S. Marseglia *Res. Number Theory* (2019) 5:35
https://doi.org/10.1007/s40993-019-0174-x

Research in Number Theory

RESEARCH

Computing abelian varieties over finite fields isogenous to a power

Stefano Marseglia[1,2*]

*Correspondence:
stefanom@math.su.se,
s.marseglia@uu.nl
[1]Matematiska institutionen,
Stockholms universitet, 106 91
Stockholm, Sweden
Full list of author information is
available at the end of the article

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.

Keywords: Abelian varieties, Finite fields, Polarizations, Bass orders

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 [8] 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 [7] 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 included in this equivalence the notions of dual variety and polarizations, see [16].

In [24] 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^r 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 [2] and [22], and we can explicitly compute representatives of the isomorphism classes of the abelian varieties.

There are other categorical descriptions of the category of abelian varieties isogenous to a power of elliptic curves in terms of modules with extra-structure, see the Appendix in [19,21] and [18]. We do not make use of such descriptions and instead we work with Deligne's and Centeleghe–Stix equivalences because they allow us to deduce results also about powers of abelian varieties of dimension greater than 1.

The paper is structured as follows. In Sect. 2 we recall the notion of an order and a fractional ideal, with a focus on Bass orders. In Sect. 3 we describe the categorical equivalences that we are going to use in Sect. 4, where we focus on the case of abelian varieties with characteristic polynomial of the form $h = g^r$, with g square-free. These equivalences are based on the theorems of Deligne and Centeleghe–Stix cited above and the target category of the functors realizing them is well suited for computational purposes.

In Sect. 5 we translate the notion of a polarization into module-theoretic language. Finally, in Sect. 6 we apply our description and present the results of some computations.

The aim of the paper is to provide an effective algorithm to perform computations of isomorphism classes of abelian varieties. The implementations can be found on the author's web-page. We plan to use such algorithms to produce representatives that will be uploaded to the LMFDB [29]. Nevertheless the machinery built allows us to produce also theoretical results about the isogeny classes with characteristic polynomial of the form g^r. For example, if R is a Bass order, we can prove that if $r > 1$ then an abelian variety in such an isogeny class is not just isogenous but also isomorphic to a product of r abelian varieties, see Corollary 4.3. We can also prove that given two abelian varieties A and B is such an isogeny class, there exists and integer r such that A^r and B^r are isomorphic if and only if A and B have the same endomorphism ring, see Corollary 4.6. We get also statements about polarized abelian varieties, see Corollary 5.7 and Remark 5.8. In a forthcoming paper we plan to use the machinery introduced to answer questions related to field extensions, for example, whether an abelian variety A over $\mathbb{F}_q$ can be defined over a proper subfield of $\mathbb{F}_q$.

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 $\mathrm{Hom}(A, B)$ for $\mathrm{Hom}_k(A, B)$. 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

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

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 $I=\alpha_1\mathbb{Z}\oplus\cdots\oplus\alpha_n\mathbb{Z}$ then $I^t=\alpha_1^*\mathbb{Z}\oplus\cdots\oplus\alpha_n^*\mathbb{Z}$, where $\left\{\alpha_i^*\right\}_i$ is the dual basis characterized by the relations $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^*\alpha_j)=1$ if $i=j$ and 0 otherwise.

Given any full lattice I in K the set $(I:I)$ is an order. If I is a 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 [5, Proposition 2.7]. Examples of Gorenstein orders are $\mathcal{O}_K$ and the monogenic order $R=\mathbb{Z}[x]/(f)$, see [5, 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 [2] on Gorenstein rings. There are many sources where one can find a proof of Proposition 2.1 (and other characterizations), for example [22, 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

$$\mathrm{ICM}(R)=\{\text{fractional}R-\text{ideals}\}/_{\simeq}$$

and the *ideal class group* as

$$\mathrm{Pic}(R)=\{\text{invertible fractional}R-\text{ideals}\}/_{\simeq},$$

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

$$\mathrm{ICM}(R)\supseteq\bigsqcup_S\mathrm{Pic}(S),$$

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 [20]. For more about the computation of $\mathrm{ICM}(R)$, even in the non-Bass case, we refer to [25].

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

Definition 2.2 For an order R in K, we define $\mathscr{B}(r)$ as the category of torsion-free R-modules M such that $M \otimes K$ is a free K-module of rank r. The morphisms are the R-linear morphisms.

