\pi_A = \overline{\pi_A}$. Therefore, Table 3.2 only lists $\mathfrak{p}_1^n$ and $\mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}}$. The latter is only possible if $3|n$. Applying Theorem 3.13 gives $r(A) = 3$ if $(\pi_A) = \mathfrak{p}_1^n$ and $r(A) = 0$ if $(\pi_A) = \mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}}$.

Case (II). We have $p\mathcal{O}_K = \mathfrak{p}_1^3\overline{\mathfrak{p}_1}^3$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$. There exist $c_1, c_2 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1}) = p^{c_1}p^{c_2} = p^{c_1+c_2},$$

so $3n = c_1 + c_2$. The invariants are

$$i_{\mathfrak{p}_1} = f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n},$$
$$i_{\overline{\mathfrak{p}_1}} = f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}.$$

Thus, it holds that $c_1, c_2 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise we get $(\pi_A) = (\overline{\pi_A})$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$(\pi_A) = \mathfrak{p}_1^{3n},$$
$$(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^{2n}.$$

Applying Theorem 3.13 gives $r(A) = 3$ if $(\pi_A) = \mathfrak{p}_1^{3n}$ and $r(A) = 0$ if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^{2n}$.

Case (III). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 4$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{c_1}p^{c_2}p^{4c_3} = p^{c_1+c_2+4c_3},$$

so $3n = c_1 + c_2 + 4c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n},\\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n},\\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{4c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, n, 2n, 3n\}$ and $c_3 \in \{0, \frac{n}{4}, \frac{n}{2}, \frac{3n}{4}\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^{\frac{n}{2}},\\ (\pi_A) &= \mathfrak{p}_1^{2n}\mathfrak{p}_2^{\frac{n}{4}}. \end{aligned}$$

The first is only possible if n is even and the second only if $4|n$. Applying Theorem 3.13 gives $r(A) = 1$ in both cases.

Case (IV). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = f(\mathfrak{p}_2) = 2$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{2c_1}p^{2c_2}p^{2c_3} = p^{2c_1+2c_2+2c_3},$$

so $3n = 2c_1 + 2c_2 + 2c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n},\\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{2c_2}{n},\\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{2c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2, c_3 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^{\frac{n}{2}},\\ (\pi_A) &= \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n. \end{aligned}$$

Both are only possible if n is even. Applying Theorem 3.13 gives $r(A) = 2$ in both cases.

Case (V). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 2$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{c_1}p^{c_2}p^{2c_3} = p^{c_1+c_2+2c_3},$$

so $3n = c_1 + c_2 + 2c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n},\\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n},\\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{2c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, n, 2n, 3n\}$ and $c_3 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^n,\\ (\pi_A) &= \mathfrak{p}_1^{2n}\mathfrak{p}_2^{\frac{n}{2}}. \end{aligned}$$

The second is only possible if n is even. Applying Theorem 3.13 gives $r(A) = 1$ in both cases.

Case (VI). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 2$ and $f(\mathfrak{p}_2) = 1$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{2c_1}p^{2c_2}p^{c_3} = p^{2c_1+2c_2+c_3},$$

so $3n = 2c_1 + 2c_2 + c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n},\\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{2c_2}{n},\\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$ and $c_3 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^n,\\ (\pi_A) &= \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^{2n}. \end{aligned}$$

The second is only possible if n is even. Applying Theorem 3.13 gives $r(A) = 2$ in both cases.

Case (VII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 2$. There exist $c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}\overline{\mathfrak{p}_2}^{c_4}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_4} \\ &= p^{c_1}p^{c_2}p^{2c_3}p^{2c_4} = p^{c_1+c_2+2c_3+2c_4}, \end{aligned}$$

so $3n = c_1 + c_2 + 2c_3 + 2c_4$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{2c_3}{n}, \\ i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{2c_4}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, n, 2n, 3n\}$ and $c_3, c_4 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$. Furthermore, we have $c_1 \neq c_2$ or $c_3 \neq c_4$, otherwise $(\pi_A) = (\overline{\pi_A})$. Moreover, at least one of c_1 and c_2 and at least one of c_3 and c_4 is nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$ and in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^n, \\ (\pi_A) &= \mathfrak{p}_1^{2n}\mathfrak{p}_2^{\frac{n}{2}}, \\ (\pi_A) &= \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}, \\ (\pi_A) &= \mathfrak{p}_1^n\mathfrak{p}_2^{\frac{n}{2}}\overline{\mathfrak{p}_2}^{\frac{n}{2}}. \end{aligned}$$

The second, third and last case are only possible if n is even. Applying Theorem 3.13 gives $r(A) = 3$ if $(\pi_A) = \mathfrak{p}_1^n\mathfrak{p}_2^n$ or $(\pi_A) = \mathfrak{p}_1^{2n}\mathfrak{p}_2^{\frac{n}{2}}$, p-rank $r(A) = 2$ if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}$ and $r(A) = 1$ if $(\pi_A) = \mathfrak{p}_1^n\mathfrak{p}_2^{\frac{n}{2}}\overline{\mathfrak{p}_2}^{\frac{n}{2}}$.

Case (VIII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 2$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{c_1}p^{c_2}p^{2c_3} = p^{c_1+c_2+2c_3},$$

so $3n = c_1 + c_2 + 2c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{2c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, n, 2n, 3n\}$ and $c_3 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^n, \\ (\pi_A) &= \mathfrak{p}_1^{2n} \mathfrak{p}_2^{\frac{n}{2}}. \end{aligned}$$

The second is only possible if n is even. Applying Theorem 3.13 gives $r(A) = 1$ in both cases.

Case (IX). We have $p\mathcal{O}_K = \mathfrak{p}_1 \overline{\mathfrak{p}_1} \mathfrak{p}_2^4$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = f(\mathfrak{p}_2) = 1$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \overline{\mathfrak{p}_1}^{c_2} \mathfrak{p}_2^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} = p^{c_1} p^{c_2} p^{c_3} = p^{c_1+c_2+c_3},$$

so $3n = c_1 + c_2 + c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2, c_3 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_1 \neq c_2$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_3 \neq 0$, because $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^{2n}, \\ (\pi_A) &= \mathfrak{p}_1^{2n} \mathfrak{p}_2^n. \end{aligned}$$

Applying Theorem 3.13 gives $r(A) = 1$ in both cases.

Case (X). We have $p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2^2 \overline{\mathfrak{p}_2}^2$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \overline{\mathfrak{p}_2}^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_3} = p^{2c_1} p^{c_2} p^{c_3} = p^{2c_1+c_2+c_3},$$

so $3n = 2c_1 + c_2 + c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n} \\ i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$ and $c_2, c_3 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_2 \neq c_3$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^n, \\ (\pi_A) &= \mathfrak{p}_1^{\frac{n}{2}} \mathfrak{p}_2^{2n}. \end{aligned}$$

The second is only possible if n is even. Applying Theorem 3.13 gives $r(A) = 2$ in both cases.

Case (XI). We have $p\mathcal{O}_K = \mathfrak{p}_1^2 \mathfrak{p}_2^2 \overline{\mathfrak{p}_2}^2$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. There exist $c_1, c_2, c_3 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \overline{\mathfrak{p}_2}^{c_3}$. Then

$$p^{3n} = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_3} = p^{c_1} p^{c_2} p^{c_3} = p^{c_1+c_2+c_3},$$

so $3n = c_1 + c_2 + c_3$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n} \\ i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_3}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2, c_3 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_2 \neq c_3$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^{2n}, \\ (\pi_A) &= \mathfrak{p}_1^{2n} \mathfrak{p}_2^n. \end{aligned}$$

Applying Theorem 3.13 gives $r(A) = 2$ in both cases.

Case (XII). We have $p\mathcal{O}_K = \mathfrak{p}_1 \overline{\mathfrak{p}_1} \mathfrak{p}_2^2 \overline{\mathfrak{p}_2}^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. There exist $c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \overline{\mathfrak{p}_1}^{c_2} \mathfrak{p}_2^{c_3} \overline{\mathfrak{p}_2}^{c_4}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_4} \\ &= p^{c_1} p^{c_2} p^{c_3} p^{c_4} = p^{c_1+c_2+c_3+c_4}, \end{aligned}$$

so $3n = c_1 + c_2 + c_3 + c_4$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_3}{n}, \\ i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_4}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2, c_3, c_4 \in \{0, n, 2n, 3n\}$. Furthermore, we have $c_1 \neq c_2$ or $c_3 \neq c_4$, otherwise $(\pi_A) = (\overline{\pi_A})$. Moreover, at least one of c_1 and c_2 and at least one of c_3 and c_4 is nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$ and in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$. Hence, up to conjugation, the possibilities for the factorization of (π_A) are

$$\begin{aligned} (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^{2n}, \\ (\pi_A) &= \mathfrak{p}_1^{2n} \mathfrak{p}_2^n, \\ (\pi_A) &= \mathfrak{p}_1^n \overline{\mathfrak{p}_1}^n \mathfrak{p}_2^n, \\ (\pi_A) &= \mathfrak{p}_1^n \mathfrak{p}_2^n \overline{\mathfrak{p}_2}^n. \end{aligned}$$

Applying Theorem 3.13 gives $r(A) = 3$ if $(\pi_A) = \mathfrak{p}_1^n \mathfrak{p}_2^{2n}$ or $(\pi_A) = \mathfrak{p}_1^{2n} \mathfrak{p}_2^n$, p-rank $r(A) = 2$ if $(\pi_A) = \mathfrak{p}_1^n \overline{\mathfrak{p}_1}^n \mathfrak{p}_2^n$ and $r(A) = 1$ if $(\pi_A) = \mathfrak{p}_1^n \mathfrak{p}_2^n \overline{\mathfrak{p}_2}^n$.

Case (XIII). We have $p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = 2$ and $f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. There exist $c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \mathfrak{p}_3^{c_3} \overline{\mathfrak{p}_3}^{c_4}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_3} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_4} \\ &= p^{2c_1} p^{2c_2} p^{c_3} p^{c_4} = p^{2c_1 + 2c_2 + c_3 + c_4}, \end{aligned}$$

so $3n = 2c_1 + 2c_2 + c_3 + c_4$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{2c_2}{n}, \\ i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_3}{n}, \\ i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_4}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$ and $c_3, c_4 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_3 \neq c_4$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1, c_2 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$

and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^{\frac{n}{2}}\mathfrak{p}_3^n$, which happens only if n is even. Applying Theorem 3.13 gives $r(A) = 1$.

Case (XIV). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}_2) = f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. There exist $c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\mathfrak{p}_3^{c_3}\overline{\mathfrak{p}_3}^{c_4}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_3}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_4} \\ &= p^{2c_1}p^{c_2}p^{c_3}p^{c_4} = p^{2c_1+c_2+c_3+c_4}, \end{aligned}$$

so $3n = 2c_1 + c_2 + c_3 + c_4$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_3}{n}, \\ i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_4}{n}. \end{aligned}$$

Thus, it holds that $c_1 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$ and $c_2, c_3, c_4 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_3 \neq c_4$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1, c_2 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\mathfrak{p}_3^n$, which happens only if n is even. Applying Theorem 3.13 gives $r(A) = 1$.

Case (XV). We have $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. There exist $c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\mathfrak{p}_3^{c_3}\overline{\mathfrak{p}_3}^{c_4}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_3}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_4} \\ &= p^{c_1}p^{c_2}p^{c_3}p^{c_4} = p^{c_1+c_2+c_3+c_4}, \end{aligned}$$

so $3n = c_1 + c_2 + c_3 + c_4$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3)\cdot\frac{\mathrm{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_3}{n}, \\ i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3})\cdot\frac{\mathrm{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_4}{n}. \end{aligned}$$

Thus, it holds that $c_1, c_2, c_3, c_4 \in \{0, n, 2n, 3n\}$. Moreover, we have $c_3 \neq c_4$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1, c_2 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^n \mathfrak{p}_2^n \mathfrak{p}_3^n$. Applying Theorem 3.13 gives $r(A) = 1$.

Case (XVI). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}) = 1$ for prime $\mathfrak{p} \in \{\mathfrak{p}_2, \overline{\mathfrak{p}_2}, \mathfrak{p}_3, \overline{\mathfrak{p}_3}\}$. There exist $c_1, c_2, c_3, c_4, c_5 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}\mathfrak{p}_3^{c_4}\overline{\mathfrak{p}_3}^{c_5}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_3}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_4}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_5} \\ &= p^{2c_1}p^{c_2}p^{c_3}p^{c_4}p^{c_5} = p^{2c_1+c_2+c_3+c_4+c_5}, \end{aligned}$$

so $3n = 2c_1 + c_2 + c_3 + c_4 + c_5$. The invariants are

$$\begin{aligned} i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{2c_1}{n}, \\ i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\mathrm{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n}, \\ i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\mathrm{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_3}{n} \\ i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3) \cdot \frac{\mathrm{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_4}{n}, \\ i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3}) \cdot \frac{\mathrm{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_5}{n}. \end{aligned}$$

Thus, it holds that $c_1 \in \{0, \frac{n}{2}, n, \frac{3n}{2}, 2n, \frac{5n}{2}, 3n\}$ and $c_2, c_3, c_4, c_5 \in \{0, n, 2n, 3n\}$. Furthermore, we have $c_2 \neq c_3$ or $c_4 \neq c_5$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$. Moreover, at least one of c_2 and c_3 and at least one of c_4 and c_5 is nonzero, because π_A is contained in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\mathfrak{p}_3^n$, which happens only if n is even. Applying Theorem 3.13 gives $r(A) = 2$.

Case (XVII). We have $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}) = 1$ for all primes $\mathfrak{p}$ lying above p. There exist $c_1, c_2, c_3, c_4, c_5 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}\mathfrak{p}_3^{c_4}\overline{\mathfrak{p}_3}^{c_5}$. Then

$$\begin{aligned} p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_2}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_3}\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_4}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_5} \\ &= p^{c_1}p^{c_2}p^{c_3}p^{c_4}p^{c_5} = p^{c_1+c_2+c_3+c_4+c_5}, \end{aligned}$$

so $3n = c_1 + c_2 + c_3 + c_4 + c_5$. The invariants are

$$\begin{aligned}
i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\
i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_2}{n}, \\
i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_3}{n} \\
i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_4}{n}, \\
i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_5}{n}.
\end{aligned}$$

Thus, it holds that $c_1, c_2, c_3, c_4, c_5 \in \{0, n, 2n, 3n\}$. Furthermore, we have $c_2 \neq c_3$ or $c_4 \neq c_5$, otherwise $(\pi_A) = (\overline{\pi_A})$, and $c_1 \neq 0$, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$. Moreover, at least one of c_2 and c_3 and at least one of c_4 and c_5 is nonzero, because π_A is contained in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^n \mathfrak{p}_2^n \mathfrak{p}_3^n$. Applying Theorem 3.13 gives $r(A) = 2$.

