Computing abelian varieties over finite fields isogenous to a power

Stefano Marseglia

Abstract

In this paper we give a module-theoretic description of the isomorphism classes of abelian varieties $A$ isogenous to $B^r$, where the characteristic polynomial $g$ of Frobenius of $B$ is an ordinary square-free $q$-Weil polynomial, for a power $q$ of a prime $p$, or a square-free $p$-Weil polynomial with no real roots. Under some extra assumptions on the polynomial $g$ we give an explicit description of all the isomorphism classes which can be computed in terms of fractional ideals of an order in a finite product of number fields. In the ordinary case, we also give a module-theoretic description of the polarizations of $A$.

1 Introduction

It is well known that abelian varieties of dimension $g$ over the complex numbers can be functorially described by full lattices $L \subset \mathbb{C}^g$ and that such a description becomes an equivalence of categories when we only consider the lattices $L$ such that the associated torus $\mathbb{C}^g / L$ admits a Riemann form. When we move to the wilder realm of positive characteristic we cannot have such a functorial description due to the existence of objects like supersingular elliptic curves whose endomorphisms form a quaternionic algebra which does not admit a 2-dimensional representation, as pointed out by Serre. Nevertheless, when we are working over a finite field $\mathbb{F}_q$, with $q$ a power of a prime $p$, we have analogous descriptions if we restrict ourselves to some subcategories of the category of abelian varieties over finite fields. More precisely, Deligne proved in [Del69] that there is an equivalence between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category of finitely generated free $\mathbb{Z}$-modules with an endomorphism satisfying some easy-to-state axioms. This description has been extended by Centeleghe and Stix in [CS15] for abelian varieties over the prime field $\mathbb{F}_p$ whose characteristic polynomial of Frobenius does not have real roots. In the ordinary case, Howe has extended this equivalence to include the notions of dual variety and polarizations, see [How95].

In [Mar18b] we have used such descriptions to produce algorithms to compute the isomorphism classes of abelian varieties with square-free characteristic polynomial of Frobenius and, when applicable, the polarizations and the corresponding automorphism groups. The algorithms make use of the fact that the
target category of Deligne’s and Centeleghe-Stix functors is equivalent to a category of fractional ideals of a certain order in the étale algebra \( \mathbb{Q}[x]/(h) \), where \( h \) is the characteristic polynomial.

In the present paper we extend such a description to the case when the characteristic polynomial \( h \) is a power of a square-free polynomial, say \( h = g^r \). Instead of fractional ideals we will have to consider lattices in \( K' \) with an \( R \)-modules structure, where \( K = \mathbb{Q}[x]/(g) \) and \( R = \mathbb{Z}[x, y]/(g(x), xy - q) \). In the ordinary case we translate the notion of a polarization to this context.

When the order \( R \) is Bass there is a classification of such modules, see [Bas63] and [LW85], and we can explicitly compute representatives of the isomorphism classes of the abelian varieties.

There are other categorical descriptions, which we do not make use of, of the category of abelian varieties isogenous to a power of elliptic curves, see the Appendix in [Lau02], [Kan11] and [JKP + 17].

The paper is structured as follows. In Section 2 we recall the notion of an order and a fractional ideal, with a focus on Bass orders. In Section 3 we describe the categorical equivalences that we are going to use in Section 4, where we focus on the case of abelian varieties with characteristic polynomial of the form \( h = g^r \), with \( g \) square-free. In Section 5 we translate the notion of a polarization into our module-theoretic language. Finally, in Section 6 we apply our description and present the results of some computations.

Acknowledgments

The author would like to thank Jonas Bergström for helpful discussions and Rachel Newton and Christophe Ritzenthaler for comments on a previous version of the paper, which is part of the author’s Ph.D thesis [Mar18a].

Conventions

All rings considered are commutative and unital. All morphisms between abelian varieties \( A \) and \( B \) over a field \( k \) are also defined over \( k \), unless otherwise specified. In particular, we write \( \text{Hom}(A, B) \) for \( \text{Hom}_k(A, B) \). Also, an abelian variety \( A \) is simple if it is so over the field of definition.

2 Orders

Let \( g \) be an integral square-free monic polynomial, say of degree \( n \). Let \( K \) be the étale \( \mathbb{Q} \)-algebra \( \mathbb{Q}[x]/(g) \). Note that \( K \) is a finite product of distinct number fields. An order \( R \) in \( K \) is a subring of \( K \) whose additive group is isomorphic to \( \mathbb{Z}^n \). Among all orders in \( K \) there exists a maximal one with respect to inclusion, which is called the maximal order of \( K \) and is denoted \( \mathcal{O}_K \). An over-order of \( R \) is an order \( S \) in \( K \) containing \( R \). Since the quotient \( \mathcal{O}_K/R \) is finite there are only
finitely many over-orders of $R$. A fractional ideal of $R$ is a finitely generated sub-$R$-module of $K$ containing a non-zero-divisor. Given two fractional $R$-ideals $I$ and $J$, we have that $I + J$, $I \cap J$, $IJ$, $(I : J)$ and $I^t$ are also fractional $R$-ideals. Recall that the quotient ideal $(I : J)$ and the trace dual ideal $I^t$ are defined respectively as

$$(I : J) = \{ x \in K : xJ \subseteq I \}$$

and

$$I^t = \{ x \in K : \text{Tr}_{K/Q}(xI) \subseteq \mathbb{Z} \}.$$ 

Observe that the underlying additive subgroup of any fractional ideal $I$ is a free abelian group of rank $n$, that is $I$ is a lattice in $K$. Recall, that if $I = \alpha_1 \mathbb{Z} \oplus \ldots \oplus \alpha_n \mathbb{Z}$ then $I^t = \alpha_1^* \mathbb{Z} \oplus \ldots \oplus \alpha_n^* \mathbb{Z}$, where $\{\alpha_i^*\}$ is the dual basis characterized by the relations $\text{Tr}_{K/Q}(\alpha_i^* \alpha_j) = 1$ if $i = j$ and 0 otherwise.