Crucial for our purpose is the fact that, when R is a Bass order, the modules in $\mathscr{B}(r)$ 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 $\mathscr{B}(r)$. Then there are fractional R-ideals $I_1, \dots, I_r$ with $(I_1 : I_1) \subseteq \cdots \subseteq (I_r : I_r)$ such that*

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

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

This result was first proved in [1, Theorem 1.7] for Noetherian integral domains with finite integral closure such that every ideal can be generated by 2 elements. Later it was reproved with a different method in [3, Theorem 8] for an order in a commutative, separable, semisimple extension of the quotient field of a Dedekind domain. In [22, Theorem 7.1] the results was generalized to Bass rings, that is, commutative rings without nilpotents with finite integral closure such that every ideal can be generated by 2 elements.

Using the same notation as in Theorem 2.3, we see that M can be written in a canonical form

$$M \simeq S_1 \oplus \cdots \oplus S_{r-1} \oplus I,$$

with $S_1 \subseteq \cdots \subseteq S_{r-1} \subseteq (I : I)$ where $S_i = (I_i : I_i)$ and $[I] = [I_1 \dots I_r]$. Moreover, the 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 $\mathscr{B}(r)$, for every r.

Proposition 2.4 *Let $M = I_1 \oplus \cdots \oplus I_r \in \mathscr{B}(r)$ and $N = J_1 \oplus \cdots \oplus J_s \in \mathscr{B}(r)$. Then*

$$\mathrm{Hom}_R(M, N) = \left\{ A \in \mathscr{M}_{s \times r}(K) : A_{j,i} \in (J_j : I_i) \right\}.$$

Proof The statement follows from the fact that $\mathrm{Hom}_R(I_i, J_j) = (J_j : I_i)$ since every R-linear morphism $\varphi : I_i \to J_j$ is a multiplication by $\alpha \in K$, where α is the image of 1_K under the induced K-linear endomorphism $\varphi \otimes \mathbb{Q}$ of K. □

In particular, for $M = S_1 \oplus \cdots \oplus S_{r-1} \oplus I$ as above we have

$$\mathrm{End}_R(M) = \begin{pmatrix} S_1 & (S_1 : S_2) & \cdots & (S_1 : S_{r-1}) & (S_1 : I) \\ S_2 & S_2 & \cdots & (S_2 : S_{r-1}) & (S_2 : I) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{r-1} & S_{r-1} & \cdots & S_{r-1} & (S_{r-1} : I) \\ I & I & \cdots & I & (I : I) \end{pmatrix}$$

and

$$\mathrm{Aut}_R(M) = \left\{A \in \mathrm{End}_R(M) \cap \mathrm{GL}_r(K) : A^{-1} \in \mathrm{End}_R(M)\right\}.$$

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 realizing the isomorphism, as the next example shows.

Example 2.5 ([3, Lemma 8]). Let R be a Bass order and 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

$$I_1 \oplus I_2 \simeq S_1 \oplus (I_1 I_2).$$

We want to exhibit a matrix A realizing the isomorphism. Since I_1 is invertible in S_1, there are elements c_1 and c_2 in $K^\times$ such that $c_1 I_1 + c_2 I_2 = S_1$, see [6, Algorithm 1.3.14]. Thus there are $a_1 \in c_1 I_1$ and $a_2 \in c_2 I_2$ such that $1 = a_1 + a_2$. We claim that the matrix

$$A = \begin{pmatrix} c_1 & -c_2 \\ \dfrac{a_2}{c_2} & \dfrac{a_1}{c_1} \end{pmatrix}$$

satisfies $A(I_1 \oplus I_2) = S_1 \oplus I_1 I_2$ (where the action is on column vectors). Indeed given $i_1 \in I_1$ and $i_2 \in I_2$ we have

$$A \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} = \begin{pmatrix} c_1 i_1 - c_2 i_2 \\ \dfrac{a_2}{c_2} i_1 + \dfrac{a_1}{c_1} i_2 \end{pmatrix}.$$

Observe that

$$c_1 i_1 - c_2 i_2 \in c_1 I_1 + c_2 I_2 = S_1$$

and

$$\frac{a_2}{c_2} i_1 + \frac{a_1}{c_1} i_2 \in I_1 I_2,$$

as required. Furthermore, note that $\det(A) = 1$ and that given $s_1 \in S_1$ and $i_1 i_2 \in I_1 I_2$ we have

$$A^{-1} \begin{pmatrix} s_1 \\ i_1 i_2 \end{pmatrix} = \begin{pmatrix} \dfrac{a_1}{c_1} & c_2 \\ -\dfrac{a_2}{c_2} & c_1 \end{pmatrix} \begin{pmatrix} s_1 \\ i_1 i_2 \end{pmatrix} = \begin{pmatrix} \dfrac{a_1}{c_1} s_1 + c_2 i_2 i_1 \\ -\dfrac{a_2}{c_2} s_1 + c_1 i_1 i_2 \end{pmatrix}.$$

Since $a_1/c_1 \in I_1$, $a_2/c_2 \in I_2$, $c_1 i_1, c_2 i_2 \in S_1$ and $I_1 I_2$ is additively generated by elements of the form $i_1 i_2$, we conclude that $A^{-1}(S_1 \oplus I_1 I_2) \subset I_1 \oplus I_2$.