Case (XVIII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}) = 1$ for all primes $\mathfrak{p}$ lying above p. There exist $c_1, c_2, c_3, c_4, c_5, c_6 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}\overline{\mathfrak{p}_2}^{c_4}\mathfrak{p}_3^{c_5}\overline{\mathfrak{p}_3}^{c_6}$. Then

$$\begin{aligned}
p^{3n} &= \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1)^{c_1} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_1})^{c_2} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2)^{c_3} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_2})^{c_4} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3)^{c_5} \mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}_3})^{c_6} \\
&= p^{c_1} p^{c_2} p^{c_3} p^{c_4} p^{c_5} p^{c_6} = p^{c_1+c_2+c_3+c_4+c_5+c_6},
\end{aligned}$$

so $3n = c_1 + c_2 + c_3 + c_4 + c_5 + c_6$. The invariants are

$$\begin{aligned}
i_{\mathfrak{p}_1} &= f(\mathfrak{p}_1) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_1}(\pi_A)}{n} = \frac{c_1}{n}, \\
i_{\overline{\mathfrak{p}_1}} &= f(\overline{\mathfrak{p}_1}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_1}}(\pi_A)}{n} = \frac{c_2}{n}, \\
i_{\mathfrak{p}_2} &= f(\mathfrak{p}_2) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_2}(\pi_A)}{n} = \frac{c_3}{n}, \\
i_{\overline{\mathfrak{p}_2}} &= f(\overline{\mathfrak{p}_2}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_2}}(\pi_A)}{n} = \frac{c_4}{n} \\
i_{\mathfrak{p}_3} &= f(\mathfrak{p}_3) \cdot \frac{\operatorname{ord}_{\mathfrak{p}_3}(\pi_A)}{n} = \frac{c_5}{n}, \\
i_{\overline{\mathfrak{p}_3}} &= f(\overline{\mathfrak{p}_3}) \cdot \frac{\operatorname{ord}_{\overline{\mathfrak{p}_3}}(\pi_A)}{n} = \frac{c_6}{n}.
\end{aligned}$$

Thus, it holds that $c_1, c_2, c_3, c_4, c_5, c_6 \in \{0, n, 2n, 3n\}$. Furthermore, we have $c_1 \neq c_2$ or $c_3 \neq c_4$ or $c_5 \neq c_6$, otherwise $(\pi_A) = (\overline{\pi_A})$. Moreover, at least one of c_1 and c_2, at

least one of c_3 and c_4 and at least one of c_5 and c_6 is nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$, in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. Hence, up to conjugation, the only possibility for the factorization of (π_A) is $(\pi_A) = \mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n$. Applying Theorem 3.13 gives $r(A) = 3$. □

Remark 3.18. Bradford's table in [2, Appendix A] is constructed in the same way as Table 3.2, except that Bradford starts with an absolutely simple abelian threefold A defined over the finite field $\mathbb{F}_p$. Consequently, every factorization of (π_A) in Table 3.2 that has $\frac{n}{2}$ or $\frac{n}{4}$ occurring as the exponent of one of the prime ideals dividing (π_A), does not appear in Bradford's table. Specifically cases (III), (IV), (XIII), (XIV) and (XVI) are absent from Bradford's table. We would expect that if we set $n = 1$ and remove all factorizations of (π_A) with $\frac{n}{2}$, $\frac{n}{3}$, $\frac{2n}{3}$ or $\frac{n}{4}$ as the exponent of one of the prime ideals dividing (π_A), we obtain Bradford's table. However, there are differences. In cases (IX) and (XI), Bradford only mentions one of the two factorizations of (π_A). The same happens in case (XII). Here Bradford only mentions the factorizations $(\pi_A) = \mathfrak{p}_1\mathfrak{p}_2^2$ and $(\pi_A) = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}$, while the factorizations $(\pi_A) = \mathfrak{p}_1^2\mathfrak{p}_2$ and $(\pi_A) = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ are also possible. The factorization $(\pi_A) = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ even corresponds to a different p-rank than the two factorizations mentioned by Bradford. Finally, case (X) is absent from Bradford's table, while we do have the factorization $(\pi_A) = \mathfrak{p}_1\mathfrak{p}_2$ corresponding to $r(A) = 2$.

Remark 3.19. The relation between the factorization of p in a CM field K and the p-rank of the reduction of an absolutely simple abelian threefold with CM by $\mathcal{O}_K$ and commutative endomorphism ring, see Chapter 4, is studied by Zaytsev [24]. The absolutely simple abelian threefolds considered by Zaytsev form a subset of the absolutely simple abelian threefolds considered in Theorem 3.17. There are a few differences between the table in Zaytsev [24, Theorem 1.2] and Table 3.2. First of all, Zaytsev does not restrict to absolutely simple abelian threefolds. In his table he includes abelian threefolds isogenous to the third power of an elliptic curve. This explains why Zaytsev considers factorizations of $p\mathcal{O}_K$ appearing in Table 3.1 and finds p-rank 0 in case (IV). Furthermore, if $p\mathcal{O}_K$ splits as in case (XIII) of Table 3.17, then we find that the p-rank is 1. Zaytsev also finds p-rank 3 corresponding to an abelian threefold isogenous to the third power of an ordinary elliptic curve. This abelian threefold is not absolutely simple and hence does not occur in Table 3.2. In case (VII), we find p-ranks 1, 2 and 3, while Zaytsev only finds p-ranks 1 and 3. This could be due to the fact that the absolutely simple abelian threefolds considered by Zaytsev form a subset of the abelian threefolds considered in Theorem 3.17, see also Remark 3.20.

Remark 3.20. The way we constructed Table 3.2 implies that it is complete, so every possible factorization of (p) and (π) in the maximal order of $\mathbb{Q}(\pi_A)$ for an absolutely simple abelian threefold $A/\mathbb{F}_q$ with $\mathrm{End}^0(A) \cong \mathbb{Q}(\pi_A)$ is contained in Table 3.2. However, it might be that not all factorizations of $\pi\mathcal{O}_K$ actually occur. This could also explain while we find p-ranks 1, 2 and 3 in case (VII), while Zaytsev only finds p-ranks 1 and 3.

The following corollaries and remark contain results that are deduced from Table 3.2.

Corollary 3.21. Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold with f_A irreducible. Then the p-rank of A is zero if and only if one of the following occurs

(i) $(\pi_A) = \mathfrak{p}_1^{\frac{n}{3}}\overline{\mathfrak{p}_1}^{\frac{2n}{3}}$ (provided that $3|n$),

(ii) $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^{2n}$.

Corollary 3.22. Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold with f_A irreducible. Then $r(A) = 3$ if and only if (π_A) and $(\overline{\pi_A})$ are relatively prime.

Remark 3.23. In dimension $g = 1$, knowing the endomorphism algebra $\mathrm{End}^0(E)$ of an elliptic curve $E/\mathbb{F}_q$ is enough to determine the p-rank $r(E)$. In dimension $g = 2$, the factorization of (p) in the maximal order of $\mathbb{Q}(\pi_S)$, which only depends on the endomorphism algebra $\mathrm{End}^0(S)$, completely determines the p-rank $r(S)$ of an absolutely simple abelian surface $S/\mathbb{F}_q$. In dimension $g = 3$ however, knowing the endomorphism algebra $\mathrm{End}^0(A)$ and the splitting type of (p) in the maximal order of $\mathbb{Q}(\pi_A)$ is no longer sufficient to determine the p-rank $r(A)$ of an absolutely simple abelian threefold $A/\mathbb{F}_q$ with $\mathrm{End}^0(A) \cong \mathbb{Q}(\pi_A)$.

The following theorem describes when a simple abelian threefold $A/\mathbb{F}_q$ is supersingular in terms of the prime factorization of p in the field $\mathbb{Q}(\pi_A)$, where π_A is the Frobenius endomorphism of A.

Theorem 3.24. Let $A/\mathbb{F}_q$, with $q = p^n$, be a simple abelian threefold. Let π_A be a root of f_A and let $K = \mathbb{Q}(\pi_A)$.

(i) If f_A is not irreducible, then A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve if and only if p is inert or ramified in K.

(ii) If f_A is irreducible, then A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve if and only if $p\mathcal{O}_K$ factors as in Table 3.1 or (π_A) factors as in the following table.

$p\mathcal{O}_K$ splits as in	Factorization of (π_A)
(III)	$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{4}}$
(IV)	$\mathfrak{p}_1^{\frac{n}{2}}\overline{\mathfrak{p}_1}^{\frac{n}{2}}\mathfrak{p}_2^{\frac{n}{2}}$
(V)	$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}$
(VI)	$\mathfrak{p}_1^{\frac{n}{2}}\overline{\mathfrak{p}_1}^{\frac{n}{2}}\mathfrak{p}_2^n$
(VIII)	$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}$
(IX)	$\mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^n$
(X)	$\mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\overline{\mathfrak{p}_2}^n$
(XI)	$\mathfrak{p}_1^n\mathfrak{p}_2^n\overline{\mathfrak{p}_2}^n$

Table 3.4: The factorizations of (π_A) satisfying $(\pi_A) = (\overline{\pi_A})$. The numbers in the left column refer to the cases of Table 3.2.

Proof. Proposition 3.15 states that A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve if and only if $(\pi_A) = (\overline{\pi_A})$ in K. By Proposition 3.1, the polynomial f_A is irreducible or $f_A = h^3$, where h is a second degree irreducible Weil polynomial. If $f_A = h^3$, then $[K : \mathbb{Q}] = 2$ and p splits, ramifies or is inert in K. If p ramifies or is inert in K, then every prime ideal above p in K is its own conjugate and $(\pi_A) = (\overline{\pi_A})$. Suppose p splits, so $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. There exist $c_1, c_2 \in \mathbb{Z}$ such that $(\pi_A) = \mathfrak{p}^{c_1}\overline{\mathfrak{p}_1}^{c_2}$. Then

$$p^n = \mathrm{N}_{K/\mathbb{Q}}(\pi_A) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{c_1}\,\mathrm{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}})^{c_2} = p^{c_1}p^{c_2} = p^{c_1+c_2},$$

so $n = c_1 + c_2$. By Theorem 2.24, we have $e = [\mathrm{End}^0_{\mathbb{F}_q}(A) : \mathbb{Q}(\pi_A)]^{\frac{1}{2}} = 3$. Thus, the least common denominator of the invariants $i_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\pi_A)$, is equal to 3 by Theorem 2.25. We have

$$i_{\mathfrak{p}} = f(\mathfrak{p}) \cdot \frac{\mathrm{ord}_{\mathfrak{p}}(\pi_A)}{n} = \frac{c_1}{n} \qquad \text{and} \qquad i_{\overline{\mathfrak{p}}} = f(\overline{\mathfrak{p}}) \cdot \frac{\mathrm{ord}_{\overline{\mathfrak{p}}}(\pi_A)}{n} = \frac{c_2}{n}.$$

Since the least common denominator of all invariants is 3, it holds that $i_{\mathfrak{p}}$ and $i_{\overline{\mathfrak{p}}}$ are multiples of $\frac{1}{3}$. Therefore, $c_1, c_2 \in \{0, \frac{n}{3}, \frac{2n}{3}, n\}$. There are no integers $c_1, c_2 \in \{0, \frac{n}{3}, \frac{2n}{3}, n\}$ satisfying $c_1 = c_2$ and $c_1 + c_2 = n$. Hence, if p splits in K, then $(\pi_A) = (\overline{\pi_A})$ is not possible. This proves the first statement.

Next, assume f_A is irreducible. If every prime ideal above p in K is its own conjugate, then $(\pi_A) = (\overline{\pi_A})$ and A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve. This happens precisely when $p\mathcal{O}_K$ factors as in Table 3.1. Moreover, if (π_A)

splits as in Table 3.4, then $(\pi_A) = (\overline{\pi_A})$ and A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve.

Table 3.2 contains all possible splitting behaviours of $p\mathcal{O}_K$ in the maximal order of K such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$ for at least one prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lying above p. We follow the same strategy as in the proof of Theorem 3.17, but now we look for factorizations of (π_A) satisfying $(\pi_A) = (\overline{\pi_A})$.

Case (I). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 3$. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}$, where $3c_1 + 3c_2 = 3n$ and $\frac{3c_1}{n}, \frac{3c_2}{n} \in \mathbb{Z}$. It follows that $c_1 \neq c_2$, so $(\pi_A) = (\overline{\pi_A})$ is not possible.

Case (II). We have $p\mathcal{O}_K = \mathfrak{p}_1^3\overline{\mathfrak{p}_1}^3$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}$, where $c_1 + c_2 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n} \in \mathbb{Z}$. It follows that $c_1 \neq c_2$, so $(\pi_A) = (\overline{\pi_A})$ is not possible.

Case (III). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 4$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $c_1 + c_2 + 4c_3 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{4c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{4}}$, which happens only if $4|n$.

Case (IV). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_2}) = f(\mathfrak{p}_2) = 2$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $2c_1 + 2c_2 + 2c_3 = 3n$ and $\frac{2c_1}{n}, \frac{2c_2}{n}, \frac{2c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\overline{\mathfrak{p}_1}^{\frac{n}{2}}\mathfrak{p}_2^{\frac{n}{2}}$, which happens only if n is even.

Case (V). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 2$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $c_1 + c_2 + 2c_3 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{2c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}$, which happens only if n is even.

Case (VI). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 2$ and $f(\mathfrak{p}_2) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $2c_1 + 2c_2 + c_3 = 3n$ and $\frac{2c_1}{n}, \frac{2c_2}{n}, \frac{c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\overline{\mathfrak{p}_1}^{\frac{n}{2}}\mathfrak{p}_2^n$, which happens only if n is even.

Case (VII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 2$. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}\overline{\mathfrak{p}_2}^{c_4}$, where $c_1 + c_2 + 2c_3 + 2c_4 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{2c_3}{n}, \frac{2c_4}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_1 = c_2$ and $c_3 = c_4$. Moreover, the integers c_1, c_2, c_3 and c_4 are all nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$ and in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and $c_1 = c_2$ and $c_3 = c_4$. But that implies $c_1 + c_2 + 2c_3 + 2c_4 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (VIII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = 1$ and $f(\mathfrak{p}_2) = 2$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $c_1 + c_2 + 2c_3 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{2c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^{\frac{n}{2}}$, which happens only if n is even.

Case (IX). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^4$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = f(\mathfrak{p}_2) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}$, where $c_1 + c_2 + c_3 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n} \in \mathbb{Z}$. Moreover, at least one of c_1 and c_2 is nonzero, and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^n\overline{\mathfrak{p}_1}^n\mathfrak{p}_2^n$.

Case (X). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\overline{\mathfrak{p}_2}^2$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}$, where $2c_1 + c_2 + c_3 = 3n$ and $\frac{2c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n} \in \mathbb{Z}$. Moreover, the integer c_1 is nonzero, and at least one of c_2 and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^{\frac{n}{2}}\mathfrak{p}_2^n\overline{\mathfrak{p}_2}^n$, which happens only if n is even.

Case (XI). We have $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\overline{\mathfrak{p}_2}^2$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}$, where $c_1+c_2+c_3 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n} \in \mathbb{Z}$. Moreover, the integer c_1 is nonzero, and at least one of c_2 and c_3 is nonzero. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $(\pi_A) = \mathfrak{p}_1^n\mathfrak{p}_2^n\overline{\mathfrak{p}_2}^n$.

Case (XII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$ with $f(\mathfrak{p}_1) = f(\overline{\mathfrak{p}_1}) = f(\mathfrak{p}_2) = f(\overline{\mathfrak{p}_2}) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}\overline{\mathfrak{p}_2}^{c_4}$, where $c_1+c_2+c_3+c_4 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_1 = c_2$ and $c_3 = c_4$. Moreover, the integers c_1, c_2, c_3 and c_4 are all nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$ and in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$, and $c_1 = c_2$ and $c_3 = c_4$. But that implies $c_1 + c_2 + c_3 + c_4 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XIII). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = 2$ and $f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\mathfrak{p}_3^{c_3}\overline{\mathfrak{p}_3}^{c_4}$, where $2c_1 + 2c_2 + c_3 + c_4 = 3n$ and $\frac{2c_1}{n}, \frac{2c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_3 = c_4$. Moreover, the integers c_1, c_2, c_3 and c_4 are all nonzero, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$, and π_A is contained in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $2c_1 + 2c_2 + c_3 + c_4 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XIV). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}_2) = f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\mathfrak{p}_3^{c_3}\overline{\mathfrak{p}_3}^{c_4}$, where $2c_1+c_2+c_3+c_4 = 3n$ and $\frac{2c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_3 = c_4$. Moreover, the integers c_1, c_2, c_3 and c_4 are all nonzero, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$, and π_A is contained in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $2c_1 + c_2 + c_3 + c_4 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XV). We have $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = f(\mathfrak{p}_3) = f(\overline{\mathfrak{p}_3}) = 1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\mathfrak{p}_3^{c_3}\overline{\mathfrak{p}_3}^{c_4}$, where $c_1 + c_2 + c_3 + c_4 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_3 = c_4$. Moreover, the integers c_1, c_2, c_3 and c_4

are all nonzero, because $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$, and π_A is contained in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $c_1+c_2+c_3+c_4 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XVI). We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}_1) = 2$ and $f(\mathfrak{p}) = 1$ for all primes $\mathfrak{p}$ lying above p satisfying $\mathfrak{p} \neq \mathfrak{p}_1$. Then it holds that $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}\mathfrak{p}_3^{c_4}\overline{\mathfrak{p}_3}^{c_5}$, where $2c_1 + c_2 + c_3 + c_4 + c_5 = 3n$ and $\frac{2c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n}, \frac{c_5}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_2 = c_3$ and $c_4 = c_5$. Moreover, the integers c_2, c_3, c_4 and c_5 are all nonzero, because π_A is contained in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $2c_1 + c_2 + c_3 + c_4 + c_5 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XVII). We have $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}) = 1$ for all primes $\mathfrak{p}$ lying above p. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\overline{\mathfrak{p}_2}^{c_3}\mathfrak{p}_3^{c_4}\overline{\mathfrak{p}_3}^{c_5}$, where $c_1+c_2+c_3+c_4+c_5 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n}, \frac{c_5}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_2 = c_3$ and $c_4 = c_5$. Moreover, the integers c_2, c_3, c_4 and c_5 are all nonzero, because π_A is contained in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $c_1 + c_2 + c_3 + c_4 + c_5 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

Case (XVIII). We have $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $f(\mathfrak{p}) = 1$ for all primes $\mathfrak{p}$ lying above p. Then $(\pi_A) = \mathfrak{p}_1^{c_1}\overline{\mathfrak{p}_1}^{c_2}\mathfrak{p}_2^{c_3}\overline{\mathfrak{p}_2}^{c_4}\mathfrak{p}_3^{c_5}\overline{\mathfrak{p}_3}^{c_6}$, where $c_1 + c_2 + c_3 + c_4 + c_5 + c_6 = 3n$ and $\frac{c_1}{n}, \frac{c_2}{n}, \frac{c_3}{n}, \frac{c_4}{n}, \frac{c_5}{n}, \frac{c_6}{n} \in \mathbb{Z}$. It follows that $(\pi_A) = (\overline{\pi_A})$ if and only if $c_1 = c_2$ and $c_3 = c_4$ and $c_5 = c_6$. Moreover, the integers c_1, c_2, c_3, c_4, c_5 and c_6 are all nonzero, because π_A is contained in at least one of $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$, in at least one of $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$, and in at least one of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. But that implies $c_1 + c_2 + c_3 + c_4 + c_5 + c_6 > 3n$. Hence, it is not possible that $(\pi_A) = (\overline{\pi_A})$.