Given any full lattice $I$ in $K$ the set $(I : I)$ is an order. If $I$ is fractional $R$-ideal then $(I : I)$ will contain $R$. This order is called the multiplicator ring of $I$. A fractional ideal $I$ is called invertible if $I/(S : I) = S$, where $S$ is the multiplicator ring of $I$.

An order $S$ is called Gorenstein if every fractional ideal with multiplicator ring $S$ is invertible, or equivalently if $S^t$ is an invertible ideal, see [BL94, Proposition 2.7]. Examples of Gorenstein orders are $\mathcal{O}_K$ and the monogenic order $R = \mathbb{Z}[x]/(f)$, see [BL94, Example 2.8]. An order $R$ is called Bass if every over-order of $R$ is Gorenstein. Since in this paper we will extensively use the properties of Bass orders we will list here other equivalent definitions.

**Proposition 2.1.** Let $R$ be an order. The following are equivalent:

- $R$ is Bass (every over-order is Gorenstein);
- every fractional $R$-ideal can be generated by 2 elements;
- $R$ is a cyclic index order, that is the finite $R$-module $\mathcal{O}_K/R$ is cyclic.

The study of such orders started with the paper [Bas63] on Gorenstein rings. There are many sources where one can find a proof of Proposition 2.1 (and other characterizations), for example [LW85, Theorem 2.1]. Since every fractional ideal of a quadratic order can be generated by 2 elements as an abelian group, they are examples of Bass orders.

Given an order $R$ we define the ideal class monoid as

$$\text{ICM}(R) = \text{fractional } R\text{-ideals}/\sim$$

and the ideal class group as

$$\text{Pic}(R) = \text{invertible fractional } R\text{-ideals}/\sim.$$
where the operations are induced by ideal multiplication. We will denote the class of the ideal $I$ by $[I]$. Note that $\text{ICM}(R) \cong \text{Pic}(R)$ with equality if and only if $R = \mathcal{O}_K$. In general we have that

$$\text{ICM}(R) \cong \bigcup_S \text{Pic}(S),$$

where the disjoint union is taken over the over-orders of $R$, with equality if and only if $R$ is Bass. In particular, if this is the case, once we have a complete list of over-orders of $R$, it is easy to compute all the ideal classes of $R$, using the results from [KP05]. For more about the computation of $\text{ICM}(R)$, even in the non-Bass case, we refer to [Mar18c].

Recall that an $R$-module $M$ is torsion-free if the canonical map $M \to M \otimes R K$ is injective.

**Definition 2.2.** Let $R$ be an order in $K$ and let $\mathcal{B}(r)$ be the category of torsion-free $R$-modules $M$ such that $M \otimes K$ is a free $K$-module of rank $r$ together with $R$-linear morphisms.

Crucial for our purpose is the fact that, when $R$ is a Bass order, the modules in $\mathcal{B}(r)$ can be written in a canonical form in terms of over-orders of $R$ and fractional ideals.

**Theorem 2.3.** Let $R$ be a Bass order and let $M$ be in $\mathcal{B}(r)$. Then there are fractional $R$-ideals $I_1, \ldots, I_r$ with $(I_1 : I_1) \subseteq \ldots \subseteq (I_r : I_r)$ such that

$$M \cong I_1 \oplus \ldots \oplus I_r.$$

The isomorphism class of $M$ is uniquely determined by the chain of over-orders $(I_1 : I_1)$ and the isomorphism class $[I_1 \cdots I_r]$.

This result was first proved in [Bas62, Theorem 1.7] and then proved with a different method in [BF65, Theorem 8]. It was generalized to Bass rings in [LW85, Theorem 7.1]. As an immediate consequence of Theorem 2.3 we get that $M$ can be written in a canonical form

$$M = S_1 \oplus \ldots \oplus S_{r-1} \oplus I,$$

with $S_1 \subseteq \ldots \subseteq S_{r-1} \subseteq S_r = (I : I)$ and this chain of over-orders of $R$ together with $[I]$ uniquely determines $M$ up to isomorphism. In particular, if we know all the over-orders of $R$ and their Picard groups we can easily compute representatives for all the isomorphism classes of modules in $\mathcal{B}(r)$, for every $r$.

**Proposition 2.4.** Let $M = I_1 \oplus \ldots \oplus I_r$ and $N = J_1 \oplus \ldots \oplus J_s$. Then

$$\text{Hom}_R(M, N) = \{ A \in \mathcal{M}_{s \times 1}(K) : A_{j,i} \in (J_j : I_i) \}.$$

**Proof.** The statement follows from the fact that $\text{Hom}_R(I_1, J_1) = (J_1 : I_1)$ since every $R$-linear morphism $\varphi : I_1 \to J_1$ is a multiplication by $a \in K$, where $a$ is the image of $1_K$ under the induced $K$-linear endomorphism $\varphi \otimes Q$ of $K$. \qed
In particular, for \( M = S_1 \oplus \ldots \oplus S_{r-1} \oplus I \) as above we have

\[
\text{End}_R(M) = \begin{pmatrix}
S_1 & S_2 & \ldots & S_{r-1} & I \\
(S_1 : S_2) & S_2 & \ldots & S_{r-1} & I \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
(S_1 : S_{r-1}) & (S_2 : S_{r-1}) & \ldots & S_{r-1} & I \\
(S_1 : I) & (S_2 : I) & \ldots & (S_{r-1} : I) & (I : I)
\end{pmatrix}
\]

and

\[
\text{Aut}_R(M) = \{ A \in \text{End}_R(M) \cap \text{GL}_r(K) : A^{-1} \in \text{End}_R(M) \}.
\]

If \( R \) is a Bass order and \( M \) and \( N \) are two modules in \( \mathscr{B}(r) \), it is easy using Theorem 2.3 to check whether they are isomorphic. If this is the case, it is possible to explicitly construct a matrix \( A_0 \) realizing the isomorphism, as the next example shows.