3 The category of abelian varieties over a finite field

Let q be a power of a prime number p and let $\mathrm{AV}(q)$ be the category of abelian varieties defined over $\mathbb{F}_q$. For A in $\mathrm{AV}(q)$ 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

$$A \sim B_1^{e_1} \times \cdots \times B_r^{e_r},$$

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 $\mathrm{AV}(q)$ 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 [30, 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 [12] for $g = 3$ and [17] for $g = 4$. By Honda–Tate theory, see [28] and [15], this corresponds to describing all isogeny classes of abelian varieties in $\mathrm{AV}(q)$ of a given dimension g. For such a polynomial h, denote by $\mathrm{AV}(h)$ the full subcategory of $\mathrm{AV}(q)$ whose objects are the abelian varieties in the isogeny class determined by h.

We will restrict our attention to two subcategories of $\mathrm{AV}(q)$. Recall that an abelian variety A over $\mathbb{F}_q$ is called *ordinary* if exactly half of the roots of h_A over $\overline{\mathbb{Q}}_p$ are p-adic units. There are many other characterizations of ordinary abelian varieties. For example see [8, Sect. 2]. We will denote the full subcategory of $\mathrm{AV}(q)$ consisting of ordinary abelian varieties by $\mathrm{AV}^{\mathrm{ord}}(q)$. We will also consider the subcategory $\mathrm{AV}^{\mathrm{cs}}(p)$ 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 $\mathrm{AV}^{\mathrm{ord}}(q)$ and $\mathrm{AV}^{\mathrm{cs}}(p)$ in terms of $\mathbb{Z}$-lattices with extra structure. More precisely, consider the following categories:

- The category $\mathscr{M}^{\mathrm{ord}}(q)$ 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 $T \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $\mathscr{M}^{\mathrm{cs}}(p)$ 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 $T \otimes_{\mathbb{Z}} \mathbb{Q}$ 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

$$\begin{array}{ccc} T & \xrightarrow{\varphi} & T' \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F'} \\ T & \xrightarrow{\varphi} & T' \end{array}$$

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

Theorem 3.1 *There are equivalences of categories*

$$\mathscr{F}^{ord} : \mathrm{AV}^{ord}(q) \to \mathscr{M}^{ord}(q)$$

and

$$\mathscr{F}^{cs} : \mathrm{AV}^{cs}(p) \to \mathscr{M}^{cs}(p).$$

If $A \mapsto (T, F)$, *then* $\mathrm{rank}_{\mathbb{Z}}\, T = 2\dim A$ *and the Frobenius endomorphism* Frob_A *is sent to* F, *so in particular they have the same characteristic polynomial.*

Proof For the ordinary case over $\mathbb{F}_q$ see [8, Sect. 7]. For the case with no-real roots over $\mathbb{F}_p$ we use the covariant version [7, 1.7] of the equivalence given in [7, Theorem 1]. □

Remark 3.2 We remark that the functors of Theorem 3.1 depend on some choices, which can be made in a way that $\mathscr{F}^{\mathrm{cs}}$ extends $\mathscr{F}^{\mathrm{ord}}$ on $\mathrm{AV}^{\mathrm{ord}}(p)$, see [7, 7.4].

4 Abelian varieties isogenous to a power

Let h be a characteristic polynomial of an abelian variety in $\mathrm{AV}^{\mathrm{ord}}(q)$ or $\mathrm{AV}^{\mathrm{cs}}(p)$. Assume moreover that $h = g^r$ for some square-free polynomial g in $\mathbb{Z}[x]$. Put $K = \mathbb{Q}[x]/(g)$ and $\alpha = x \bmod (g)$. Denote with R the order $\mathbb{Z}[\alpha, q/\alpha]$ in K (with $q = p$ if we are in $\mathrm{AV}^{\mathrm{cs}}(p)$). Observe that the order R is Gorenstein, see [7, Theorem 11].

Theorem 4.1 *(a) If* $\mathrm{AV}(h) \subset \mathrm{AV}^{ord}(q)$ *or* $\mathrm{AV}(h) \subset \mathrm{AV}^{cs}(p)$ *then there is an equivalence of categories* $\mathscr{F} : \mathrm{AV}(h) \to \mathscr{B}(r)$.