This shows that Table 3.4 contains all factorizations of (π_A) satisfying $(\pi_A) = (\overline{\pi_A})$. Hence, the abelian threefold A is $\overline{\mathbb{F}_q}$-isogenous to the third power of a supersingular elliptic curve if and only if $p\mathcal{O}_K$ factors as in Table 3.1 or (π_A) factors as in Table 3.4. □

Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold. Let π_A be a root of f_A and let $K = \mathbb{Q}(\pi_A)$. If $K/\mathbb{Q}$ is an abelian extension, then p splits completely in K. To prove this result, we need the following lemma.

Lemma 3.25. If K/M is an abelian extension, then every intermediate field is an abelian extension of M.

Proof. To prove this result, we will use the fundamental theorem of Galois extensions. The fundamental theorem of Galois extensions states that K^H, the set of those elements of K fixed by every automorphism in a subgroup H of $\mathrm{Gal}(K/M)$, is a Galois extension of M if and only if H is a normal subgroup of $\mathrm{Gal}(K/M)$.

Let L be a field such that $M \subseteq L \subseteq K$. The group $\mathrm{Aut}(K/L)$ is a subgroup of $\mathrm{Gal}(K/M)$.

The set of elements of K that is fixed by every automorphism of $\mathrm{Aut}(K/L)$ is precisely L. Moreover, the group $\mathrm{Gal}(K/M)$ is abelian, because K/M is an abelian extension. Therefore, the group $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/M)$. Hence, the fundamental theorem of Galois extensions implies that L is a Galois extension of M, because $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/M)$. Moreover,

$$\mathrm{Gal}(L/M) = \mathrm{Gal}(K/M)/\mathrm{Aut}(K/L).$$

Since the quotient of an abelian group by any subgroup is abelian, it follows that $\mathrm{Gal}(L/M)$ is abelian. Hence, the extension L/M is an abelian extension. □

The following theorem by Gonzalez states that p splits completely in K if $K/\mathbb{Q}$ is an abelian extension.

Theorem 3.26. ([7, Theorem 3.6(iii)]) Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold and assume that the center $\mathcal{Z}(\mathrm{End}^0(A))$ of $\mathrm{End}^0(A)$ is an abelian extension of $\mathbb{Q}$. Then p splits completely in $\mathcal{Z}(\mathrm{End}^0(A))$.

Proof. There exists an integer $N > 0$ such that $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^N}}(A)$. Let $q' = q^N$ and consider $A/\mathbb{F}_{q'}$. If π_A is the Frobenius of $A/\mathbb{F}_q$, then $\pi'_A = \pi_A^N$ is the Frobenius of $A/\mathbb{F}_{q'}$. By Theorem 2.10, the center of $\mathrm{End}^0_{\mathbb{F}_{q'}}(A)$ is isomorphic to $\mathbb{Q}(\pi'_A)$, so

$$\mathcal{Z}(\mathrm{End}^0(A)) = \mathcal{Z}(\mathrm{End}^0_{\mathbb{F}_{q'}}(A)) \cong \mathbb{Q}(\pi'_A).$$

For all integers $r > 0$, it holds that $\mathrm{End}^0_{\mathbb{F}_{q'}}(A) \subseteq \mathrm{End}^0_{\mathbb{F}_{(q')^r}}(A) \subseteq \mathrm{End}^0(A)$. Since we have $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q'}}(A)$, this implies that $\mathrm{End}^0_{\mathbb{F}'_q}(A) = \mathrm{End}^0_{\mathbb{F}_{(q')^r}}(A)$ for all integers $r > 0$. In particular, the centers $\mathbb{Q}(\pi'_A)$ and $\mathbb{Q}((\pi'_A)^r)$ of $\mathrm{End}^0_{\mathbb{F}_{q'}}(A)$ and $\mathrm{End}^0_{\mathbb{F}_{(q')^r}}(A)$ are equal for all integers $r > 0$. Hence, it holds that $\mathbb{Q}((\pi'_A)^r) = \mathbb{Q}(\pi'_A)$ for all integers $r > 0$. We will use K to denote the field $\mathbb{Q}(\pi'_A)$.

The endomorphism algebra $\mathrm{End}^0(A)$ is either K or $\mathcal{D}_A$. Therefore, the degree of the abelian extension $K/\mathbb{Q}$ is either 2 or 6. Suppose $[K : \mathbb{Q}] = 2$. Corollary 3.16 states that there exists at least one prime ideal $\mathfrak{p}$ in K dividing p such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$, because $A/\mathbb{F}_{q'}$ is absolutely simple. This implies that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and p splits completely.

Next, assume $[K : \mathbb{Q}] = 6$. Then the characteristic polynomial f'_A of π'_A is irreducible. Since $K/\mathbb{Q}$ is an abelian extension, there exist $e, f \in \mathbb{Z}$ such that $e(\mathfrak{p}) = e$ and $f(\mathfrak{p}) = f$ for all primes $\mathfrak{p}$ lying above p in K. Also K_+, the subfield of K fixed by complex conjugation, is an abelian extension by Lemma 3.25. Therefore, there exist $e_+, f_+ \in \mathbb{Z}$ such that $e(\mathfrak{P}) = e_+$ and $f(\mathfrak{P}) = f_+$ for all primes $\mathfrak{P}$ lying above p in K_+. Moreover, it holds

that $[K:\mathbb{Q}] = 6$ and Corollary 3.16 implies that at least one prime ideal $\mathfrak{p}$ above p in K satisfies $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Therefore, we have $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ or $p\mathcal{O}_K = \mathfrak{p}^3\overline{\mathfrak{p}}^3$ or $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$, see cases (I), (II) and (XVIII) of Table 3.2 respectively.

Suppose $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ or $p\mathcal{O}_K = \mathfrak{p}^3\overline{\mathfrak{p}}^3$. Since

$$(\pi'_A)(\overline{\pi'_A}) = (\pi'_A\overline{\pi'_A}) = (p^{nN}) = (p)^{nN},$$

it holds that all prime ideals appearing in the factorization of (π'_A) are lying above p. In both cases $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and $p\mathcal{O}_K = \mathfrak{p}^3\overline{\mathfrak{p}}^3$, there are two prime ideals lying above p that are each others conjugate. Hence, we can assume that $(\pi'_A) = \mathfrak{p}^a\overline{\mathfrak{p}}^b$ for some positive integers a and b, regardless of the factorization of p. Let

$$\mathcal{D} \coloneqq \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

be the decomposition group of $\mathfrak{p}$. Then $|\mathcal{D}| = ef$, where e is the ramification index and f the residue class degree of $\mathfrak{p}$ with respect to p. Recall that $e(\mathfrak{p}) = e$ and $f(\mathfrak{p}) = f$ for all primes $\mathfrak{p}$ above p in K, because $K/\mathbb{Q}$ is an abelian extension. Since $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ or $p\mathcal{O}_K = \mathfrak{p}^3\overline{\mathfrak{p}^3}$, it holds that $|\mathcal{D}| = ef > 1$. Hence there exists $\sigma \in \mathcal{D}$ such that σ is not the identity map. Since complex conjugation commutes with all automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$, we have

$$\sigma(\overline{\mathfrak{p}}) = \overline{\sigma(\mathfrak{p})} = \overline{\mathfrak{p}}.$$

Since $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(\overline{\mathfrak{p}}) = \overline{\mathfrak{p}}$, it holds that

$$(\sigma(\pi'_A)) = \sigma((\pi'_A)) = \sigma(\mathfrak{p}^a\overline{\mathfrak{p}}^b) = \sigma(\mathfrak{p})^a\sigma(\overline{\mathfrak{p}})^b = \mathfrak{p}^a\overline{\mathfrak{p}}^b = (\pi'_A).$$

Hence, the ideals (π'_A) and $(\sigma(\pi'_A))$ coincide. It follows that there exists a unit $u \in \mathcal{O}_K$ such that $\pi'_A = u\sigma(\pi'_A)$. The characteristic polynomial f'_A of π'_A is a Weil polynomial by Corollary 2.19. Since f'_A has coefficients in $\mathbb{Q}$ and $\mathbb{Q}$ is invariant under σ, it holds that $\sigma(\pi'_A)$ is a root of f'_A. Hence, both π'_A and $\sigma(\pi'_A)$ are Weil q'-numbers. Thus, we have $|\phi(\pi'_A)| = |\phi(\sigma(\pi'_A))|$ for all embeddings $\phi : K \to \mathbb{C}$. Since $\pi'_A = u\sigma(\pi'_A)$, it follows that $|\phi(u)| = 1$ for all embeddings $\phi : K \to \mathbb{C}$. Hence, the element u is a root of unity by Lemma 3.14. Let s be the order of u. Then $(\pi'_A)^s = u^s\sigma(\pi'_A)^s = \sigma((\pi'_A)^s)$, so $(\pi'_A)^s$ is invariant under σ. This implies that $[\mathbb{Q}((\pi'_A)^s) : \mathbb{Q}] < [\mathbb{Q}(\pi'_A) : \mathbb{Q}]$. Recall that in the beginning of this proof, we showed that $\mathbb{Q}((\pi'_A)^r) = \mathbb{Q}(\pi'_A)$ for all integers $r > 0$ and therefore $[\mathbb{Q}((\pi'_A)^s) : \mathbb{Q}] = [\mathbb{Q}(\pi'_A) : \mathbb{Q}]$. Since we obtained a contradiction, we can conclude that p does not split as $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ or $p\mathcal{O}_K = \mathfrak{p}^3\overline{\mathfrak{p}}^3$. Hence, it holds that $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ and p splits completely in K. □

Corollary 3.27. Let $A/\mathbb{F}_q$, with $q = p^n$, be an absolutely simple abelian threefold and assume that the center $\mathcal{Z}(\mathrm{End}^0(A))$ of $\mathrm{End}^0(A)$ is an abelian extension of $\mathbb{Q}$. Let the integer $N > 0$ be such that $\mathrm{End}^0(A) = \mathrm{End}^0_{\mathbb{F}_{q^N}}(A)$ and set $q' = q^N$. Let π'_A be the Frobenius endomorphism of $A/\mathbb{F}_{q'}$ and f'_A the characteristic polynomial of π'_A. If f'_A is irreducible, then $r(A) = 3$; otherwise, $r(A) = 0$.

Proof. Proposition 3.1 states that f'_A is irreducible or $f'_A = h^3$, where h is a second degree irreducible Weil polynomial, because $A/\mathbb{F}_{q'}$ is simple. If $f'_A = h^3$, then Theorem 3.7 implies that $r(A) = 0$.

Assume f'_A is irreducible and let $K = \mathbb{Q}(\pi'_A)$. Then p splits completely in K by Theorem 3.26. Thus, $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3\overline{\mathfrak{p}_3}$ and $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$ for each prime $\mathfrak{p}$ above p in K. Since f'_A is irreducible, the invariants $f(\mathfrak{p}) \cdot \frac{\mathrm{ord}_{\mathfrak{p}}(\pi'_A)}{nN} = \frac{\mathrm{ord}_{\mathfrak{p}}(\pi'_A)}{nN} \in \mathbb{Z}$ for each prime $\mathfrak{p}$ above p in K by Corollary 2.26. Thus, it holds that $\mathrm{ord}_{\mathfrak{p}}(\pi'_A)$ is an integer multiple of nN for all primes $\mathfrak{p}$ above p in K. For each $i \in \{1,2,3\}$, the primes $\mathfrak{p}_i$ and $\overline{\mathfrak{p}_i}$ contain p and hence contain $\pi'_A\overline{\pi'_A} = p^n$. Therefore, π'_A or $\overline{\pi'_A}$ must be contained in $\mathfrak{p}_i$ and the same holds for $\overline{\mathfrak{p}_i}$. This shows that π'_A is contained in at least one of $\mathfrak{p}_i$ and $\overline{\mathfrak{p}}_i$. As $\mathrm{ord}_{\mathfrak{p}}(\pi'_A)$ is an integer multiple of nN for all primes $\mathfrak{p}$ above p in K, this implies that $\mathrm{ord}_{\mathfrak{p}_i}(\pi_A) + \mathrm{ord}_{\overline{\mathfrak{p}_i}}(\pi_A) \geq nN$. Moreover, $\mathrm{N}_{K/\mathbb{Q}}(\pi_A) = p^{3nN}$ and every prime $\mathfrak{p}$ above p in K has norm p, because $f(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ above p in K. So by comparing the norms of (π'_A) and the prime ideals $\mathfrak{p}|p$, it holds that

$$\mathrm{ord}_{\mathfrak{p}_i}(\pi'_A) + \mathrm{ord}_{\overline{\mathfrak{p}_i}}(\pi'_A) = nN$$

for all $i \in \{1,2,3\}$. Furthermore, $\mathrm{ord}_{\mathfrak{p}_i}(\pi'_A), \mathrm{ord}_{\overline{\mathfrak{p}_i}}(\pi'_A) \in \{0, nN\}$, because the invariants are integers. Hence, precisely one of $\mathfrak{p}_i$ and $\overline{\mathfrak{p}_i}$ appears in the prime factorization of (π'_A) and it follows that (π'_A) and $(\overline{\pi'_A})$ are relatively prime. Then

$$(\pi'_A)(\overline{\pi'_A}) = (\pi'_A\overline{\pi'_A}) = (p)^{nN} = \mathfrak{p}_1^{nN}\overline{\mathfrak{p}_1}^{nN}\mathfrak{p}_2^{nN}\overline{\mathfrak{p}_2}^{nN}\mathfrak{p}_3^{nN}\overline{\mathfrak{p}_3}^{nN},$$

and without loss of generality $(\pi'_A) = \mathfrak{p}_1^{nN}\mathfrak{p}_2^{nN}\mathfrak{p}_3^{nN}$ and $(\overline{\pi'_A}) = \overline{\mathfrak{p}_1}^{nN}\overline{\mathfrak{p}_2}^{nN}\overline{\mathfrak{p}_3}^{nN}$. Thus, the primes above p are $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\overline{\mathfrak{p}_1}$, $\overline{\mathfrak{p}_2}$ and $\overline{\mathfrak{p}_3}$ and π'_A is not contained in $\overline{\mathfrak{p}_1}$, $\overline{\mathfrak{p}_2}$ and $\overline{\mathfrak{p}_3}$. Hence, we have $r(A) = 3$ by Theorem 3.13. □

Chapter 4

Reduction of CM abelian threefolds

In this chapter, we will introduce CM abelian varieties. For this purpose, we will first give a short background on CM fields and CM types. Our focus will be on CM abelian threefolds, which have CM by a sextic CM field. We will restrict to sextic CM fields of which the Galois group of the normal closure is cyclic or isomorphic to the dihedral group D_6. The goal is to determine the endomorphism algebra and p-rank of the reduction of an absolutely simple CM abelian threefold.

4.1 CM fields and CM types

In this section, we explain the basics of CM fields and CM types. After that, we restrict to sextic CM fields of which the Galois group of the normal closure is cyclic or isomorphic to D_6. In both cases we explore the CM types and the corresponding reflex CM pairs. This section is mainly based on Shimura-Taniyama [18] and Lang [13].

Definition 4.1. A *CM field* is a totally imaginary quadratic extension of a totally real number field K_+. In other words, a CM field is a field $K = K_+(\sqrt{-d})$ for a totally real number field K_+ and a totally positive element $d \in K_+$.

By Lang [13, §2], we can also characterize a CM field as a field K with complex conjugation commuting with every complex embedding of K, and K is not real. Since a CM field K is a quadratic extension of a totally real number field K_+, it follows

that $[K : \mathbb{Q}] = 2g$, where $g = [K_+ : \mathbb{Q}]$. Hence, a CM field K has g pairs of complex conjugate embeddings.

Definition 4.2. Let K be a CM field of degree $2g$ and let K' be the normal closure of K. Then a *CM type* Φ of K with values in K' is a set of g embeddings of K such that exactly one embedding of each of the g pairs of complex conjugate embeddings is in Φ. We call (K, Φ) a *CM type* or *CM pair*.