**Example 2.5** ([BF65, Lemma 8]). Let \( I_1 \) and \( I_2 \) be fractional \( R \)-ideals with multiplicator rings \( S_1 \) and \( S_2 \), respectively, with \( S_1 \subseteq S_2 \). Then by the classification given in Theorem 2.3 we have an \( R \)-linear isomorphism

\[
I_1 \oplus I_2 \cong S_1 \oplus (I_1 I_2).
\]

We want to exhibit a matrix \( A_0 \) realizing the isomorphism. Since \( I_1 \) is invertible in \( S_1 \), there are elements \( c_1 \) and \( c_2 \) in \( K \) such that \( c_1 I_1 + c_2 I_2 = S_1 \). So we can assume that \( I_1 \) and \( I_2 \) are coprime in \( S_1 \). Thus there are \( a_1 \in I_1 \) and \( a_2 \in I_2 \) such that \( 1 = a_1 + a_2 \). Then it is easy to check that the matrix

\[
A_0 = \begin{pmatrix}
1 & -1 \\
a_2 & a_1
\end{pmatrix}
\]

satisfies \( A_0(I_1 \oplus I_2) = S_1 \oplus I_1 I_2 \) (where the action is on column vectors).

## 3 The category of abelian varieties over a finite field

Let \( q \) be a power of a prime number \( p \) and let \( \text{AV}(q) \) be the category of abelian varieties defined over \( \mathbb{F}_q \). For \( A \in \text{AV}(q) \) consider the induced action of the Frobenius endomorphism on the \( l \)-adic Tate modules \( T_l A \), for any prime \( l \neq p \), and let \( h_A \) be the corresponding characteristic polynomial. Then \( h_A \) is a \( q \)-Weil polynomial, that is a monic polynomial in \( \mathbb{Z}[x] \) of even degree with roots of complex absolute value \( \sqrt{q} \). In particular \( h_A \) has degree \( 2 \dim(A) \) and uniquely determines the isogeny class of \( A \), in the sense that an abelian variety \( B \) is isogenous to \( A \) if and only if \( h_A = h_B \).

By the Poincaré Decomposition Theorem we know \( A \) is isogenous to a product

\[
A \sim B_{r_1}^{e_1} \times \ldots \times B_{r_r}^{e_r},
\]
where $e_i$ are positive integers and the $B_i$'s are simple pairwise non-isogenous abelian varieties. It follows that

$$h_A = h_{B_1}^{e_1} \cdots h_{B_r}^{e_r}.$$ 

Recall that for a simple abelian variety $B$ in $AV(q)$ the polynomial $h_B$ is a power of an irreducible polynomial, say $m^a$, and the exponent $a$ is uniquely determined by the $p$-adic factorization of $m$, see [WM71 Theorem 8].

Using this recipe, we can list all characteristic polynomials $h$ of the Frobenius of abelian varieties over a finite field $\mathbb{F}_q$ of a given dimension $g$, for example see [Hal10] for $g = 3$ and [HS12] for $g = 4$. By Honda-Tate theory, see [Tat66] and [Hon68], this corresponds to describing all isogeny classes of abelian varieties in $AV(q)$ of a given dimension $g$. For such a polynomial $h$, denote by $AV(h)$ the full subcategory of $AV(q)$ whose objects are the abelian varieties in the isogeny class determined by $h$.

We will restrict our attention to two subcategories of $AV(q)$. Recall that an abelian variety $A$ over $\mathbb{F}_q$ is called ordinary if exactly half of the roots of $h_A$ over $\mathbb{Q}_p$ are $p$-adic units. There are many other characterizations of ordinary abelian varieties. For example see [Del69 Section 2]. We will denote the full subcategory of $AV(q)$ consisting of ordinary abelian varieties by $AV^{\text{ord}}(q)$. We will also consider the subcategory $AV^{\text{cs}}(p)$ of abelian varieties $A$ over the prime field $\mathbb{F}_p$ such that $h_A$ has no real roots, that is $h_A(\sqrt{p}) \neq 0$. We will give functorial descriptions of $AV^{\text{ord}}(q)$ and $AV^{\text{cs}}(p)$ in terms of $\mathbb{Z}$-lattices with extra structure. More precisely, consider the following categories:

- the category $\mathcal{M}^{\text{ord}}(q)$ consisting of pairs $(T,F)$ where $T$ is a free-finitely generated $\mathbb{Z}$-module and $F$ is a $\mathbb{Z}$-linear endomorphism of $T$ such that
  - the action of $F \otimes \mathbb{Q}$ on $T \otimes \mathbb{Q}$ is semisimple;
  - the eigenvalues of $F \otimes \mathbb{Q}$ have complex absolute value $\sqrt{q}$;
  - half of the roots of the characteristic polynomial of $F \otimes \mathbb{Q}$ over $\overline{\mathbb{Q}}_p$ are units;
  - there exists an endomorphism $V$ of $T$ such that $FV = q$;

- the category $\mathcal{M}^{\text{cs}}(p)$ consisting of pairs $(T,F)$ where $T$ is a free-finitely generated $\mathbb{Z}$-module and $F$ is a $\mathbb{Z}$-linear endomorphism of $T$ such that
  - the action of $F \otimes \mathbb{Q}$ on $T \otimes \mathbb{Q}$ is semisimple;
  - the eigenvalues of $F \otimes \mathbb{Q}$ have complex absolute value $\sqrt{p}$;
  - the characteristic polynomial of $F \otimes \mathbb{Q}$ has no real roots;
  - there exists an endomorphism $V$ of $T$ such that $FV = p$. 


In both categories, a morphism \((T, F) \to (T', F')\) is a \(\mathbb{Z}\)-linear morphism \(\varphi : T \to T'\) inducing a commutative diagram

\[
\begin{array}{ccc}
T & \xrightarrow{\varphi} & T' \\
F \downarrow & & \downarrow F' \\
T & \xrightarrow{\varphi} & T'
\end{array}
\]

The main tools to understand the categories \(AV^{\text{ord}}(q)\) and \(AV^{\text{cs}}(p)\) are given in the following theorem.

**Theorem 3.1.** There is an equivalence of categories

\[\mathcal{F}^{\text{ord}} : AV^{\text{ord}}(q) \to \mathcal{M}^{\text{ord}}(q)\]

and an anti-equivalence of categories

\[\mathcal{F}^{\text{cs}} : AV^{\text{cs}}(p) \to \mathcal{M}^{\text{cs}}(p).\]

If \(A \to (T, F)\), then \(\text{rank}_\mathbb{Z} T = 2 \dim A\) and the endomorphism \(F\) corresponds to the Frobenius endomorphism of \(A\).