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

$$\mathrm{AV}(h)/_{\simeq}$$

and the set of pairs

$$(S_1 \subseteq S_2 \subseteq \cdots \subseteq S_r, [I]),$$

where each S_i *is an over-order of* R *and* $[I]$ *denotes the isomorphism class of a fractional ideal with* $(I : I) = S_r$.

Proof Denote by $\mathscr{M}(h)$ the image of $\mathrm{AV}(h)$ via $\mathscr{F}^{\mathrm{ord}}$ (or $\mathscr{F}^{\mathrm{cs}}$). We will define an equivalence $\mathscr{G} : \mathscr{M}(h) \to \mathscr{B}(r)$. Take A in $\mathrm{AV}(h)$ and let (T, F) be the image of A in $\mathscr{M}(h)$ via $\mathscr{F}^{\mathrm{ord}}$ (or $\mathscr{F}^{\mathrm{cs}}$). The minimal polynomial of the $\mathbb{Q}$-linear endomorphism $F \otimes \mathbb{Q}$ of $T \otimes \mathbb{Q}$ is g. So by definition of $\mathscr{M}^{\mathrm{ord}}(q)$ (or $\mathscr{M}^{\mathrm{cs}}(p)$) we have that F and V induce on T an R-module structure via the isomorphism $R \simeq \mathbb{Z}[F, V]$ given by $\alpha \mapsto F$. Denote this R-module by M and put $\mathscr{G}((T, F)) = M$. 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 $g = g_1 \dots g_s$. 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 $1_K = e_1 + \cdots + e_s$ and $Ke_i \simeq K_i$ 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 $T \otimes_{\mathbb{Z}} \mathbb{Q} = W_1 \oplus \cdots \oplus W_s$ such that the action of $F \otimes \mathbb{Q}$ on each W_i is simple. This means that,

possibly after renumbering, we can assume that the minimal polynomial of $F \otimes \mathbb{Q}|_{W_i}$ is g_i and so $\dim_{\mathbb{Q}} W_i = r \deg(g_i)$. In particular the action of $F \otimes \mathbb{Q}$ on W_i is the same as the action of α on $M \otimes_R Ke_i$. Since $\deg(g_i) = \dim_{\mathbb{Q}} Ke_i$ it follows that $\dim_{Ke_i}(M \otimes_R Ke_i) = r$ and hence, by taking the direct sum over i, we obtain an isomorphism

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

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

Remark 4.2 The equivalence $\mathscr{F}$ of part (a) of Theorem 4.1 is compatible with products. More precisely, if we denote $\mathscr{F}_i$ the equivalence $\mathrm{AV}(g^i) \to \mathscr{B}(i)$ then we pick A and B respectively in $\mathrm{AV}(g^m)$ and $\mathrm{AV}(g^n)$ then we have a canonical isomorphism

$$\mathscr{F}_{m+n}(A \times B) \simeq \mathscr{F}_m(A) \oplus \mathscr{F}_n(B) \in \mathscr{B}(m+n).$$

We will denote all these functors with $\mathscr{F}$.

Corollary 4.3 *Assume that R is a Bass order. Then every abelian variety A in $\mathrm{AV}(h)$ is isomorphic to*

$$B_1 \times \cdots \times B_r,$$

for some abelian varieties B_i in $\mathrm{AV}(g)$.

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

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

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

Remark 4.4 In Corollary 4.3, the abelian varieties B_i are simple if and only if g is irreducible. This follows from [16, Theorem 3.3] for the ordinary case over $\mathbb{F}_q$ and from [30, Theorem 8] for characteristic polynomials over $\mathbb{F}_p$ with no real roots.

Corollary 4.5 *Let A be in $\mathrm{AV}(h^r)$. If $r > 1$ then $\mathrm{End}(A)$ is not commutative.*

Proof It follows from the fact that $\mathrm{End}(A) \otimes \mathbb{Q} \simeq \mathscr{M}_{r \times r}(K)$, see Proposition 2.4. □

Corollary 4.6 *Assume that R is a Bass order. Let A and B be in $\mathrm{AV}(g)$. Then there exists a positive integer r such that A^r and B^r are isomorphic if and only if $\mathrm{End}(A) = \mathrm{End}(B)$. If this is the case, then r is bounded by the exponent of $\mathrm{Pic}(R)$.*