Let (K, Φ) be a CM pair and let σ be an automorphism of K. Then define

$$\Phi\sigma \coloneqq \{\phi \circ \sigma : \phi \in \Phi\}.$$

If K' is the normal closure of K and γ is an automorphism of K', then define

$$\gamma\Phi \coloneqq \{\gamma \circ \phi : \phi \in \Phi\}.$$

Definition 4.3. The CM types Φ_1 and Φ_2 of a CM field K are called *equivalent* if there is an automorphism σ of K such that $\Phi_1 = \Phi_2\sigma$.

Every CM type of a CM field K is equivalent to itself, because the identity map is an automorphism of K. Let Φ_1, Φ_2 and Φ_3 be CM types of K. If there exist automorphisms σ and γ of K such that $\Phi_1 = \Phi_2\sigma$ and $\Phi_2 = \Phi_3\gamma$, then $\Phi_1 = \Phi_3\gamma\sigma$. Since the composition of two automorphisms is also an automorphism of K, it follows that Φ_1 and Φ_3 are equivalent. Moreover, if $\Phi_1 = \Phi_2\sigma$, then $\Phi_2 = \Phi_1\sigma^{-1}$. The map σ^{-1} exists and is an automorphism of K, since σ is an automorphism of K. Hence, the equivalence relation of Definition 4.3 is reflexive, transitive and symmetric, and that means it is an equivalence relation.

Definition 4.4. Let K be a CM field with normal closure K'. If K_0 is a proper CM subfield of K and Φ_0 is a CM type of K_0 with values in K', then the CM type of K *induced* by Φ_0 is $\{\phi \in \mathrm{Hom}(K, K') : \phi|_{K_0} \in \Phi_0\}$. A CM type Φ of K is called *primitive* if Φ is not induced by the CM type of a proper CM subfield of K.

The following proposition by Shimura-Taniyama can be used to check if a CM type is primitive.

Proposition 4.5. ([18, Proposition II.26]) Let (K, Φ) be a CM pair and let K' be the normal closure of K. Let $\Phi_{K'}$ be the CM type of K' induced by Φ. Then (K, Φ) is primitive if and only if

$$\mathrm{Gal}(K'/K) = \{\gamma \in \mathrm{Gal}(K'/\mathbb{Q}) : \gamma\Phi_{K'} = \Phi_{K'}\}.$$

Corollary 4.6. Let K be a normal CM field and Φ a CM type of K. Then (K, Φ) is primitive if and only if there is no nontrivial element $\gamma \in \mathrm{Gal}(K/\mathbb{Q})$ satisfying $\gamma\Phi = \Phi$.

Let (K, Φ) be a CM type and let K' be the normal closure of K. Let $\Phi_{K'}$ be the CM type of K' induced by Φ. The maps in $\Phi_{K'}$ are embeddings from K' to K' and therefore isomorphisms. Hence, the inverse $\Phi_{K'}^{-1} \coloneqq \{\phi^{-1} : \phi \in \Phi_{K'}\}$ is well-defined and will be used in the following proposition by Shimura-Taniyama.

Proposition 4.7. ([18, Proposition II.28]) Let (K, Φ) be a CM pair, let K' be the normal closure of K and let $\Phi_{K'}$ be the CM type of K' induced by Φ. Let K^r be the fixed field of

$$\{\gamma : \gamma \in \mathrm{Gal}(K'/\mathbb{Q}), \gamma\phi_{K'}^{-1} = \Phi_{K'}^{-1}\}$$

and $\Phi^r = \Phi_{K'}^{-1}|_{K^r}$. Then (K^r, Φ^r) is a primitive CM type and

$$K^r = \mathbb{Q}\Big(\Big\{ \sum_{\phi\in\Phi} \phi(x) : x \in K\Big\}\Big).$$

Definition 4.8. The primitive CM type (K^r, Φ^r) as given in Proposition 4.7 is called the *reflex pair* or *reflex type* of the CM pair (K, Φ). The field K^r is the *reflex field* of (K, Φ) and the CM type Φ^r is the *reflex CM type* of (K, Φ).

Proposition 4.9. ([11, Lemma 1.2.5]) Let (K, Φ) be a CM pair. Then the reflex field K^{rr} of (K^r, Φ^r) is a subfield of K with primitive CM type Φ^{rr}. If Φ is primitive, then $K^{rr} = K$ and $\Phi^{rr} = \Phi$.

Definition 4.10. The *type norm* of a CM pair (K, Φ) is the multiplicative map

$$\begin{aligned} \mathrm{N}_\Phi : K &\to K^r \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x). \end{aligned}$$

Let (K, Φ) be a CM pair. The type norm of the reflex pair (K^r, Φ^r) of (K, Φ) is

$$\begin{aligned} \mathrm{N}_{\Phi^r} : K^r &\to K^{rr} \\ x &\mapsto \prod_{\phi\in\Phi^r} \phi(x). \end{aligned}$$

If Φ is primitive, then $K^{rr} = K$ by Proposition 4.9 and $\mathrm{N}_{\Phi^r} : K^r \to K$. The following proposition by Shimura-Taniyama shows that $\mathrm{N}_{\Phi^r} : K^r \to K$ regardless of Φ being primitive and explains what happens if we apply N_{Φ^r} to an ideal of K^r.

Proposition 4.11. ([17, Proposition II.29]) Let (K, Φ) be a CM pair, let (K^r, Φ^r) be its reflex CM pair and let K' be the normal closure of K. Let α be an element of K^r and put $\mathrm{N}_{\Phi^r}(\alpha) = \prod_{\phi\in\Phi^r} \phi(\alpha)$. Then $\mathrm{N}_{\Phi^r}(\alpha)$ is an element of K satisfying $\mathrm{N}_{\Phi^r}(\alpha)\overline{\mathrm{N}_{\Phi^r}(\alpha)} = N_{K^r/\mathbb{Q}}(\alpha)$. Let further $\mathfrak{p}$ be an ideal in K^r. Then there exists an ideal $N_{\Phi^r}(\mathfrak{p})$ in K such that

$$N_{\Phi^r}(\mathfrak{p})\mathcal{O}_{K'} = \prod_{\phi\in\Phi^r} \phi(\mathfrak{p})\mathcal{O}_{K'} \qquad \text{and} \qquad \mathrm{N}_{\Phi^r}(\mathfrak{p})\overline{\mathrm{N}_{\Phi^r}(\mathfrak{p})} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K.$$

Dodson classified the possible Galois groups of the normal closure of an arbitrary sextic CM field.

Theorem 4.12. ([5], [1, Proposition 2.1]) Let K be a sextic CM field and let K' be the normal closure of K. Then $\mathrm{Gal}(K'/\mathbb{Q})$ is one of the following groups

(i) C_6,

(ii) D_6, the dihedral group with 12 elements,

(iii) $(C_2)^3 \rtimes C_3$,

(iv) $(C_2)^3 \rtimes S_3$,

where $\rtimes$ denotes the semi-direct product of groups, so C_3 and S_3 are acting by permutations on the three copies of C_2.

We restrict to sextic CM fields K of which the Galois group of the normal closure is cyclic or isomorphic to D_6. In both cases, we list the possible CM types of K and determine the equivalence classes, the primitive CM types and the reflex CM pairs.

4.1.1 Cyclic case.

Let $K/\mathbb{Q}$ be a cyclic CM field of degree 6 over $\mathbb{Q}$. Then

$$\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\} = \langle\sigma\rangle,$$

where σ^3 is complex conjugation. The eight different CM types of K are

$$\begin{aligned} \Phi_1 &= \{1, \sigma, \sigma^2\}, & \Phi_5 &= \{\sigma^3, \sigma^4, \sigma^5\}, \\ \Phi_2 &= \{1, \sigma, \sigma^5\}, & \Phi_6 &= \{\sigma^2, \sigma^3, \sigma^4\}, \\ \Phi_3 &= \{1, \sigma^2, \sigma^4\}, & \Phi_7 &= \{\sigma, \sigma^3, \sigma^5\}, \\ \Phi_4 &= \{1, \sigma^4, \sigma^5\}, & \Phi_8 &= \{\sigma, \sigma^2, \sigma^3\}. \end{aligned}$$

For $i \in \{3, 7\}$, we find $\sigma^2\Phi_i = \Phi_i$. Hence, the CM types Φ_3 and Φ_7 are not primitive by Corollary 4.6. They are equivalent, because $\Phi_3 = \Phi_7\sigma^3$. For $i \in \{1, 2, 4, 5, 6, 8\}$, it holds that $\gamma\Phi_i \neq \Phi_i$ for all $\gamma \in \mathrm{Gal}(K/\mathbb{Q})\backslash\{1\}$. Hence, the CM types $\Phi_1, \Phi_2, \Phi_4, \Phi_5, \Phi_6$ and Φ_8 are primitive by Corollary 4.6. Table 4.1 shows that every primitive CM type of K is equivalent to Φ_1. It then follows from the fact that the equivalence is reflexive, symmetric and transitive, that all primitive CM types of K are equivalent.

i	$\gamma \in \mathrm{Aut}(K) \,:\, \Phi_i\gamma = \Phi_1$
1	1
2	σ
4	σ^2
5	σ^3
6	σ^4
8	σ^5

Table 4.1: The left column contains the numbers i corresponding to the primitive CM types Φ_i of K. In the right column are the automorphisms γ of K such that $\Phi_i\gamma = \Phi_1$.

Since K is normal, the reflex type of a CM type (K, Φ) is (K, Φ^{-1}). The reflex CM types of $\Phi_1, \ldots, \Phi_8$ are listed in Table 4.2.

i	1	2	3	4	5	6	7	8
Φ_i^r	Φ_4	Φ_2	Φ_3	Φ_1	Φ_8	Φ_6	Φ_7	Φ_5

Table 4.2: The top row contains the number i corresponding to the CM types Φ_i of K. The bottom row contains the reflex CM types Φ_i^r of (K, Φ_i).

4.1.2 $\mathbf{D_6}$ case.

Let K be a sextic CM field of which the Galois group of the normal closure K' is isomorphic to D_6. Then

$$\begin{aligned}\mathrm{Gal}(K'/\mathbb{Q}) \cong D_6 &= \langle x, y : x^2 = y^6 = xyxy = 1\rangle \\ &= \{1, x, y, y^2, y^3, y^4, y^5, xy, xy^2, xy^3, xy^4, xy^5\},\end{aligned}$$

where complex conjugation is given by y^3. The elements $1, x \in \mathrm{Gal}(K'/\mathbb{Q})$ fix K, so

$$\begin{aligned} 1|_K &= x|_K, & y|_K &= xy|_K, \\ y^2|_K &= xy^2|_K, & y^3|_K &= xy^3|_K, \\ y^4|_K &= xy^4|_K, & y^5|_K &= xy^5|_K. \end{aligned}$$

It follows that $\{1|_K, y|_K, y^2|_K, y^3|_K, y^4|_K, y^5|_K\}$ is the set of complex embeddings of K with values in K'. The eight different CM types of K are

$$\begin{aligned} \Phi_1 &= \{1|_K, y|_K, y^2|_K\}, & \Phi_5 &= \{y^3|_K, y^4|_K, y^5|_K\}, \\ \Phi_2 &= \{1|_K, y|_K, y^5|_K\}, & \Phi_6 &= \{y^2|_K, y^3|_K, y^4|_K\}, \\ \Phi_3 &= \{1|_K, y^2|_K, y^4|_K\}, & \Phi_7 &= \{y|_K, y^3|_K, y^5|_K\}, \\ \Phi_4 &= \{1|_K, y^4|_K, y^5|_K\}, & \Phi_8 &= \{y|_K, y^2|_K, y^3|_K\}. \end{aligned}$$

We use Proposition 4.5 to check which of the CM types above are primitive. Since $[K' : K] = 2$ and K is fixed by $1, x \in \mathrm{Gal}(K'/\mathbb{Q})$, we have $\mathrm{Gal}(K'/K) = \{1, x\}$. Let $\Phi^i_{K'}$ be the CM type of K' induced by Φ_i. The induced CM types of K' are listed in Table 4.3.

i	$\Phi^i_{K'}$
1	$\{1, x, y, y^2, xy, xy^2\}$
2	$\{1, x, y, y^5, xy, xy^5\}$
3	$\{1, x, y^2, y^4, xy^2, xy^4\}$
4	$\{1, x, y^4, y^5, xy^4, xy^5\}$
5	$\{y^3, y^4, y^5, xy^3, xy^4, xy^5\}$
6	$\{y^2, y^3, y^4, xy^2, xy^3, xy^4\}$
7	$\{y, y^3, y^5, xy, xy^3, xy^5\}$
8	$\{y, y^2, y^3, xy, xy^2, xy^3\}$

Table 4.3: The left column contains the numbers i corresponding to the CM types Φ_i of K. In the right column are the CM types $\Phi^i_{K'}$ induced by Φ_i.

We have $\gamma\Phi^i_{K'} = \Phi^i_{K'}$ for all $i \in \{1, \ldots, 8\}$ and for all $\gamma \in \mathrm{Gal}(K'/K)$. For $i \in \{3, 7\}$, we find $y^4\Phi^i_{K'} = \Phi^i_{K'}$. Therefore, the CM types Φ_3 and Φ_7 are not primitive by Proposition 4.5. They are equivalent, because $\Phi_3 = \Phi_7 y^3|_K$ and $y^3|_K$ is an automorphism of K. For $i \in \{1, 2, 4, 5, 6, 8\}$, it holds that $\gamma\Phi^i_{K'} \neq \Phi^i_{K'}$ for all $\gamma \in \mathrm{Gal}(L/\mathbb{Q})\backslash\mathrm{Gal}(K'/K)$. Hence, the CM types $\Phi_1, \Phi_2, \Phi_4, \Phi_5, \Phi_6$ and Φ_8 are primitive by Proposition 4.5.

To find the equivalences in the set of primitive CM types $\{\Phi_1, \Phi_2, \Phi_4, \Phi_5, \Phi_6\}$, we first determine the automorphisms of K. The degree $[K : \mathbb{Q}] = 6$, so $|\mathrm{Aut}(K/\mathbb{Q})| \leq 6$.

Moreover, the maps $1|_K$ and $y^3|_K$ are automorphisms of K and the order of $y^3|_K$ in $\mathrm{Aut}(K/\mathbb{Q})$ is 2. Therefore, it holds that $|\mathrm{Aut}(K/\mathbb{Q})|$ is divisible by 2. Furthermore, the extension $K/\mathbb{Q}$ is not Galois, so $\mathrm{Aut}(K/\mathbb{Q}) \neq [K : \mathbb{Q}] = 6$. Hence, we have $|\mathrm{Aut}(K/\mathbb{Q})| \in \{2, 4\}$. Suppose $|\mathrm{Aut}(K/\mathbb{Q})| = 4$ and let $F \coloneqq K^{\mathrm{Aut}(K/\mathbb{Q})}$, the subfield of K fixed by $\mathrm{Aut}(K/\mathbb{Q})$. Then we have $[K : F] = |\mathrm{Aut}(K/\mathbb{Q})| = 4$, see Dummit-Foote [6, Theorem 14.9]. But $[K : F]$ has to divide $[K : \mathbb{Q}] = 6$. Therefore, it is not possible that $|\mathrm{Aut}(K/\mathbb{Q})| = 4$. It follows that $\mathrm{Aut}(K/\mathbb{Q}) = \{1|_K, y^3|_K\}$. Since $\Phi_1 = \Phi_5 y^3|_K$, $\Phi_2 = \Phi_6 y^3|_K$ and $\Phi_4 = \Phi_8 y^3|_K$, we find that the primitive CM types of K are divided into three equivalence classes: $\{\Phi_1, \Phi_5\}$, $\{\Phi_2, \Phi_6\}$ and $\{\Phi_4, \Phi_8\}$.

Let Φ be a CM type of K and let $\Phi_{K'}$ be the CM type of K' induced by Φ. The reflex field K^r and the reflex CM type Φ_i^r of (K, Φ_i) for $i \in \{1, \ldots, 8\}$ are listed in Table 4.4.

i	$\{\gamma : \gamma \in \mathrm{Gal}(L/\mathbb{Q}), \gamma\phi_{K'}^{-1} = \Phi_{K'}^{-1}\}$	Φ_i^r
1	$\{1, xy^2\}$	$\{1\|_{K^r}, y^4\|_{K^r}, y^5\|_{K^r}\}$
2	$\{1, x\}$	Φ_2
3	$\{1, x\}$	Φ_3
4	$\{1, xy^4\}$	$\{1\|_{K^r}, y\|_{K^r}, y^2\|_{K^r}\}$
5	$\{1, xy^2\}$	$\{y\|_{K^r}, y^2\|_{K^r}, y^3\|_{K^r}\}$
6	$\{1, x\}$	Φ_6
7	$\{1, x\}$	Φ_7
8	$\{1, xy^4\}$	$\{y^3\|_{K^r}, y^4\|_{K^r}, y^5\|_{K^r}\}$

Table 4.4: The first column contains the numbers i corresponding to the CM types Φ_i of K. In the second column are the subsets of $\mathrm{Gal}(K'/\mathbb{Q})$ that fix the reflex field K^r of (K, Φ_i). The last column contains the reflex CM types Φ_i^r of (K, Φ_i).