**Proof.** For the ordinary case over \(\mathbb{F}_q\) see [Del69, Section 7]. For the case with no-real roots over \(\mathbb{F}_p\) see [CS15, Theorem 1].

\[\Box\]

4 **Abelian varieties isogenous to a power**

Let \(h\) be a characteristic polynomial of an abelian variety in \(AV^{\text{ord}}(q)\) or \(AV^{\text{cs}}(p)\). Assume moreover that \(h = g^r\) for some square-free polynomial \(g\) in \(\mathbb{Z}[x]\). Put \(K = \mathbb{Q}[x]/(g)\) and \(\alpha = x \mod (g)\). Denote with \(R\) the order \(\mathbb{Z}[\alpha, q/\alpha]\) in \(K\) (with \(q = p\) if we are in \(AV^{\text{cs}}(p)\)). Observe that the order \(R\) is Gorenstein, see [CS15, Theorem 11].

**Theorem 4.1.** (a) If \(AV(h) \subset AV^{\text{ord}}(q)\) then there is an equivalence of categories \(\mathcal{F} : AV(h) \to \mathcal{B}(r).\) If \(AV(h) \subset AV^{\text{cs}}(p)\) then there is an anti-equivalence of categories \(\mathcal{F} : AV(h) \to \mathcal{B}(r).\)

(b) If \(R\) is a Bass order, \(\mathcal{F}\) induces a bijection between

\[AV(h)/\sim\]

and the set of pairs

\[(S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r, [I]),\]

where each \(S_i\) is an over-order of \(R\) and \([I]\) denotes the isomorphism class of a fractional \(S_r\)-ideal \(I\).
Proof. Denote by $\mathcal{M}(h)$ the image of $AV(h)$ via $\mathcal{F}^{\text{ord}}$ (or $\mathcal{F}^{\text{cs}}$). We will define an equivalence $\mathcal{G}: \mathcal{M}(h) \to B(r)$. Take $A$ in $AV(h)$ and let $(T, F)$ be the image of $A$ in $\mathcal{M}(h)$ via $\mathcal{F}^{\text{ord}}$ (or $\mathcal{F}^{\text{cs}}$). The minimal polynomial of the $\mathbb{Q}$-linear endomorphism $F \otimes \mathbb{Q}$ of $T \otimes \mathbb{Q}$ is $g$. So by definition of $\mathcal{M}^{\text{ord}}(q)$ (or $\mathcal{M}^{\text{cs}}(p)$) we have that $F$ and $V$ induce on $T$ an $R$-module structure via the isomorphism $R \simeq \mathbb{Z}[F, V]$ given by $\alpha \mapsto \text{char}$. Denote this $R$-module by $M$ and put $G((T, F)) = M$. Observe that the action of $F$ on $T$ is faithful, since it becomes multiplication by $q$ (or by $p$) after composing with $V$, and hence $M$ is torsion free. Let’s prove that $M \otimes_R K$ is a free $K$-module of rank $r$. Since $g$ is square-free, it is a product of distinct irreducible polynomials, say $g = g_1 \cdots g_s$. In particular, $K$ is isomorphic to the product of number fields $\prod_i K_i$, where $K_i = \mathbb{Q}[x]/(g_i)$. Let $e_i$ be the image in $K$ of the multiplicative unit of $K_i$ under this isomorphism, so that $1_K = e_1 + \ldots + e_s$ and $K e_i \simeq K_i$ for each $i$. Hence

$$M \otimes_R K = M \otimes_R \left( \bigoplus_{i=1}^s Ke_i \right) \simeq \bigoplus_{i=1}^s (M \otimes_R Ke_i).$$

Since the action of $F \otimes \mathbb{Q}$ is semisimple, there is a direct sum decomposition $T \otimes_\mathbb{Q} \mathbb{Q} = W_1 \oplus \ldots \oplus W_s$ such that the action of $F \otimes \mathbb{Q}$ on each $W_i$ is simple. This means that, after renumbering, we can assume that the minimal polynomial of $F \otimes \mathbb{Q}|_{W_i}$ is $g_i$ and that

$$\dim_\mathbb{Q} W_i = r \deg(g_i).$$

Since $\deg(g_i) = \dim_\mathbb{Q} Ke_i$ it follows that $\dim_{K e_i} (M \otimes_R Ke_i) = r$ and hence, by taking the direct sum over $i$, we obtain an isomorphism

$$M \otimes_R K \simeq K^r.$$

Therefore $M$ is in $B(r)$. It is clear by construction that $\mathcal{G}$ is a fully faithful and essentially surjective functor. Define $\mathcal{F}$ as the composition of the equivalences $\mathcal{F}^{\text{ord}}$ (or $\mathcal{F}^{\text{cs}}$) and $\mathcal{G}$. In particular $\mathcal{F}$ is an equivalence as well and we have concluded the proof of part (a). Part (b) now follows directly from Theorem 2.3.

**Corollary 4.2.** Assume that $R$ is a Bass order. Then every abelian variety $A$ in $AV(h)$ is isomorphic to

$$B_1 \times \ldots \times B_r,$$

for some abelian varieties $B_i$ in $AV(g)$.

**Proof.** Put $M = \mathcal{F}(A)$ by Theorem 4.1. By Theorem 2.3 we have that there are fractional ideals $I_1, \ldots, I_r$ such that

$$M \simeq I_1 \oplus \ldots \oplus I_r.$$

Again by Theorem 4.1 we get that there are abelian varieties $B_i$ in $AV(g)$ such that $B_i = \mathcal{F}(I_i)$ for each $i = 1, \ldots, r$. 

8
Remark 4.3. In Corollary 4.2, the abelian varieties $B_i$ are simple if and only if $g$ is irreducible. This follows from [How95, Theorem 3.3] for the ordinary case over $\mathbb{F}_q$ and from [WM71, Theorem 8] for characteristic polynomial over $\mathbb{F}_p$ with no real roots.