4.2 CM abelian varieties

In this brief section based on Shimura [17] and Shimura-Taniyama [18], we explain CM abelian varieties and give two results.

Definition 4.13. An abelian variety A over a field k of dimension g has *complex multiplication* (CM) by a CM field K if K has degree $2g$ and there is an embedding $\theta : K \hookrightarrow \mathrm{End}^0(A)$. If $\theta^{-1}(\mathrm{End}(A)) = \mathcal{O}$ for an order $\mathcal{O} \subset K$, then A has CM by the order $\mathcal{O}$.

Let A be an abelian variety with CM by a CM field K and let θ be the embedding $\theta : K \hookrightarrow \mathrm{End}^0(A)$. The pair (A, θ) uniquely determines a CM type Φ of K, see

Shimura-Taniyama [18, §5.2]. In that case, (A, θ) is called an *abelian variety of CM type* (K, Φ).

Proposition 4.14. ([17, Proposition II.30]) Let (A, θ) be an abelian variety over a field k of CM type (K, Φ). Let K^r be the reflex CM field of (K, Φ). If every element of $\theta(K) \cap \mathrm{End}(A)$ is defined over k, then $K^r \subset k$. Conversely, if $K^r \subset k$ and Φ is primitive, then every element of $\mathrm{End}(A)$ is defined over k.

The CM type of a CM abelian variety A can be used to determine whether or not A is absolutely simple. This is the subject of the following theorem by Shimura.

Theorem 4.15. ([17, §8.2]) Let (K, Φ) be a CM type. A CM abelian variety of CM type (K, Φ) is absolutely simple if and only if Φ is primitive.

4.3 Reduction of absolutely simple CM abelian threefolds

In this section we will study the endomorphism algebra of the reduction of an absolutely simple abelian threefold with CM by $\mathcal{O}_K$, where K is a sextic CM field. The sextic CM fields we consider are restricted to those of which the Galois group of the normal closure is cyclic or isomorphic to D_6. In the case that K is a cyclic sextic CM field, we will show that the endomorphism algebra of the reduction of an abelian threefold with CM by $\mathcal{O}_K$ determines the rank. This does not hold when K is a sextic CM field of which the Galois group of the normal closure is isomorphic to D_6. We finish with an example in which we determine the endomorphism algebra and rank of the reduction of an abelian threefold with CM by $\mathcal{O}_K$, where K is a sextic CM field of which the Galois group of the normal closure is isomorphic to D_6. For this purpose, we first give some information about reduced abelian varieties and state important related results.

An elliptic curve E over $\mathbb{Q}$ is given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The only coordinate changes fixing the point at infinity $[0, 1, 0]$, and preserving the Weierstrass form of the equation for E are of the form

$$(x, y) \mapsto (u^2x' + r, u^3y' + u^2sx' + t),$$

where $u, r, s, t \in \overline{\mathbb{Q}}$ and $u \neq 0$. The discriminant Δ' of E after the coordinate change can be computed as $\Delta' = u^{-12}\Delta$. Let p be a rational prime and let $v_p(\cdot) = \mathrm{ord}_p(\cdot)$. A *minimal Weierstrass equation for E at v_p* is a Weierstrass equation for E such that $v_p(\Delta)$ is minimized subject to the condition that $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{Z}$. As coordinate changes

affect the discriminant by $\Delta' = u^{-12}\Delta$, it holds that $v_p(\Delta)$ can only be changed by multiples of 12. This implies that $v_p(\Delta) < 12$ is a sufficient (but not necessary) condition for the Weierstrass equation for an elliptic curve to be minimal. By reducing the coefficients of the minimal Weierstrass equation modulo p, we obtain the *reduction of E modulo p*. The reduction of E modulo p is possibly singular, meaning that the discriminant of E modulo p is zero. In this case, we say that E has *bad reduction at p*. If the reduction of E modulo p is nonsingular, then E has *good reduction at p* and the reduction of E modulo p is an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$.

Example 4.16. Consider the elliptic curve E over $\mathbb{Q}$ defined by

$$E : y^2 = x^3 + x^2 - 114x - 127.$$

The discriminant of E is $\Delta = 92236816 = 2^4 \cdot 7^8$. Thus, we have $v_p(\Delta) < 12$ for all primes p. Hence, the Weierstrass equation for E is minimal at v_p for all primes p. For $p = 2$ and $p = 7$, we find $v_p(\Delta) > 0$. This implies that the reduction of E modulo p is singular for $p = 2$ and $p = 7$, so E has bad reduction at $p = 2$ and $p = 7$. For all other primes, it holds that $v_p(\Delta) = 0$, so E has good reduction at all primes except $p = 2$ and $p = 7$.

Similar as for elliptic curves, abelian varieties over a number field k are defined by a (not unique) set of equations with coefficients in k. By reducing the coefficients of the defining equations for an abelian variety A modulo a prime ideal $\mathfrak{p}$ in k, we obtain the *reduction of A modulo $\mathfrak{p}$*. If for some set of equations defining A, the reduction of A modulo $\mathfrak{p}$ is again an abelian variety over $\mathcal{O}_k/\mathfrak{p}$, then A has *good reduction at $\mathfrak{p}$*. Otherwise, A has *bad reduction at $\mathfrak{p}$*. If A has good reduction at all primes $\mathfrak{p}$ in k, then A has *good reduction everywhere*.

Definition 4.17. If A is an abelian variety defined over a number field k and there exists a finite extension M of k such that A/M has good reduction at a prime ideal $\mathfrak{p} \subset \mathcal{O}_M$, then we say that A/k has *potential good reduction* at $\mathfrak{p} \cap \mathcal{O}_k$. If A/k has potential good reduction at all prime ideals in k, then A/k has *potential good reduction everywhere*.

Example 4.18. Consider the elliptic curve E over $\mathbb{Q}$ of Example 4.16 given by the minimal Weierstrass equation

$$E : y^2 = x^3 + x^2 - 114x - 127.$$

We showed in Example 4.16 that E has bad reduction at $p = 2$ and $p = 7$ and good reduction at all other primes. We make a base change to $M = \mathbb{Q}(\sqrt[3]{28})$. Applying the coordinate change

$$(x, y) \mapsto \left(7\sqrt[3]{28}x' + 16,\ 98y' + 49\sqrt[3]{28}x' + 49\right)$$

results in the Weierstrass equation

$$E : (y')^2 + \sqrt[3]{28}x'y' + y' = (x')^3.$$

Let $v_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of M. The discriminant of E/M is $\Delta' = 1$, so the Weierstrass equation is minimal at $v_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of M. Moreover, it holds that $v_{\mathfrak{p}}(\Delta) = 0$ for every prime ideal $\mathfrak{p}$. Hence, E/M has good reduction everywhere.

The following theorem by Serre and Tate states that every CM abelian variety defined over a number field has potential good reduction.

Theorem 4.19. ([16, Theorem 7], [14, Proposition 2.10]) Let A be a CM abelian variety over a number field k. Then there exists a cyclic extension M of k over which A acquires good reduction everywhere.

Once an abelian variety A over a number field k has good reduction everywhere over a finite extension M of k, the abelian variety A will have good reduction everywhere over every finite extension of M, see Milne [14, Theorem 17.3]

The next theorem, proven by Chai, Conrad and Oort, is about the abelian subvarieties of the reduction of CM abelian threefolds.

Theorem 4.20. ([1, Theorem 4.5], [3, Theorem 1.3.1.1]) Let A be a CM abelian threefold over a number field k. Suppose A has good reduction at a prime ideal $\wp \subset \mathcal{O}_k$ and let $\overline{A} \coloneqq A \mod \wp$. Then $\overline{A}$ is isotypic over both $\mathcal{O}_k/\wp$ and the algebraic closure of $\mathcal{O}_k/\wp$.

We can deduce the possible endomorphism algebras of the reduction of a CM abelian threefold from Theorem 4.20.

Corollary 4.21. Let A be a CM abelian threefold with CM by a CM field K defined over a number field k. Suppose A has good reduction at a prime ideal $\wp \subset \mathcal{O}_k$ and let $\overline{A} \coloneqq A \mod \wp$. Then

(i) $\mathrm{End}^0(\overline{A}) \cong K$ if $\overline{A}$ is absolutely simple and $f_{\overline{A}}$ is irreducible;

(ii) $\mathrm{End}^0(\overline{A}) \cong \mathcal{D}_{\overline{A}}$, where $\mathcal{D}_{\overline{A}}$ is a central simple algebra over $\mathbb{Q}(\pi_{\overline{A}})$ which splits at all finite primes of $\mathbb{Q}(\pi_{\overline{A}})$ not dividing p, but does not split at any real prime of $\mathbb{Q}(\pi_{\overline{A}})$, if $\overline{A}$ is absolutely simple and $f_{\overline{A}}$ is of the form h^e with $e > 1$;

(iii) $\mathrm{End}^0(\overline{A}) \cong M_3(\mathbb{Q}(\pi_{\overline{A}}))$ if A is isogenous to E^3 over the algebraic closure of $\mathcal{O}_k/\wp$, where E is an ordinary elliptic curve;

(iv) $\mathrm{End}^0(\overline{A}) \cong M_3(B_{p,\infty})$ if A is isogenous to E^3 over the algebraic closure of $\mathcal{O}_k/\wp$, where E is a supersingular elliptic curve.

Proof. Theorem 4.20 states that $\overline{A}$ is isotypic over the algebraic closure of $\mathcal{O}_k/\wp$, meaning that $\overline{A}$ is either absolutely simple, or isogenous over the algebraic closure of $\mathcal{O}_k/\wp$ to E^3, where E is an elliptic curve. If $\overline{A}$ is absolutely simple, then the possibilities for $\mathrm{End}^0(\overline{A})$ are (i) or (ii) by Theorem 2.22. Options (iii) and (iv) follow from Proposition 2.13(ii). If the elliptic curve E is supersingular, then $\mathrm{End}^0(E) \cong B_{p,\infty}$, see Theorem 1.17, and $\mathrm{End}^0(\overline{A}) \cong M_3(B_{p,\infty})$. If the elliptic curve E is ordinary, then $\mathrm{End}^0(E) \cong \mathbb{Q}(\pi_E)$, see Theorem 1.20, and $\mathrm{End}^0(\overline{A}) \cong M_3(\mathbb{Q}(\pi_E))$. Since $f_{\overline{A}} = f_E^3$ by Theorem 2.14, it follows that $\pi_E = \pi_{\overline{A}}$. □

Let A be an absolutely simple abelian variety over a number field k of CM type (K, Φ) and assume that A has CM by $\mathcal{O}_K$. Suppose A has good reduction at a prime ideal $\wp \subset \mathcal{O}_k$. Then there is a relation between the Frobenius endomorphism of $\overline{A} \coloneqq A \mod \wp$ and the reflex CM type of (K, Φ). This is the subject of the following important theorem by Shimura.

Theorem 4.22. ([17, Theorem III.1]) Let A be an absolutely simple abelian variety of dimension g over a number field k of CM type (K, Φ). Suppose A has CM by the ring of integers $\mathcal{O}_K$ of the CM field K with $[K : \mathbb{Q}] = 2g$. Let $\wp \subset \mathcal{O}_k$ be a prime ideal such that A has good reduction at $\wp$ and let $\overline{A} \coloneqq A \mod \wp$. Then the Frobenius endomorphism $\pi \in \mathcal{O}_K \subset \mathrm{End}(\overline{A})$ generates the ideal $\mathrm{N}_{\Phi^r}(\mathrm{N}_{k/K^r}(\wp)) = (\pi)$.

The following proposition by Kılıçer, Labrande, Lercier, Ritzenthaler, Sijsling and Streng uses Theorem 4.20 and Theorem 4.22 to classify the endomorphism algebras of the reduction of abelian threefolds with CM by $\mathcal{O}_K$, where K is a sextic cyclic CM field, with respect to the factorization of $p\mathcal{O}_K$ into prime ideals. The proposition is stated in [12, Proposition 4.1]. There only a sketch of the proof is given. We give a full detailed proof.

Proposition 4.23. ([12, Proposition 4.1]) Let A be an absolutely simple abelian threefold over a number field k such that A has good reduction at every prime of $\mathcal{O}_k$. Suppose A has CM by $\mathcal{O}_K$ for a sextic cyclic CM field K. Let $\wp \subset \mathcal{O}_k$ be a prime lying over a rational prime p. Let m be the number of prime factors of $p\mathcal{O}_K$.

Then the reduction $\overline{A} \coloneqq A \mod \wp$ satisfies $\overline{A} \sim B^d$, where B is absolutely simple and

(i) if $m = 6$, then $d = 1$, the reduced abelian threefold $\overline{A} = B$ is absolutely simple, and $\mathrm{End}^0(\overline{A}) \cong K$.

(ii) if $m = 2$, then $d = 1$, the reduced abelian threefold $\overline{A} = B$ is absolutely simple, and $\mathrm{End}^0(\overline{A})$ is a central simple division algebra of reduced degree 9 over the imaginary quadratic subfield K_1 of K.

(iii) in all other cases, we have $d = 3$, the reduction $\overline{A}$ is supersingular, the endomorphism algebra $\mathrm{End}^0(B)$ is the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and infinity, and $\mathrm{End}^0(\overline{A})$ is the 3×3 matrix algebra over $B_{p,\infty}$.

Lemma 4.24. Let A_1 and A_2 be absolutely simple abelian varieties of dimension g defined over the same number field k such that A_1 and A_2 have good reduction at every prime of $\mathcal{O}_k$. Suppose A_1 is of CM type (K, Φ_1) and A_2 is of CM type (K, Φ_2), where K is an abelian CM field of degree $2g$ and Φ_1 and Φ_2 are equivalent primitive CM types of K.

Let $\wp \subset \mathcal{O}_k$ be a prime ideal and define $\overline{A_1} \coloneqq A_1 \mod \wp$ and $\overline{A_2} \coloneqq A_2 \mod \wp$. Let π_1 and π_2 be the Frobenius endomorphisms of $\overline{A_1}$ and $\overline{A_2}$ respectively. Then

(i) $[\mathbb{Q}(\pi_1) : \mathbb{Q}] = [\mathbb{Q}(\pi_2) : \mathbb{Q}]$,

(ii) if $g = 3$ and K is a cyclic sextic CM field, then $\mathbb{Q}(\pi_1) = \mathbb{Q}(\pi_2)$.

Proof. The CM types Φ_1 and Φ_2 of K are equivalent, so there is an automorphism τ of K such that $\Phi_1 = \Phi_2\tau$. For all CM types Φ of K, it holds that the reflex type of (K, Φ) is (K, Φ^{-1}), because K is abelian. Therefore, it holds that

$$\Phi_1^r = \Phi_1^{-1} = (\Phi_2\tau)^{-1} = \tau^{-1}\Phi_2^{-1} = \tau^{-1}\Phi_2^r.$$

Let $\Phi_2 = \{\sigma_1, \sigma_2, \ldots, \sigma_g\}$ and define $\mathfrak{p} \coloneqq \wp \cap \mathcal{O}_K$. Using Theorem 4.22, it follows that

$$\begin{aligned}
(\pi_1) &= \mathrm{N}_{\Phi_1^r}(\mathrm{N}_{k/K^r}(\wp)) \\
&= \mathrm{N}_{\tau^{-1}\Phi_2^r}(\mathrm{N}_{k/K}(\wp)) \\
&= \mathrm{N}_{\tau^{-1}\Phi_2^{-1}}(\mathfrak{p})^{f(\wp/\mathfrak{p})} \\
&= \left(\mathfrak{p}^{\tau^{-1}\sigma_1^{-1}}\mathfrak{p}^{\tau^{-1}\sigma_2^{-1}}\cdots\mathfrak{p}^{\tau^{-1}\sigma_g^{-1}}\right)^{f(\wp/\mathfrak{p})} \\
&= \left(\left(\mathfrak{p}^{\sigma_1^{-1}}\mathfrak{p}^{\sigma_2^{-1}}\mathfrak{p}^{\sigma_g^{-1}}\right)^{f(\wp/\mathfrak{p})}\right)^{\tau^{-1}} \\
&= \tau^{-1}\left(\mathrm{N}_{\Phi_2^r}(\mathrm{N}_{k/K^r}(\wp))\right) \\
&= (\tau^{-1}\pi_2).
\end{aligned}$$

This implies that $\pi_1\mathcal{O}_K = \tau^{-1}(\pi_2)\mathcal{O}_K$. Let $\gamma \in \mathrm{Gal}(K/\mathbb{Q})$. Then

$$\begin{aligned}(\gamma\pi_1) = (\pi_1) &\iff (\gamma\tau^{-1}\pi_2) = (\tau^{-1}\pi_2)\\ &\iff (\tau^{-1}\gamma\pi_2) = (\tau^{-1}\pi_2)\\ &\iff (\gamma\pi_2) = (\pi_2),\end{aligned}$$

so γ fixes (π_1) if and only if γ fixes (π_2). Therefore, we have $[\mathbb{Q}(\pi_1) : \mathbb{Q}] = [\mathbb{Q}(\pi_2) : \mathbb{Q}]$.