Corollary 4.4. Let $A$ be in $AV(h^r)$. If $r > 1$ then $\text{End}(A)$ is not commutative.

Proof. It follows from the fact that $\text{End}(A) \otimes \mathbb{Q} = M_{r \times r}(K)$. \hfill \square

Remark 4.5. Note that Theorem 4.1 is a generalization of [Mar18b, Theorem 4.3], where we deal with the case when $h$ is square-free, that is $r = 1$.

Remark 4.6. Theorem 2.3 tells us that if $R$ is a Bass order, then every torsion-free $R$-module of finite rank is isomorphic to a direct sum of fractional $R$-ideals. The reverse implication does not hold. In [Bas63], the author describes when it fails, but overlooks some cases. The gaps were filled in [NR67] and in [Hae90] in the local case and in [HL88] it is described how to go from the local case to the global case. We have not analyzed if those exceptions could arise from orders generated by Weil polynomials, which could potentially extend our description to more isogeny classes.

5 Polarizations

In this section we will continue using the same notation as in Section 4, but we will restrict to the case when $h$ is ordinary. Our goal is to describe what the polarizations of an abelian variety $A$ in $AV(h)$ correspond to in the category $B(r)$ via the equivalence $F$ of Theorem 4.1(b).

Note that $K$ is a CM-algebra, that is, there is an involution $a \mapsto \bar{a}$ that acts as complex conjugation after composing with any non-zero homomorphism $\varphi : K \to \mathbb{C}$. In particular, we have that $\bar{a} = q/a$. Observe that the homomorphisms $K \to \mathbb{C}$ come in conjugate pairs. We call a choice of half of these homomorphisms, one for each conjugate pair, a CM-type of $K$. For every $R$-module $M$ in $B(r)$, since we can identify $M$ with a submodule of $K^r$, we see that the trace $\text{Tr}_{K/Q} : K \to \mathbb{Q}$ induces a non-degenerate bilinear form $\text{Tr}$ on $M$ by

$$\text{Tr} : M \times M \to \mathbb{Q}, \quad ((x_i)_{i=1}^r, (y_j)_{j=1}^r) \mapsto \sum_{i=1}^r \text{Tr}_{K/Q}(x_i y_i),$$

where we think of all vectors in $K^r$ as columns vectors. In analogy to the $r = 1$ case, when $M$ is a fractional $R$-ideal, we define the trace dual $M^t$ of $M$ to be the dual module with respect to $\text{Tr}$. In particular, if $n = \deg(h)$ and we fix a $\mathbb{Z}$-basis

$$M = \alpha_1 \mathbb{Z} \oplus \ldots \oplus \alpha_n \mathbb{Z}, \quad \text{with } \alpha_j \in K$$

then we can write

$$M^t = \alpha_1^* \mathbb{Z} \oplus \ldots \oplus \alpha_n^* \mathbb{Z},$$
where \( \alpha_i^* \) is the dual basis characterized by \( \text{Tr}_{K/Q}(\alpha_i \alpha_j^*) = 1 \) if \( i = j \) and 0 otherwise.

**Proposition 5.1.** Let \( A \) be an abelian variety in \( \text{AV}(h) \) and put \( M = \mathcal{F}(A) \). If \( A^\vee \) is the dual abelian variety of \( A \), then \( \mathcal{F}(A^\vee) = M^\vee \), where \( M^\vee = \overline{M} \). In particular, if \( M = I_1 \oplus \ldots \oplus I_r \), then \( M^\vee = \overline{I}_1 \oplus \ldots \oplus \overline{I}_r \).

**Proof.** Let \( \mathcal{G} \) be the functor defined in the proof of Theorem 4.1. Put \( (T, F) = \mathcal{F}(A) \), so that \( \mathcal{G}((T, F)) = M \). Following [How95], Proposition 4.5, we have that \( \mathcal{F}(A^\vee) = (T^\vee, F^\vee) \), where \( T^\vee = \text{Hom}_\mathbb{Z}(T, \mathbb{Z}) \). Let \( F^\vee(\psi) = \psi \circ V \) for every \( \psi \in T^\vee \). To conclude, we need to show that \( \mathcal{G}(T^\vee, F^\vee) = M^\vee \). It is clear that \( \mathcal{G} \) sends \( T^\vee \) to \( \text{Hom}_\mathbb{Z}(M, \mathbb{Z}) \) (as abelian groups). Since the action of \( F^\vee \) on \( T^\vee \) is “pre-composition with \( V \)” and \( \overline{V} = F \), we see that it will correspond, via \( \mathcal{G} \), to the multiplication by \( \alpha \) after taking the complex conjugate. More precisely, write \( M = \alpha_1 \mathbb{Z} \oplus \ldots \oplus \alpha_n \mathbb{Z} \), for \( \alpha_j \in K \), with \( n = [K : \mathbb{Q}] \), and consider the \( \mathbb{Z} \)-linear isomorphism

\[
\text{Hom}_\mathbb{Z}(M, \mathbb{Z}) \rightarrow \mathbb{M}^\vee
\]

\[
\psi \mapsto \sum_{i=1}^{n} \psi(\alpha_i) \overline{\alpha}_i^*
\]

with inverse

\[
\text{Tr}(\overline{x}^T, -) \mapsto x
\]

where \( \overline{x}^T \) is the transpose of \( \overline{x} \). Using this identification the pre-composition with \( \overline{\alpha} \) on \( \text{Hom}_\mathbb{Z}(M, \mathbb{Z}) \) will correspond to multiplication by \( \alpha \) on \( \overline{M}^\vee \).

**Corollary 5.2.** Let \( \mu : A \rightarrow B \) be a morphism of abelian varieties in \( \text{AV}(h) \). Put \( \mathcal{F}(\mu) = \Lambda \in \text{Hom}_\mathbb{R}(M, N) \) in \( \mathcal{B}(r) \). Then \( \mu \) is an isogeny if and only if \( \det \Lambda \in K^* \). Moreover, the dual morphism \( \mu^\vee : B^\vee \rightarrow A^\vee \) corresponds via \( \mathcal{F} \) to the morphism \( \Lambda^\vee = \overline{\Lambda}^T \in \text{Hom}_\mathbb{R}(N^\vee, M^\vee) \), where \( \overline{\Lambda}^T \) is the transpose of \( \overline{\Lambda} \).

**Proof.** Put \( (T, F) = \mathcal{F}(A) \), \( (T', F') = \mathcal{F}(B) \) and \( \mathcal{F}(\mu) = (T, F) \rightarrow (T', F') \). Then \( \mu \) is an isogeny if and only if the induced morphism \( \Lambda \circ \mathcal{G} \) is invertible. Let \( \mathcal{G} \) be the functor defined in the proof of Theorem 4.1. Observe that \( \mathcal{G}(\Lambda) = \Lambda \) and hence \( \Lambda \circ \mathcal{G} \) is invertible if and only if the matrix \( \Lambda \) is invertible over \( K \).

Put \( \mathcal{F}(\mu^\vee) = \Lambda^\vee \) where \( (T^\vee, F^\vee) \rightarrow (T', F') \) is defined by \( \Lambda^\vee(\psi) = \psi \circ \Lambda \) for every \( \psi \in T^\vee \). Using Proposition 5.1 we see that, if \( \mathcal{G}(\Lambda) = \Lambda \) then \( \mathcal{G}(\Lambda^\vee) = \overline{\Lambda}^T \).

In order to describe the polarizations we need a particular kind of CM-type which, roughly speaking, detects the complex structure “coming from characteristic \( p \)” on a pair \( (T, F) \) in \( \mathcal{F}^\text{ord}(q) \). More precisely, put

\[
\Phi = \{ \varphi \in \text{Hom}(K, \mathbb{C}) : \nu_p(\varphi(\alpha)) > 0 \}
\]
where $v_p$ is the $p$-adic valuation induced by a fixed isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$. In [Mar18b] we give an algorithm to compute such a $\Phi$. Recall that an element $a$ in $K$ is called totally imaginary if $\overline{a} = -a$. For such an $a$, we say that it is $\Phi$-non-positive if $\operatorname{Im}(\varphi(a)) \leq 0$ for every $\varphi$ in $\Phi$.

Observe that in $\mathcal{M}^\text{ord}(q)$, an isogeny $\lambda : (T, F) \to (T^\vee, F^\vee)$ induces a bilinear form

$$b : T \times T \to \mathbb{Z}, \quad b(s, t) = \lambda(t)(s).$$

Then there exists a unique bilinear form $S$ on $T \otimes \mathbb{Q}$ such that $b = \operatorname{Tr}_{K/\mathbb{Q}} \circ S$ and, using [How95, Proposition 4.9], we have that $\mu$ is a polarization if and only if the associated $S$ is skew-Hermitian and for every $a$ in $K$ the element $S(a, a)$ is $\Phi$-non-positive.

**Theorem 5.3.** Let $A$ be an abelian variety in $\mathcal{A}(h)$ and let $\mu : A \to A^\vee$ be an isogeny. Put $\mathcal{F}(\mu) = \Lambda : M \to M^\vee$. Then $\mu$ is a polarization if and only if

- $\Lambda = -\Lambda^T$ and,
- for every column vector $a$ in $K$, the element $a^T \Lambda a$ is $\Phi$-non-positive.

**Proof.** Put $\mathcal{F}^\text{ord}(A) = (T, F)$. Using the functor $\mathcal{G}$ from the proof of Theorem 4.1(a) we can identify $T \otimes \mathbb{Q}$ with $K^\vee$ and, by abuse of notation, we will denote also by $b$ and $S$ the forms on $M$ and $M \otimes \mathbb{Q}$ induced by $\mathcal{G}$. Let $m$ be a (column) vector in $M$ (seen as a sub-module of $K^\vee$). Composing $\Lambda$ with the inverse of the isomorphism described in the proof of Proposition 5.1, we obtain

$$M \xrightarrow{\Lambda} M^\vee \xrightarrow{-} \operatorname{Hom}_\mathbb{Z}(M, \mathbb{Z})$$

$$m \mapsto \Lambda m \mapsto \operatorname{Tr}((\Lambda m)^T, -) = \operatorname{Tr}(m^T \Lambda^T, -).$$

So we deduce that the bilinear form $S$ is given by

$$S(a, a') = (\overline{a'})^T \Lambda a$$

where $a$ and $a'$ are column vectors in $K^\vee$. Thus $S$ is skew-Hermitian if and only if $S(a, a')$ equals

$$-S(a', a) = -\overline{(a')^T \Lambda a} = -\overline{(a^T \Lambda a)^T}$$

for arbitrary $a$ and $a'$, which is equivalent to $\Lambda = -\Lambda^T$.

The second condition follows directly from this description. For the statement about the degree see [How04, Section 4].

Let $(M, \Lambda)$ and $(M', \Lambda')$ be the modules corresponding to two polarized abelian varieties. A morphism of polarized abelian varieties will be a morphism $\Psi : M \to M'$ satisfying

$$\overline{\Psi}^T \Lambda' \Psi = \Lambda,$$

since the dual morphism $\Psi^\vee$ is $\overline{\Psi}^T$ by Corollary 5.2. Denote by $\operatorname{Pol}(M)$ the set of polarizations of $M$. 

11
**Theorem 5.4.** There is a degree-preserving action of $\text{Aut}(M)$ on the set $\text{Pol}(M)$ given by

$$\text{Aut}(M) \times \text{Pol}(M) \longrightarrow \text{Pol}(M)$$

$$(U, \Lambda) \longmapsto U^T \Lambda U$$

Two polarizations of $M$ give rise to isomorphic polarized abelian varieties if and only if they lie in the same orbit. In particular, given a polarization $\Lambda$ on $M$, we have

$$\text{Aut}(M, \Lambda) = \text{Stab}(\Lambda).$$

**Proof.** All the statements follow directly from Theorem 5.3. \qed

**Remark 5.5.** Let $\text{Pol}^1(M)$ be the subset of $\text{Pol}(M)$ consisting of principal polarizations. Since the action of $\text{Aut}(M)$ on $\text{Pol}(M)$ is degree-preserving, we get an induced action on $\text{Pol}^1(M)$. Recall that an abelian variety defined over a finite field admits only finitely many non-isomorphic principal polarizations, or, in other words, the quotient

$$Q = \frac{\text{Pol}^1(M)}{\text{Aut}(M)}$$

is finite. Moreover, the action of $\text{Aut}(M)$ on $\text{Pol}^1(M)$ can be extended to the set $\text{Isom}(M, M^\vee)$ of isomorphisms from $M$ to $M^\vee$ and, fixing an element $A_0 \in \text{Isom}(M, M^\vee)$, we have that

$$\text{Isom}(M, M^\vee) = \{ A_0 V : V \in \text{Aut}(M) \}. $$

In particular, a good understanding of $\text{Aut}(M)$ will most likely allow us to handle $Q$, but if $r > 1$, then $\text{Aut}(M)$ is an infinite non-abelian group, making the situation computationally difficult, even if we were able to produce a (finite) set of generators.