Assume that $g = 3$ and that K is a cyclic sextic CM field. Then $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ with complex conjugation given by σ^3. The degree of $\mathbb{Q}(\pi_1)$ and $\mathbb{Q}(\pi_2)$ over $\mathbb{Q}$ is 1, 2 or 6. If the degree is 1, then $\mathbb{Q}(\pi_1) = \mathbb{Q}(\pi_2) = \mathbb{Q}$. If the degree is 6, then

$$6 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\pi_i)][\mathbb{Q}(\pi_i) : \mathbb{Q}] = [K : \mathbb{Q}(\pi_i)] \cdot 6$$

for $i \in \{1, 2\}$, so $\mathbb{Q}(\pi_1) = \mathbb{Q}(\pi_2) = K$. If $[\mathbb{Q}(\pi_1) : \mathbb{Q}] = [\mathbb{Q}(\pi_2) : \mathbb{Q}] = 2$, then $\mathbb{Q}(\pi_1)$ and $\mathbb{Q}(\pi_2)$ are both imaginary quadratic fields contained in K. The subfield $K^{\langle\sigma^2\rangle}$ of K fixed by 1, σ^2 and σ^4 is the unique imaginary quadratic field subfield of K. Hence, we have $\mathbb{Q}(\pi_1) = \mathbb{Q}(\pi_2) = K^{\langle\sigma^2\rangle}$. □

Proof of Proposition 4.23. Theorem 4.20 implies that $\overline{A} \sim B^d$, where B is absolutely simple. Furthermore, the reduced abelian threefold $\overline{A}$ is isogenous to B^d over $\mathcal{O}_k/\wp$ by Theorem 4.20. Then $f_{\overline{A}} = f_B^d$ by Theorem 2.14, where $f_{\overline{A}}$ and f_B are the characteristic polynomials of the Frobenius endomorpisms $\pi_{\overline{A}}$ and π_B of $\overline{A}$ and B respectively. Therefore, we can assume that $\pi_{\overline{A}} = \pi_B$. The reduction $\overline{A}$ is defined over $\mathbb{F}_q$, where $q = |\mathcal{O}_k/\wp| = p^{f(\wp/p)}$.

The abelian threefold A is absolutely simple, so A is of CM type (K, Φ_A), where Φ_A is primitive by Theorem 4.15. Let $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ and let Φ be the primitive CM type $\{1, \sigma, \sigma^5\}$ satisfying $\Phi = \Phi^r$. Let A'/k be an absolutely simple abelian threefold of CM type (K, Φ) such that A' has good reduction at every prime of $\mathcal{O}_k$ and define $\overline{A'} \coloneqq A' \mod \wp$. Let $\pi_{\overline{A}}$ and π be the Frobenius endomorphisms of $\overline{A}$ and $\overline{A'}$ respectively. Then Lemma 4.24 states that $\mathbb{Q}(\pi_{\overline{A}}) = \mathbb{Q}(\pi)$.

By Theorem 4.22, the Frobenius endomorphism $\pi \in \mathcal{O}_K \subset \mathrm{End}(\overline{A'})$ generates the ideal $\mathrm{N}_{\phi^r}(\mathrm{N}_{k/K^r}(\wp)) = (\pi)$. Since $\Phi = \{1, \sigma, \sigma^5\}$, the reflex CM type of (K, Φ) is Φ itself, see Table 4.2. This implies that $K^r = K$ by Proposition 4.7. Therefore, it holds that

$$(\pi) = \mathrm{N}_\Phi(\mathrm{N}_{k/K}(\wp)) = \mathrm{N}_\Phi(\mathfrak{p}^{f(\wp/\mathfrak{p})}) = \left(\mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^5}\right)^{f(\wp/\mathfrak{p})}, \tag{4.1}$$

where $f(\wp/\mathfrak{p}) = [\mathcal{O}_k/\wp : \mathcal{O}_K/\mathfrak{p}]$, the residual degree of $\wp$ over $\mathfrak{p}$.

Since K is normal, the possible splitting behaviours of p in K are

- $\mathfrak{p}_1$,
- $\mathfrak{p}_1^2$,
- $\mathfrak{p}_1^3$,
- $\mathfrak{p}_1^6$,
- $\mathfrak{p}_1\overline{\mathfrak{p}_1}$,
- $\mathfrak{p}_1^3\overline{\mathfrak{p}_1}^3$,
- $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$,
- $\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$,
- $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}$.

Case (i). Assume $m = 6$. Then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}$. The prime $\mathfrak{p} = \wp \cap \mathcal{O}_K$ is a prime lying above p in K, so $\mathfrak{p} \in \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}, \overline{\mathfrak{p}_3}\}$. Since $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes lying above p in K, it holds that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^2}\mathfrak{p}^{\sigma^3}\mathfrak{p}^{\sigma^4}\mathfrak{p}^{\sigma^5}$. By equation (4.1), we have $(\pi) = \left(\mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^5}\right)^{f(\wp/\mathfrak{p})}$. For all $\tau \in \mathrm{Gal}(K/\mathbb{Q})\backslash\{1\}$, it holds that

$$(\pi)^\tau = \left((\mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^5})^{f(\wp/\mathfrak{p})}\right)^\tau = (\mathfrak{p}^\tau\mathfrak{p}^{\sigma\tau}\mathfrak{p}^{\sigma^5\tau})^{f(\wp/\mathfrak{p})} \neq (\mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^5})^{f(\wp/\mathfrak{p})} = (\pi).$$

Hence, the ideal (π) is fixed only by the identity element of $\mathrm{Gal}(K/\mathbb{Q})$. Therefore, we have $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$. Since $\mathbb{Q}(\pi)$ is a subfield of K and

$$6 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\pi)][\mathbb{Q}(\pi) : \mathbb{Q}] = [K : \mathbb{Q}(\pi)] \cdot 6,$$

it holds that $K = \mathbb{Q}(\pi)$. Hence, we have $\mathbb{Q}(\pi_{\overline{A}}) = \mathbb{Q}(\pi) = K$. By Theorem 2.24, we have

$$\begin{aligned} 6 &= 2\dim \overline{A} = 2d \dim B \\ &= d \cdot [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})]^{\frac{1}{2}}[\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}] \\ &= d \cdot [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})]^{\frac{1}{2}} \cdot 6, \end{aligned}$$

so $d = [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})] = 1$. Hence, $\overline{A}$ is simple and $\mathrm{End}^0_{\mathbb{F}_q}(\overline{A}) \cong \mathrm{End}^0_{\mathbb{F}_q}(B) \cong K$.

Let r be an arbitrary positive integer and consider $\overline{A}/\mathbb{F}_{q^r}$. The Frobenius endomorphism of $\overline{A}/\mathbb{F}_{q^r}$ is $\pi^r_{\overline{A}}$. Since $(\pi_{\overline{A}})$ is fixed only by the identity element of $\mathrm{Gal}(K/\mathbb{Q})$, also $(\pi^r_{\overline{A}})$ is fixed only by the identity element of $\mathrm{Gal}(K/\mathbb{Q})$. Therefore, we have $[\mathbb{Q}(\pi^r_{\overline{A}}) : \mathbb{Q}] = 6$ and $\mathbb{Q}(\pi^r_{\overline{A}}) = \mathbb{Q}(\pi_{\overline{A}})$. Thus, it holds that $\mathbb{Q}(\pi^r_{\overline{A}}) = \mathbb{Q}(\pi_{\overline{A}})$ for all integers $r > 0$ and $\overline{A}$ is absolutely simple by Proposition 2.29. Hence, it holds that $d = 1$, the reduced abelian threefold $\overline{A} = B$ is absolutely simple and $\mathrm{End}^0(\overline{A}) = \mathrm{End}^0_{\mathbb{F}_q}(\overline{A}) \cong K$.

Case (ii). Assume $m = 2$. Then $p\mathcal{O}_K = \mathfrak{p}_1^a\overline{\mathfrak{p}_1}^a$, where $a \in \{1, 3\}$. The prime $\mathfrak{p} = \wp \cap \mathcal{O}_K$ is a prime lying above p in K, so $\mathfrak{p} \in \{\mathfrak{p}_1, \overline{\mathfrak{p}}_1\}$. Therefore, we have $p\mathcal{O}_K = \mathfrak{p}^a\overline{\mathfrak{p}}^a = \left(\mathfrak{p}\mathfrak{p}^{\sigma^3}\right)^a$. Since the rational prime p is invariant under σ, it holds that

$$\left(\mathfrak{p}\mathfrak{p}^{\sigma^3}\right)^a = p\mathcal{O}_K = (p\mathcal{O}_K)^\sigma = \left(\left(\mathfrak{p}\mathfrak{p}^{\sigma^3}\right)^a\right)^\sigma = \left(\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^4}\right)^a.$$

Thus, we have $\mathfrak{p}^\sigma \in \{\mathfrak{p}, \mathfrak{p}^{\sigma^3}\}$. If $\mathfrak{p}^\sigma = \mathfrak{p}$, then

$$\mathfrak{p}^{\sigma^i} = (\mathfrak{p}^\sigma)^{\sigma^{i-1}} = \mathfrak{p}^{\sigma^{i-1}} = \cdots = \mathfrak{p}$$

for every $i \in \{2,3,4,5\}$. In particular, we would have $\mathfrak{p}^{\sigma^3} = \mathfrak{p}$. But this is not true, since $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^{\sigma^3}$ and $\mathfrak{p} \neq \mathfrak{p}^{\sigma^3}$. Hence, it holds that $\mathfrak{p}^{\sigma} = \mathfrak{p}^{\sigma^3}$. Then

$$\begin{aligned}\mathfrak{p}^{\sigma} &= \mathfrak{p}^{\sigma^3},\\ \mathfrak{p}^{\sigma^2} &= \mathfrak{p}^{\sigma^4},\\ \mathfrak{p}^{\sigma^3} &= \mathfrak{p}^{\sigma^5},\\ \mathfrak{p}^{\sigma^4} &= \mathfrak{p},\end{aligned}$$

so $\mathfrak{p} = \mathfrak{p}^{\sigma^2} = \mathfrak{p}^{\sigma^4}$ and $\mathfrak{p}^{\sigma} = \mathfrak{p}^{\sigma^3} = \mathfrak{p}^{\sigma^5}$. By equation (4.1), we have

$$(\pi) = \left(\mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^5}\right)^{f(\wp/\mathfrak{p})} = \left(\mathfrak{p}(\mathfrak{p}^2)^{\sigma^3}\right)^{f(\wp/\mathfrak{p})}.$$

The automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$ satisfying

$$(\pi)^{\tau} = \left((\mathfrak{p}(\mathfrak{p}^2)^{\sigma^3})^{f(\wp/\mathfrak{p})}\right)^{\tau} = \left(\mathfrak{p}^{\tau}(\mathfrak{p}^2)^{\sigma^3\tau}\right)^{f(\wp/\mathfrak{p})} = \left(\mathfrak{p}(\mathfrak{p}^2)^{\sigma^3}\right)^{f(\wp/\mathfrak{p})} = (\pi)$$

are $1, \sigma^2$ and σ^4. This follows from the fact that $\mathfrak{p} = \mathfrak{p}^{\sigma^2} = \mathfrak{p}^{\sigma^4}$ and $\mathfrak{p}^{\sigma} = \mathfrak{p}^{\sigma^3} = \mathfrak{p}^{\sigma^5}$. Therefore, it holds that $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2$. Hence, we have $[\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}] = [\mathbb{Q}(\pi) : \mathbb{Q}] = 2$. By Theorem 2.24, we have

$$\begin{aligned}6 &= 2\dim \overline{A} = 2d \dim B\\ &= d \cdot [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})]^{\frac{1}{2}} [\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}]\\ &= d \cdot [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})]^{\frac{1}{2}} \cdot 2,\end{aligned}$$

so $d \cdot [\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})]^{\frac{1}{2}} = 3$. We thus have the following two options: either $d = 3$ and $[\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})] = 1$, or $d = 1$ and $[\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})] = 9$.

Since $p\mathcal{O}_K = \mathfrak{p}^a\overline{\mathfrak{p}}^a$, where $a \in \{1,3\}$, we have

$$(q) = (\pi_{\overline{A}}\overline{\pi_{\overline{A}}}) = (\pi_{\overline{A}})(\overline{\pi_{\overline{A}}}) = \left(\mathfrak{p}\overline{\mathfrak{p}}^2\right)^{f(\wp/\mathfrak{p})}\left(\overline{\mathfrak{p}}\mathfrak{p}^2\right)^{f(\wp/\mathfrak{p})} = (\mathfrak{p}\overline{\mathfrak{p}})^{3f(\wp/\mathfrak{p})} = \begin{cases}(p)^{3f(\wp/\mathfrak{p})} & \text{if } a = 1,\\ (p)^{f(\wp/\mathfrak{p})} & \text{if } a = 3,\end{cases}$$

so $q = p^n$ with $n = \begin{cases}3f(\wp/\mathfrak{p}) & \text{if } a = 1,\\ f(\wp/\mathfrak{p}) & \text{if } a = 3.\end{cases}$

Since $p\mathcal{O}_K = \mathfrak{p}^a\overline{\mathfrak{p}}^a$ and $\mathbb{Q}(\pi_{\overline{A}})$ is an imaginary quadratic field, we have $p\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})} = \mathfrak{P}\overline{\mathfrak{P}}$ with $f(\mathfrak{P}) = f(\overline{\mathfrak{P}}) = 1$. Thus, we have $\mathfrak{P}\mathcal{O}_K = \mathfrak{p}^a$ and $\overline{\mathfrak{P}}\mathcal{O}_K = \overline{\mathfrak{p}}^a$. There exist integers $b, c > 0$ such that $\pi_{\overline{A}}\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})} = \mathfrak{P}^b\overline{\mathfrak{P}}^c$. Then

$$\begin{aligned}\left(\mathfrak{p}\mathfrak{p}^2\right)^{f(\wp/\mathfrak{p})} &= \pi_{\overline{A}}\mathcal{O}_K = \left(\pi_{\overline{A}}\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})}\right)\mathcal{O}_K\\ &= \left(\mathfrak{P}^b\overline{\mathfrak{P}}^c\right)\mathcal{O}_K = \left(\mathfrak{P}\mathcal{O}_K\right)^b\left(\overline{\mathfrak{P}}\mathcal{O}_K\right)^c\\ &= \left(\mathfrak{p}^a\right)^b\left(\overline{\mathfrak{p}}^a\right)^c = \mathfrak{p}^{ab}\overline{\mathfrak{p}}^{ac},\end{aligned}$$

so $ab = f(\wp/\mathfrak{p})$ and $ac = 2f(\wp/\mathfrak{p})$. Hence, we have $b = \frac{f(\wp/\mathfrak{p})}{a}$ and $c = \frac{2f(\wp/\mathfrak{p})}{a}$ and $\pi_{\overline{A}}\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})} = \mathfrak{P}^{\frac{f(\wp/\mathfrak{p})}{a}}\overline{\mathfrak{P}}^{\frac{2f(\wp/\mathfrak{p})}{a}}$. Therefore, it holds that

$$i_{\mathfrak{P}} = f(\mathfrak{P}) \cdot \frac{\mathrm{ord}_{\mathfrak{P}}(\pi_{\overline{A}})}{n} = \left\{ \begin{array}{ll} \frac{f(\wp/\mathfrak{p})}{3f(\wp/\mathfrak{p})} & \text{if } a = 1 \\ \frac{f(\wp/\mathfrak{p})/3}{f(\wp/\mathfrak{p})} & \text{if } a = 3 \end{array} \right\} = \frac{1}{3},$$

$$i_{\overline{\mathfrak{P}}} = f(\overline{\mathfrak{P}}) \cdot \frac{\mathrm{ord}_{\overline{\mathfrak{P}}}(\pi_{\overline{A}})}{n} = \left\{ \begin{array}{ll} \frac{2f(\wp/\mathfrak{p})}{3f(\wp/\mathfrak{p})} & \text{if } a = 1 \\ \frac{2f(\wp/\mathfrak{p})/3}{f(\wp/\mathfrak{p})} & \text{if } a = 3 \end{array} \right\} = \frac{2}{3}.$$

The least common denominator of the invariants is three. Then Theorem 2.25 implies that the characteristic polynomial of the Frobenius endomorphism of the simple abelian variety corresponding to $\pi_{\overline{A}}$, see Theorem 2.20, is of the form h^3, where h is the minimal polynomial of $\pi_{\overline{A}}$. Note that h is a second degree polynomial, since $[\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}] = 2$. It follows that $\overline{A}$ is a simple abelian threefold with $f_{\overline{A}} = h^3$. Hence, it holds that $d = 1$ and $[\mathrm{End}^0_{\mathbb{F}_q}(B) : \mathbb{Q}(\pi_{\overline{A}})] = 9$, so $\mathrm{End}^0_{\mathbb{F}_q}(\overline{A}) \cong \mathrm{End}^0_{\mathbb{F}_q}(B)$ is a central simple division algebra of reduced degree 9 over the imaginary quadratic subfield $\mathbb{Q}(\pi_{\overline{A}})$ of K.