Recall that a polarized abelian variety $(A, \mu)$ is called decomposable if there are proper sub-varieties $B_1$ and $B_2$ of $A$, admitting polarizations $\beta_1$ and $\beta_2$, respectively, such that

$$(A, \lambda) \simeq (B_1 \times B_2, \beta_1 \times \beta_2).$$

**Corollary 5.6.** Let $(M, \Lambda)$ in $\mathcal{B}(r)$ correspond to a polarized abelian variety $(A, \mu)$. Then $(A, \mu)$ is decomposable if and only if there are polarized modules $(M_1, \Lambda_1), \ldots, (M_m, \Lambda_m)$ respectively in $\mathcal{B}(r_1), \ldots, \mathcal{B}(r_m)$ with $m > 1$ and $r_1 + \ldots + r_m = r$ and an isomorphism

$$P : M_1 \oplus \ldots \oplus M_m \longrightarrow M$$

satisfying

$$P^T (\Lambda_1 \oplus \ldots \oplus \Lambda_m)P = \Lambda.$$

**Proof.** The statement follows directly from 5.4. \qed
The next example shows that a polarized module \((M, \Lambda)\) can be decomposable even if there is no way to put \(\Lambda\) into a block diagonal matrix by the action of an element of \(\text{Aut}(M)\).

Example 5.7. Let \(K = \mathbb{Q}(F)\) be the number field generated by the 4-Weil polynomial \(x^2 - x + 4\). The order \(\mathfrak{O} = \mathbb{Z}[F, 4/F] = \mathbb{Z} + F\mathbb{Z}\) is maximal in \(K\) and it has Picard group of order 2. Put \(I = 2\mathbb{Z} + F\mathbb{Z}\). One can check that the \(\mathfrak{O}\)-ideal \(I\) is not principal and hence represents the non-trivial ideal class of \(\mathfrak{O}\). The previous discussion implies that there are 2 isomorphism classes of elliptic curves, corresponding to \(\mathfrak{O}\) and \(I\) in that isogeny class. Let \(y = \frac{1}{15}(-1 + 2F)\) and \(z = \frac{1}{30}(-1 + 2F)\) be the principal polarizations of \(\mathfrak{O}\) and \(I\), respectively, that is \(y\mathfrak{O} = \mathfrak{O}\) and \(zI = I\). In particular \(y\) and \(z\) are totally imaginary and totally positive. Now consider the abelian surfaces \(\mathfrak{O} \oplus \mathfrak{O}\) and \(I \oplus I\). Consider the following matrices

\[
P_0 = \begin{pmatrix} 1 & -\frac{3}{2} - 3F \\ -3 - 3F & -2 \end{pmatrix}, \quad M = \begin{pmatrix} 4 & 2F - 1 \\ 2F - 1 & 4 \end{pmatrix},
\]

\[
D = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}, \quad D' = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}.
\]

Note that \(M\) is a unimodular Hermitian matrix in \(\text{GL}_2(\mathfrak{O})\) and hence \(DM\) is a principal polarization on \(\mathfrak{O} \oplus \mathfrak{O}\). Also, observe that the matrix \(P_0\) represents an isomorphism

\[I \oplus I \to \mathfrak{O} \oplus \mathfrak{O},\]

and that every such isomorphism can be described as \(AP_0\) for some \(A \in \text{GL}_2(\mathfrak{O})\).

One can verify by using results contained in \([\text{GHR18}]\) that the polarization \(DM\) is not the pullback of the product polarization \(D\) of \(\mathfrak{O} \oplus \mathfrak{O}\), that is, there is no matrix \(B \in \text{GL}_2(\mathfrak{O})\) such that

\[
B^T DMB = D.
\]

On the other hand \(DM\) is the pullback of the product polarization \(D'\) of \(I \oplus I\). Indeed we have

\[
(AP_0)^T DMAP_0 = D',
\]

for

\[
A = \begin{pmatrix} 7 - 10F & -3 - 2F \\ -23 + 3F & -4 + 3F \end{pmatrix} \in \text{GL}_2(\mathfrak{O}).
\]

Again, the matrix \(A\) has been computed using results from \([\text{GHR18}]\).

6 Examples

Example 6.1. Let \(g = x^8 - x^5 + 2x^4 - 2x^3 + 4x^2 - 4x + 8\). Note that \(g\) corresponds to a simple isogeny class of abelian varieties over \(\mathbb{F}_2\) of \(p\)-rank 1. Define \(K = \mathbb{Q}[x]/(g)\) and \(\alpha = x \mod g\) and put \(R = \mathbb{Z}[\alpha, \overline{\alpha}]\). The only over-order of \(R\) is the maximal order \(\mathfrak{O}_K\) of \(K\) and, since \(R\) is Gorenstein by \([\text{CS15}, \text{Theorem 11}]\) we get that \(R\) is
Bass. We have that the Picard Group of $R$ is isomorphic to the cyclic group of order 3 and it is generated by

$$I = 8R + \left( -32 - 11\alpha - \frac{3}{2}\alpha^2 - 3\alpha^3 - \frac{3}{4}\alpha^4 + \frac{1}{4}\alpha^5 \right) R.$$ 