Let r be an arbitrary positive integer and consider $\overline{A}/\mathbb{F}_{q^r}$. The Frobenius endomorphism of $\overline{A}/\mathbb{F}_{q^r}$ is $\pi^r_{\overline{A}}$. Since $(\pi_{\overline{A}})$ is fixed only by the automorphisms $1, \sigma^2$ and σ^4 in $\mathrm{Gal}(K/\mathbb{Q})$, also $(\pi^r_{\overline{A}})$ is fixed only by $1, \sigma^2$ and σ^4. Therefore, it holds that $[\mathbb{Q}(\pi^r_{\overline{A}}) : \mathbb{Q}] = 2$ and $\mathbb{Q}(\pi^r_{\overline{A}}) = \mathbb{Q}(\pi_{\overline{A}})$. Thus, we have $\mathbb{Q}(\pi^r_{\overline{A}}) = \mathbb{Q}(\pi_{\overline{A}})$ for all integers $r > 0$ and $\overline{A}$ is absolutely simple by Proposition 2.29. Hence, it holds that $d = 1$, the reduced abelian threefold $\overline{A} = B$ is absolutely simple and $\mathrm{End}^0(\overline{A}) = \mathrm{End}^0_{\mathbb{F}_q}(\overline{A})$ is a central simple division algebra of reduced degree 9 over the imaginary quadratic field $\mathbb{Q}(\pi_{\overline{A}})$.

Case (iii). If m is not 2 or 6, then m is either 1 or 3. First assume $m = 1$. Then $p\mathcal{O}_K = \mathfrak{p}_1^a$, where $a \in \{1, 2, 3, 6\}$. The prime $\mathfrak{p} = \wp \cap \mathcal{O}_K$ is a prime lying above p in K, so $\mathfrak{p} = \mathfrak{p}_1$. By equation (4.1), we have

$$(\pi) = \left(\mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^5}\right)^{f(\wp/\mathfrak{p})} = \left(\mathfrak{p}^3\right)^{f(\wp/\mathfrak{p})}.$$

Hence, the ideal (π) is fixed by all automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$. Therefore, it holds that $[\mathbb{Q}(\pi) : \mathbb{Q}] = [\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}] = 1$.

If $m = 3$, then $p\mathcal{O}_K = \mathfrak{p}_1^a\mathfrak{p}_2^a\mathfrak{p}_3^a$, where $a \in \{1, 2\}$. The prime $\mathfrak{p}$ is one of $\mathfrak{p}_1$, $\mathfrak{p}_2$ or $\mathfrak{p}_3$. Since $\mathfrak{p}_i$ is its own conjugate for all $i \in \{1, 2, 3\}$, it holds that $\mathfrak{p} = \mathfrak{p}^{\sigma^3}$, $\mathfrak{p}^{\sigma} = \mathfrak{p}^{\sigma^4}$ and $\mathfrak{p}^{\sigma^2} = \mathfrak{p}^{\sigma^5}$ and $p\mathcal{O}_K = \left(\mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^2}\right)^a$. By equation (4.1), we have

$$(\pi) = \left(\mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^5}\right)^{f(\wp/\mathfrak{p})} = \left(\mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^2}\right)^{f(\wp/\mathfrak{p})}.$$

Since $\mathfrak{p} = \mathfrak{p}^{\sigma^3}$, $\mathfrak{p}^{\sigma} = \mathfrak{p}^{\sigma^4}$ and $\mathfrak{p}^{\sigma^2} = \mathfrak{p}^{\sigma^5}$, it follows that (π) is fixed by all automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$. Therefore, we have $[\mathbb{Q}(\pi) : \mathbb{Q}] = [\mathbb{Q}(\pi_{\overline{A}}) : \mathbb{Q}] = 1$.

Hence, if m is not 2 or 6, then the Frobenius endomorphism $\pi_{\overline{A}}$ of $\overline{A}$ is rational. Then Theorem 2.15 implies that $\overline{A}$ is $\mathbb{F}_q$-isogenous to B^3, where B is a supersingular elliptic curve, so $\overline{A}$ is supersingular. It follows that $\mathrm{End}^0_{\mathbb{F}_q}(B) = \mathrm{End}^0(B)$ is the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞ and $\mathrm{End}^0_{\mathbb{F}_q}(\overline{A}) = \mathrm{End}^0(\overline{A})$ is the 3×3 matrix algebra over $B_{p,\infty}$. □

The next corollary is about the ranks of the reduced CM abelian threefolds as given in (i), (ii) and (iii) of Proposition 4.23.

Corollary 4.25. Let A/k, K, $\wp$ and m be as in Proposition 4.23 and let $\overline{A} \coloneqq A \mod \wp$. If $m = 6$, then $r(\overline{A}) = 3$. In all other cases, we have $r(\overline{A}) = 0$.

Proof. Let $\mathfrak{p} \coloneqq \wp \cap \mathcal{O}_K$ and $q = |\mathcal{O}_k/\wp|$. For each case in Proposition 4.23, we will determine the rank of $\overline{A}$.

Case (i). Assume $m = 6$. Then p splits completely in K, so $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}$. Moreover, the reduced abelian threefold $\overline{A}$ is an absolutely simple abelian threefold over $\mathbb{F}_q$ with $\mathrm{End}^0(\overline{A}) \cong K = \mathbb{Q}(\pi_{\overline{A}})$ by Proposition 4.23(i). Hence, we can apply the results in Table 3.2. The splitting of $p\mathcal{O}_K$ corresponds to case (XVIII) of Table 3.2 and we see that $r(\overline{A}) = 3$.

Case (ii). Assume $m = 2$. Then $p\mathcal{O}_K = \left(\mathfrak{p}\mathfrak{p}^{\sigma^3}\right)^a$, where $a \in \{1, 3\}$. Since A is absolutely simple, A is of CM type (K, Φ) with Φ primitive by Theorem 4.15. The CM field K is cyclic, so $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Let $\Phi = \{\sigma^k, \sigma^l, \sigma^m\}$, with $k, l, m \in \{0, 1, 2, 3, 4, 5\}$. The CM type Φ is primitive, so Φ is not equal to $\{1, \sigma^2, \sigma^4\}$ or $\{\sigma, \sigma^3, \sigma^5\}$. Moreover, the reflex CM type of (K, Φ) is (K, Φ^{-1}), see Section 4.1.1. By Theorem 4.22, we have

$$(\pi_{\overline{A}}) = \mathrm{N}_{\Phi^r}(\mathrm{N}_{k/K^r}(\wp)) = \mathrm{N}_{\Phi^{-1}}(\mathrm{N}_{k/K}(\wp)) = \left(\mathfrak{p}^{\sigma^{-k}}\mathfrak{p}^{\sigma^{-l}}\mathfrak{p}^{\sigma^{-m}}\right)^{f(\wp/\mathfrak{p})}. \tag{4.2}$$

Following the proof of Proposition 4.23, we see that $\mathfrak{p} = \mathfrak{p}^{\sigma^2} = \mathfrak{p}^{\sigma^4}$ and $\mathfrak{p}^\sigma = \mathfrak{p}^{\sigma^3} = \mathfrak{p}^{\sigma^5}$. This implies that $(\pi_{\overline{A}}) = (\mathfrak{p}\overline{\mathfrak{p}}^2)^{f(\wp/\mathfrak{p})}$ or $(\pi_{\overline{A}}) = (\mathfrak{p}^2\overline{\mathfrak{p}})^{f(\wp/\mathfrak{p})}$. By the proof of Proposition 4.23, we have $p\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})} = \mathfrak{P}\overline{\mathfrak{P}}$ and

$$\pi_{\overline{A}}\mathcal{O}_{\mathbb{Q}(\pi_{\overline{A}})} = \begin{cases} \mathfrak{P}^{\frac{f(\wp/\mathfrak{p})}{a}}\overline{\mathfrak{P}}^{\frac{2f(\wp/\mathfrak{p})}{a}} & \text{if } \pi_{\overline{A}}\mathcal{O}_K = (\mathfrak{p}\overline{\mathfrak{p}}^2)^{f(\wp/\mathfrak{p})}, \\ \mathfrak{P}^{\frac{2f(\wp/\mathfrak{p})}{a}}\overline{\mathfrak{P}}^{\frac{f(\wp/\mathfrak{p})}{a}} & \text{if } \pi_{\overline{A}}\mathcal{O}_K = (\mathfrak{p}^2\overline{\mathfrak{p}})^{f(\wp/\mathfrak{p})}. \end{cases}$$

Thus, both primes $\mathfrak{P}$ and $\overline{\mathfrak{P}}$ that lie above p in $\mathbb{Q}(\pi_{\overline{A}})$ contain $\pi_{\overline{A}}$. Hence, it holds that $r(\overline{A}) = 0$ by Theorem 3.13.

Case (iii). Assume m is not 2 or 6. Then $\overline{A}$ is supersingular by Proposition 4.23, so $r(\overline{A}) = 0$. □

We will now look at an example of the endomorphism algebra and p-rank of different reductions of an absolutely simple CM abelian threefold A with CM by $\mathcal{O}_K$, where K is a sextic CM field of which the Galois group of the normal closure is isomorphic to D_6.

Example 4.26. Let $K_+ = \mathbb{Q}[x]/(x^3-6x-2)$ and $K = K_+(\sqrt{-3})$. The field K_+ is totally real and K is a totally imaginary quadratic extension of K_+, so K is a CM field. Let K' be the Galois closure of K. We have $\mathrm{Gal}(K'/\mathbb{Q}) \cong D_6 = \langle x, y : x^2 = y^6 = xyxy = 1\rangle$, the dihedral group with 12 elements. The automorphism y^3 represents complex conjugation. We have $K = K'^{\langle x\rangle}$ and $K_+ = K'^{\langle x, y^3\rangle}$. This example of a sextic CM field of which the Galois group of the normal closure is isomorphic to D_6 is taken from the PhD thesis of Kılıçer [11, Table 3.3].

Let A be an absolutely simple abelian threefold over a number field k such that A has good reduction at every prime ideal of k. Assume that A has CM by $\mathcal{O}_K$ and is of type $\Phi = \{1, y|_K, y^5|_K\}$. The CM type Φ is primitive and satisfies $\Phi = \Phi^r$, so also $K^r = K$, see Section 4.1.2. We will look at the reduction of A at prime ideals $\wp$ of $\mathcal{O}_k$ lying over small rational primes and compute the endomorphism algebra and p-rank of $\overline{A} = A \mod \wp$. For this, we will use the factorization of (p) into prime ideals in the fields K and K'. Table 4.5 gives the factorization of $p\mathcal{O}_K$ and $p\mathcal{O}_{K'}$ into prime ideals for the rational primes $p < 20$.

p	$p\mathcal{O}_K$	$p\mathcal{O}_{K'}$
2	$\mathfrak{p}^3$	$\mathscr{P}^3\mathscr{P}_x^3$
3	$\mathfrak{p}^6$	$\mathscr{P}^6$
5	$5\mathcal{O}_K$	$\mathscr{P}\mathscr{P}_x$
7	$\mathfrak{p}_1^2\overline{\mathfrak{p}_1}^2\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$\mathscr{P}_1^2\mathscr{P}_{1,x}^2\overline{\mathscr{P}}_1^2\overline{\mathscr{P}}_{1,x}^2\mathscr{P}_2^2\overline{\mathscr{P}}_2^2$
11	$\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$\mathscr{P}_1\mathscr{P}_{1,x}\mathscr{P}_2\mathscr{P}_{2,x}\overline{\mathscr{P}}_2\overline{\mathscr{P}}_{2,x}$
13	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$\mathscr{P}_1\overline{\mathscr{P}}_1\mathscr{P}_2\mathscr{P}_{2,x}\overline{\mathscr{P}}_2\overline{\mathscr{P}}_{2,x}$
17	$17\mathcal{O}_K$	$\mathscr{P}\mathscr{P}_x$
19	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$\mathscr{P}_1\overline{\mathscr{P}}_1\mathscr{P}_2\mathscr{P}_{2,x}\overline{\mathscr{P}}_2\overline{\mathscr{P}}_{2,x}$

Table 4.5: The prime factorizations of $p\mathcal{O}_K$ and $p\mathcal{O}_{K'}$ for the rational primes $p < 20$ computed in SAGE.

Let $\wp \subset \mathcal{O}_k$ be a prime ideal lying above a rational prime p and let $\overline{A} \coloneqq A \mod \wp$. Define $\mathfrak{p} \coloneqq \wp \cap \mathcal{O}_K$. Denote by π the Frobenius endomorphism of $\overline{A}$. For every rational prime $p < 20$, we will determine the endomorphism algebra and p-rank of $\overline{A}$.

For $p \in \{2, 3, 5, 17\}$, there is only one prime ideal $\mathfrak{p}$ lying above p in K, so $p\mathcal{O}_K = \mathfrak{p}^a$ for

some positive integer a. By Proposition 4.22, we have

$$\begin{aligned}\pi\mathcal{O}_{K'} &= \mathrm{N}_{\Phi^r}(\mathrm{N}_{k/K^r}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathrm{N}_{k/K}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathfrak{p}^{f(\wp/\mathfrak{p})})\mathcal{O}_{K'} = (\mathrm{N}_{\Phi}(\mathfrak{p})\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})} \\ &= \left((\mathfrak{p}\mathcal{O}_{K'})(\mathfrak{p}\mathcal{O}_{K'})^{y}(\mathfrak{p}\mathcal{O}_{K'})^{y^5}\right)^{f(\wp/\mathfrak{p})} = (\mathfrak{p}^3\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})},\end{aligned}$$

so $(\pi) = \mathfrak{p}^{3f(\wp/\mathfrak{p})}$ in K. Since $p \in \mathbb{Q}$ is invariant under all automorphisms in $\mathrm{Gal}(K'/\mathbb{Q})$, we have

$$\mathfrak{p}^a = p\mathcal{O}_K = (p\mathcal{O}_K)^\tau = (\mathfrak{p}^a)^\tau = (\mathfrak{p}^\tau)^a,$$

for all $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$. Therefore, the prime ideal $\mathfrak{p}$ is invariant under all automorphisms in $\mathrm{Gal}(K'/\mathbb{Q})$. It follows that also (π) is invariant under all automorphisms in $\mathrm{Gal}(K'/\mathbb{Q})$ and hence $\mathbb{Q}(\pi) = \mathbb{Q}$. Thus, the reduction $\overline{A}$ is supersingular and $\mathrm{End}^0(\overline{A})$ is the 3×3 matrix algebra over $B_{p,\infty}$. The p-rank of $\overline{A}$ is 0.