The maximal order $\mathcal{O}_K$ is a principal ideal domain. We now list the representatives of the isomorphism classes in $\text{AV}(g^3)$:

- $M_1 = R \oplus R \oplus R$
- $M_2 = R \oplus R \oplus I$
- $M_3 = R \oplus R \oplus I^2$
- $M_4 = R \oplus R \oplus \mathcal{O}_K$
- $M_5 = R \oplus \mathcal{O}_K \oplus \mathcal{O}_K$
- $M_6 = \mathcal{O}_K \oplus \mathcal{O}_K \oplus \mathcal{O}_K$

Using Proposition 2.4, we can recover the endomorphism rings of the abelian varieties. For example, $\text{End}(M_1)$ is the ring $M_3(R)$ of $3 \times 3$ matrices over $R$, while $\text{End}(M_2)$ is the matrix ring

$$\begin{pmatrix} R & R & I \\ R & R & I \\ (R : I) & (R : I) & R \end{pmatrix}$$

**Example 6.2.** Let $g = (x^2 - 3x + 13)(x^2 + 6x + 13)$. Define $K = \mathbb{Q}[x]/(g)$ and $\alpha = x \mod g$ and put $S_1 = \mathbb{Z}[\alpha, \overline{\alpha}]$. The over-orders are

- $S_2 = S_1 + \left( \frac{21}{2} + \frac{98}{13} \alpha - \frac{27}{13} \alpha^2 + \frac{2}{26} \alpha^3 \right) S_1$
- $S_3 = S_1 + \left( -\frac{26}{3} + \frac{70}{13} \alpha - \frac{17}{39} \alpha^2 + \frac{1}{13} \alpha^3 \right) S_1$
- $S_4 = S_1 + \left( \frac{11}{2} + \frac{76}{39} \alpha + \frac{3}{13} \alpha^2 - \frac{7}{78} \alpha^3 \right) S_1$
- $S_5 = S_1 + \left( -\frac{13}{9} + \frac{47}{39} \alpha - \frac{4}{117} \alpha^2 + \frac{1}{39} \alpha^3 \right) S_1$
- $S_6 = S_1 + \left( \frac{71}{18} + \frac{251}{117} \alpha + \frac{34}{117} \alpha^2 + \frac{1}{234} \alpha^3 \right) S_1$

Note that $S_6 = \mathcal{O}_K$. It is easy to check that the order $S_1$ is Bass. We now list indexes and Picard groups of the orders.

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 |
|-----|---|---|---|---|---|---|
| $[\mathcal{O}_K : S_i]$ | 162 | 81 | 18 | 9 | 2 | 1 |
| $\text{Pic}(S_i)$ | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$ | 0 | 0 |
In the next table we present how the number of isomorphism classes of abelian varieties in the isogeny class determined by $g^r$ grows as $r$ increases.

| $r$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|-----|---|---|---|---|---|---|---|---|---|----|
| $\#(\text{AV}(g^r)/\sim)$ | 62 | 97 | 144 | 206 | 286 | 387 | 512 | 664 | 846 | 1061 |

References

[Bas62] Hyman Bass, *Torsion free and projective modules*, Trans. Amer. Math. Soc. **102** (1962), 319–327. MR 0140542

[Bas63] , *On the ubiquity of Gorenstein rings*, Math. Z. **82** (1963), 8–28. MR 0153708 (27 #3669)

[BF65] Z. I. Borević and D. K. Faddeev, *Representations of orders with cyclic index*, Trudy Mat. Inst. Steklov **80** (1965), 51–65. MR 0205980

[BL94] J. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260. MR 1360644 (96m:11092)

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$*, Algebra Number Theory **9** (2015), no. 1, 225–265. MR 3317765

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243. MR 0254059

[GHR18] Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler, *Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$*, https://arxiv.org/abs/1806.03826, 2018.

[Hae90] Jeremy Haefner, *Local orders whose lattices are direct sums of ideals*, Trans. Amer. Math. Soc. **321** (1990), no. 2, 717–740. MR 978384

[Hal10] Safia Haloui, *The characteristic polynomials of abelian varieties of dimensions 3 over finite fields*, J. Number Theory **130** (2010), no. 12, 2745–2752. MR 2684495

[HL88] Jeremy Haefner and Lawrence S. Levy, *Commutative orders whose lattices are direct sums of ideals*, J. Pure Appl. Algebra **50** (1988), no. 1, 1–20. MR 931905

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR 0229642
[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. 347 (1995), no. 7, 2361–2401. MR 1297531

[How04] _______, *On the non-existence of certain curves of genus two*, Compos. Math. 140 (2004), no. 3, 581–592. MR 2041770

[HS12] Safia Haloui and Vijaykumar Singh, *The characteristic polynomials of abelian varieties of dimension 4 over finite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 59–68. MR 2961400

[JKP+17] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, arXiv:1602.06237v2, 2017.

[Kan11] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. 62 (2011), no. 3, 297–339. MR 2825715

[KP05] Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra 292 (2005), no. 1, 47–64. MR 2166795 (2006f:11142)

[Lau02] Kristin Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math. 134 (2002), no. 1, 87–111, With an appendix by Jean-Pierre Serre. MR 1931964

[LW85] Lawrence S. Levy and Roger Wiegand, *Dedekind-like behavior of rings with 2-generated ideals*, J. Pure Appl. Algebra 37 (1985), no. 1, 41–58. MR 794792

[Mar18a] Stefano Marseglia, *Computing abelian varieties over finite fields*, Stockholm University, 2018.

[Mar18b] _______, *Computing isomorphism classes of square-free polarized abelian varieties over finite fields*, https://arxiv.org/abs/1805.10223, 2018.

[Mar18c] _______, *Ideal class monoid of an order and conjugacy classes of integral matrices*, arXiv:1805.09671, 2018.

[NR67] L. A. Nazarova and A. V. Roiter, *A sharpening of a theorem of Bass*, Dokl. Akad. Nauk SSSR 176 (1967), 266–268. MR 0225810

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144. MR 0206004
[WM71] W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64. MR 0314847

S. Marseglia, Matematiska institutionen, Stockholms universitet, 106 91 Stockholm, Sweden

E-mail: stefanom@math.su.se