For $p = 7$, we find $7\mathcal{O}_K = \mathfrak{p}_1^2\overline{\mathfrak{p}_1}^2\mathfrak{p}_2\overline{\mathfrak{p}_2}$ and $7\mathcal{O}_{K'} = \mathscr{P}_1^2\mathscr{P}_{1,x}^2\overline{\mathscr{P}}_1^2\overline{\mathscr{P}}_{1,x}^2\mathscr{P}_2^2\overline{\mathscr{P}}_2^2$. Let $D_{\mathscr{P}_1}$ be the decomposition group of $\mathscr{P}_1$. We have

$$|D_{\mathscr{P}_1}| = ef = 2.$$

The elements of order 2 in $\mathrm{Gal}(K'/\mathbb{Q})$ are $x, y^3, xy, xy^2, xy^3, xy^4$ and xy^5, so

$$D_{\mathscr{P}_1} \in \{\langle x\rangle, \langle y^3\rangle, \langle xy\rangle, \langle xy^2\rangle, \langle xy^3\rangle, \langle xy^4\rangle, \langle xy^5\rangle\}.$$

The ideal $\mathfrak{P}_1 = \mathscr{P}_1 \cap \mathcal{O}_{K_+}$ is unramified in K and K', so $D_{\mathscr{P}_1} \cap \mathrm{Gal}(K'/K_+) = \{1\}$. Since $\mathrm{Gal}(K'/K_+) = \{1, x, y^3, xy^3\}$, it holds that $D_{\mathscr{P}_1} \notin \{\langle x\rangle, \langle y^3\rangle, \langle xy^3\rangle\}$. We can split the remaining possible groups for $D_{\mathscr{P}_1}$ into conjugates

$$\begin{aligned}C(\langle xy\rangle) &= \{\langle xy\rangle, \langle xy^3\rangle, \langle xy^5\rangle\} \\ C(\langle xy^2\rangle) &= \{\langle x\rangle, \langle xy^2\rangle, \langle xy^4\rangle\}.\end{aligned}$$

Suppose $D_{\mathscr{P}_1} = \langle xy\rangle$. In the group $\langle x\rangle\backslash\mathrm{Gal}(L/\mathbb{Q})/\langle xy\rangle$, we have

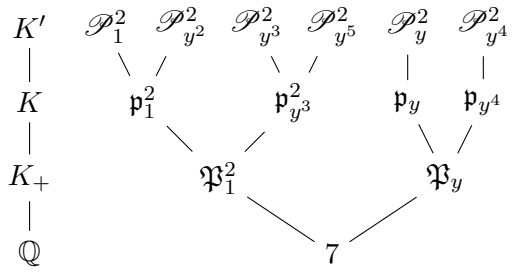
$$\langle x\rangle 1\langle xy\rangle = \langle x\rangle y\langle xy\rangle, \qquad \langle x\rangle y^2\langle xy\rangle = \langle x\rangle y^5\langle xy\rangle, \qquad \langle x\rangle y^3\langle xy\rangle = \langle x\rangle y^4\langle xy\rangle.$$

This implies that there are three prime ideals lying above $p = 7$ in K. This is a contradiction. Hence, we have $D_{\mathscr{P}_1} \neq \langle xy\rangle$. Similarly, it holds that $D_{\mathscr{P}_1} \notin C(\langle xy\rangle)$.

Without loss of generality, we can assume that $D_{\mathscr{P}_1} = \langle xy^2\rangle$. In $\langle x\rangle\backslash\mathrm{Gal}(K'/\mathbb{Q})/\langle xy^2\rangle$, we have

$$\langle x\rangle 1\langle xy\rangle = \langle x\rangle y^2\langle xy\rangle, \qquad \langle x\rangle y^3\langle xy\rangle = \langle x\rangle y^5\langle xy\rangle, \qquad \langle x\rangle y\langle xy\rangle, \qquad \langle x\rangle y^4\langle xy\rangle.$$

This leads to the following splitting diagram.



We have $\mathfrak{p} = \wp \cap \mathcal{O}_K \in \{\mathfrak{p}_1, \mathfrak{p}_{y^3}, \mathfrak{p}_y, \mathfrak{p}_{y^4}\}$. Taking $\mathfrak{p} = \mathfrak{p}_1$ or $\mathfrak{p} = \mathfrak{p}_{y^3}$ leads to the same results for the endomorphism algebra and the p-rank. The same holds for taking $\mathfrak{p} = \mathfrak{p}_y$ or $\mathfrak{p} = \mathfrak{p}_{y^4}$. We will therefore only consider $\mathfrak{p} \in \{\mathfrak{p}_1, \mathfrak{p}_y\}$.

Let $\mathfrak{p} = \mathfrak{p}_1$. By Proposition 4.22, we have

$$\begin{aligned}\pi\mathcal{O}_{K'} &= \mathrm{N}_{\Phi^r}(\mathrm{N}_{k/K^r}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathrm{N}_{k/K}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathfrak{p}_1^{f(\wp/\mathfrak{p})})\mathcal{O}_{K'} \\ &= (\mathrm{N}_{\Phi}(\mathfrak{p}_1)\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})} = \left((\mathfrak{p}_1\mathcal{O}_{K'})(\mathfrak{p}_1\mathcal{O}_{K'})^{y}(\mathfrak{p}_1\mathcal{O}_{K'})^{y^5}\right)^{f(\wp/\mathfrak{p})} \\ &= (\mathscr{P}_1\mathscr{P}_{y^2}\mathscr{P}_y\mathscr{P}_{y^3}\mathscr{P}_{y^5}\mathscr{P}_y)^{f(\wp/\mathfrak{p})} = (\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^3}\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})},\end{aligned}$$

so $(\pi) = (\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^3})^{f(\wp/\mathfrak{p})}$ in K. Then the p-rank of $\overline{A}$ is 1 by Theorem 3.13. Moreover, the ideal (π) is fixed only by the automorphisms $1, x \in \mathrm{Gal}(K'/\mathbb{Q})$, so $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$. Hence, it holds that $\mathbb{Q}(\pi) = K$ and $\mathrm{End}^0(\overline{A}) \cong K$.

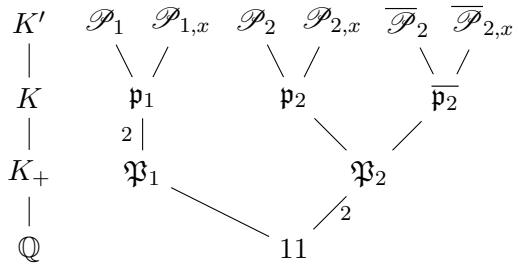
Next, assume $\mathfrak{p} = \mathfrak{p}_y$. By Proposition 4.22, we have

$$\begin{aligned}\pi\mathcal{O}_{K'} &= \mathrm{N}_{\Phi^r}(\mathrm{N}_{k/K^r}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathrm{N}_{k/K}(\wp))\mathcal{O}_{K'} = \mathrm{N}_{\Phi}(\mathfrak{p}_y^{f(\wp/\mathfrak{p})})\mathcal{O}_{K'} \\ &= (\mathrm{N}_{\Phi}(\mathfrak{p}_y)\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})} = \left((\mathfrak{p}_y\mathcal{O}_{K'})(\mathfrak{p}_y\mathcal{O}_{K'})^{y}(\mathfrak{p}_y\mathcal{O}_{K'})^{y^5}\right)^{f(\wp/\mathfrak{p})} \\ &= (\mathscr{P}_y^2\mathscr{P}_{y^2}^2\mathscr{P}_1^2)^{f(\wp/\mathfrak{p})} = (\mathfrak{p}_1^2\mathfrak{p}_y\mathcal{O}_{K'})^{f(\wp/\mathfrak{p})},\end{aligned}$$

so $(\pi) = (\mathfrak{p}_1^2\mathfrak{p}_y)^{f(\wp/\mathfrak{p})}$ in K. Then the p-rank of $\overline{A}$ is 3 by Theorem 3.13. Moreover, (π) is fixed only by the automorphisms $1, x \in \mathrm{Gal}(K'/\mathbb{Q})$, so $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$. Hence, it holds that $\mathbb{Q}(\pi) = K$ and $\mathrm{End}^0(\overline{A}) \cong K$.

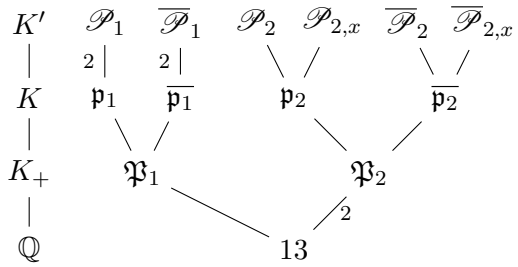
For the remaining primes $p < 20$, we use SAGE to determine the endomorphism algebra and p-rank. Using the RECIP-code of Streng, we compute $\mathrm{N}_{\Phi^r}(\mathfrak{p})$ for the prime ideals $\mathfrak{p}$ lying above p. This results in the prime factorization of $\pi\mathcal{O}_K$. The p-rank of $\overline{A}$ can be deduced from the factorizations of $p\mathcal{O}_K$ and $\pi\mathcal{O}_K$ by Theorem 3.13. Furthermore, we compute in SAGE the degree of the minimal polynomial of π. This determines the endomorphism algebra of $\overline{A}$.

For $p = 11$, we find the following splitting diagram, see Table 4.5.



If $\mathfrak{p} = \mathfrak{p}_2$ or $\mathfrak{p} = \overline{\mathfrak{p}_2}$, then $(\pi) = (\mathfrak{p}_1\mathfrak{p}_2^2)^{f(\wp/\mathfrak{p})}$ and we find $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$, so $\mathrm{End}^0(\overline{A}) \cong K$. This implies that $\overline{A}$ is absolutely simple. We can therefore apply the results in Table 3.2. The splitting of $p\mathcal{O}_K$ corresponds to case (IV) and we see that $r(\overline{A}) = 2$. If $\mathfrak{p} = \mathfrak{p}_1$, then $(\pi) = (11\mathcal{O}_K)^{f(\wp/\mathfrak{p})}$ and we find $[\mathbb{Q}(\pi) : \mathbb{Q}] = 1$, so $\overline{A}$ is supersingular and $\mathrm{End}^0(\overline{A})$ is the 3×3 matrix algebra over $B_{p,\infty}$. Then the p-rank of $\overline{A}$ is 0.

For $p = 13$, we find the following splitting diagram, see Table 4.5.



If $\mathfrak{p} = \mathfrak{p}_1$ of $\mathfrak{p} = \overline{\mathfrak{p}_1}$, then $(\pi) = (\mathfrak{p}_1\mathfrak{p}_2)^{f(\wp/\mathfrak{p})}$ and we find $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$, so $\mathrm{End}^0(\overline{A}) \cong K$. This implies that $\overline{A}$ is absolutely simple. We can therefore apply the results in Table 3.2. The splitting of $p\mathcal{O}_K$ corresponds to case (VII) and we see that $r(\overline{A}) = 3$. If $\mathfrak{p} = \mathfrak{p}_2$ or $\mathfrak{p} = \overline{\mathfrak{p}_2}$, then $(\pi) = (\mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2})^{f(\wp/\mathfrak{p})}$. In this case, it also holds that $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$, so $\mathrm{End}^0(\overline{A}) \cong K$ and $\overline{A}$ is absolutely simple. We can read off from Table 3.2 case (VII) that $r(\overline{A}) = 1$.

The results for $p = 19$ are the same as for $p = 13$.

p	$p\mathcal{O}_K$	$\pi\mathcal{O}_K$		$r(\overline{A})$	$\mathrm{End}^0(\overline{A})$
2	$\mathfrak{p}^3$	$\mathfrak{p}^3$		0	$M_3(B_{p,\infty})$
3	$\mathfrak{p}^6$	$\mathfrak{p}^6$		0	$M_3(B_{p,\infty})$
5	$\mathfrak{p}$	$\mathfrak{p}$		0	$M_3(B_{p,\infty})$
7	$\mathfrak{p}_1^2\overline{\mathfrak{p}_1}^2\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$(\mathfrak{p}_1\overline{\mathfrak{p}_1\mathfrak{p}_2})^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_1$ or $\mathfrak{p}=\overline{\mathfrak{p}_1}$	1	K
		$(\mathfrak{p}_1^2\mathfrak{p}_2)^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_2$ or $\mathfrak{p}=\overline{\mathfrak{p}_1}$	3	K
11	$\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$(\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_2})^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_1$	0	$M_3(B_{p,\infty})$
		$(\mathfrak{p}_1\mathfrak{p}_2^2)^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_2$ or $\mathfrak{p}=\overline{\mathfrak{p}_2}$	2	K
13	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$(\mathfrak{p}_1\mathfrak{p}_2)^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_1$ or $\mathfrak{p}=\overline{\mathfrak{p}_1}$	3	K
		$(\mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2})^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_2$ or $\mathfrak{p}=\overline{\mathfrak{p}_2}$	1	K
17	$\mathfrak{p}$	$\mathfrak{p}$		0	$M_3(B_{p,\infty})$
19	$\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$	$(\mathfrak{p}_1\mathfrak{p}_2)^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_1$ or $\mathfrak{p}=\overline{\mathfrak{p}_1}$	3	K
		$(\mathfrak{p}_1^2\mathfrak{p}_2\overline{\mathfrak{p}_2})^{f(\wp/\mathfrak{p})}$	if $\mathfrak{p}=\mathfrak{p}_2$ or $\mathfrak{p}=\overline{\mathfrak{p}_2}$	1	K

Table 4.6: The factorizations of $\pi\mathcal{O}_K$ deduced from the splitting behaviour of rational primes $p < 20$ in K and the corresponding p-rank and endomorphism algebra of the reduction $\overline{A}$.

Remark 4.27. Let A be an absolutely simple CM abelian threefold over a number field k such that A has good reduction at every prime of $\mathcal{O}_k$. Suppose A is of CM type (K,Φ) and has CM by $\mathcal{O}_K$, where K is a sextic CM field of which the Galois group of the normal closure K' is isomorphic to D_6. Let $\wp \subset \mathcal{O}_k$ be a prime lying over a rational prime p. In the above example, it is illustrated how the endomorphism algebra and p-rank of the reduction $\overline{A} = A \mod \wp$ can be determined from the factorization of $p\mathcal{O}_K$ into prime ideals. By listing the possible factorizations of $p\mathcal{O}_K$ and determining the endomorphism algebra and p-rank of $\overline{A}$, we obtain analogues of Proposition 4.23 and Corollary 4.25 for an absolutely simple abelian threefold with CM by $\mathcal{O}_K$ for a sextic CM field K with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_6$. Note that the primitive CM types of the sextic CM field K with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_6$ are not all equivalent, see Section 4.1.2. Therefore, in order to obtain analogues of Theorem 4.23 and Corollary 4.25, it is important to state the CM type Φ of K such that A is of CM type (K,Φ).

Bibliography

[1] I. Bouw, J. Cooley, K. Lauter, E. L. Garcia, M. Manes, R. Newton, and E. Ozman. Bad reduction of genus 3 curves with complex multiplication. *arXiv: 1407.3589*, 2014.

[2] J. Bradford. *Commutative Endomorphism Rings of Simple Abelian Varieties over Finite Fields*. PhD thesis, University of Maryland, 2012.

[3] C.-L. Chai, B. Conrad, and F. Oort. *Complex Multiplication and Lifting Problems*, volume 195 of Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2014.

[4] D. A. Cox. *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Incorporated, 2nd edition, 2013.

[5] B. Dodson. The Structure of Galois Groups of CM-Fields. *Transactions of the American Mathematical Society*, 283(1):1–32, 1984.

[6] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley & Sons, Incorporated, Hoboken, NJ, 3rd edition, 2004.

[7] J. González. On the p-rank of an abelian variety and its endomorphism algebra. *Publicacions Matemàtiques*, 42(1):119–130, 1998.

[8] S. Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *arXiv: 1003.0374*, 2010.

[9] E. W. Howe and H. J. Zhu. On the Existence of Absolutely Simple Abelian Varieties of a Given Dimension over an Arbitrary Field. *Journal of Number Theory*, 92:139–163, 2002.

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

[11] P. Kılıçer. *The CM class number one problem for curves*. PhD thesis, Universiteit Leiden and University of Bordeaux, 2016.

[12] P. Kılıçer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arithmetica*, 185(2):127–156, 2018.

[13] S. Lang. *Complex Multiplication*, volume 255 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1983.

[14] J. Milne. *Abelian Varieties*. Available at www.jmilne.org/math/, v2.0 edition, 2008.

[15] E. Nart and D. Maisner. Abelian Surfaces over Finite Fields as Jacobians. *Experiment. Math.*, 11:321–336, n° 3, 2002.

[16] J.-P. Serre and J. Tate. Good Reduction of Abelian Varieties. *Annals of Mathematics*, 88(3):492–517, 1968.

[17] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*, volume 46 of Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998.

[18] G. Shimura and Y. Taniyama. *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, volume 6 of Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, Tokyo, 1961.

[19] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2$^{\text{nd}}$ edition, 2016.

[20] J. Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones mathematicae*, 2:134–144, April 1966.

[21] J. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini. *Séminaire N. Bourbaki*, 1968/69:95–110, exp. n° 352, 1971.

[22] W. Waterhouse and J. Milne. Abelian varieties over finite fields. *Proc. Sympos. pure math.*, XX:53–64, 1969 Number Theory Institute (Stony Brook), AMS 1971.

[23] C. Xing. The characteristic polynomials of abelian varieties of dimension three and four over finite fields. *Science in China*, 37:147–150, no 3 1994.

[24] A. Zaytsev. Generalization of Deuring Reduction Theorem. *arXiv: 1209.5207*, 2012.

Acknowledgements

I wish to show my gratitude to my first supervisor Pınar Kılıçer, not only for her guidance and her help with the difficulties we came across, but also for being her open self, which made me feel comfortable to ask any question that came to mind. I would also like to thank my second supervisor Jaap Top for giving feedback in the final stage. I am grateful to my parents for always being interested in my progress, and my brother for making me laugh when my motivation was at a low. Finally, I would like to thank the members of the Thesis Tea Club, Anouk, Bas and Manoy, for making it feel like we were still classmates, although we had to stay at home, writing our thesis together and discussing our progress, motivation and loads of other things.