Proof Put $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$. Assume first that $A^r \simeq B^r$. Then using Theorem 4.1 we have that

$$\bigoplus_{i=1}^{r} I \simeq_R \bigoplus_{i=1}^{r} J$$

which is equivalent to having $I^r \simeq J^r$ and $(I : I) = (J : J)$. In particular this last condition give us $\mathrm{End}(A) = \mathrm{End}(B)$. Conversely, assume that the endomorphism rings of A and B

are the same and put $S = \mathscr{F}(\mathrm{End}(A))$. Let r be the exponent of $\mathrm{Pic}(S)$, so that $I^r \simeq J^r \simeq S$. In particular, using the same argument as before in the opposite direction we obtain that $A^r \simeq B^r$. The last statement follows from the fact that since S is an over-order of R, there is a surjective map from $\mathrm{Pic}(R)$ to $\mathrm{Pic}(S)$ and in particular the exponent of $\mathrm{Pic}(S)$ divides the exponent of $\mathrm{Pic}(R)$. □

Remark 4.7 Note that Theorem 4.1 is a generalization of [24, Theorem 4.3], where we deal with the case when h is square-free, that is, $r = 1$.

Remark 4.8 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 [2], the author describes when it fails, but overlooks some cases. The gaps were filled in [27] and in [11] in the local case and in [13] 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 Sect. 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 $\mathrm{AV}(h)$ correspond to in the category $\mathscr{B}(r)$ via the equivalence $\mathscr{F}$ of Theorem 4.1.(*b*).

Note that K is a CM-algebra, that is, there is an involution $a \mapsto \overline{a}$ that acts as complex conjugation after composing with any non-zero homomorphism $\varphi : K \to \mathbb{C}$. In particular, we have that $R = \mathbb{Z}[\alpha, \overline{\alpha}]$ where $\overline{\alpha} = q/\alpha$. 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 $\mathscr{B}(r)$, since we can identify M with a sub-R-module of K^r, we have an induced action $M \mapsto \overline{M}$. Moreover, if we consider M as a submodule of K^r, we see that the trace $\mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ induces a non-degenerate bilinear form Tr on M by

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

where we think of all vectors in K^r as column 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 Tr. In particular, if $n = \deg(h)$ and we fix a $\mathbb{Z}$-basis

$$M = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_{nr} \mathbb{Z}, \quad \text{with } \alpha_j \in K$$

then we can write

$$M^t = \alpha_1^* \mathbb{Z} \oplus \cdots \oplus \alpha_{nr}^* \mathbb{Z},$$

where α_i^* is the dual basis characterized by $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j^*) = 1$ if $i = j$ and 0 otherwise.

Proposition 5.1 *Let A be an abelian variety in $\mathrm{AV}(h)$ and put $M = \mathscr{F}(A)$. If $A^\vee$ is the dual abelian variety of A, then there is a canonical isomorphism between $\mathscr{F}(A^\vee)$ and $M^\vee$, where $M^\vee = \overline{M}^t$. In particular, if $M = I_1 \oplus \cdots \oplus I_r$ then $M^\vee = \overline{I}_1^t \oplus \cdots \oplus \overline{I}_r^t$.*

Proof Let $\mathscr{G}$ be the functor defined in the proof of Theorem 4.1.(*a*). Put $(T, F) = \mathscr{F}^{\mathrm{ord}}(A)$, so that $\mathscr{G}((T, F)) = M$. Following [16, Proposition 4.5], we have that $\mathscr{F}^{\mathrm{ord}}(A^\vee) = (T^\vee, F^\vee)$,

where $T^\vee = \mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Z})$ and $F^\vee(\psi) = \psi \circ V$ for every $\psi \in T^\vee$. To conclude, we need to show that $\mathscr{G}(T^\vee, F^\vee) = M^\vee$. It is clear that $\mathscr{G}$ sends $T^\vee$ to $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ (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 $\mathscr{G}$, to the multiplication by α after taking the complex conjugate. More precisely, write $M = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_{nr}\mathbb{Z}$, for $\alpha_j \in K$, with $n = [K : \mathbb{Q}]$, and consider the $\mathbb{Z}$-linear isomorphism

$$\begin{aligned} \rho : \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) &\to \overline{M}^t \\ \psi &\longmapsto \sum_{i=1}^{nr} \psi(\alpha_i)\overline{\alpha}_i^* \end{aligned}$$

with inverse

$$\mathrm{Tr}(\overline{x}^T, -) \longleftarrow\!\shortmid x,$$

where $\overline{x}^T$ is the transpose of $\overline{x}$. Using this identification, the pre-composition with $\overline{\alpha}$ on $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ will correspond to multiplication by α on $\overline{M}^t$, where, as usual, α is the image of the Frobenius endomorphism via the functor $\mathscr{F}$. □

Remark 5.2 From now on we will fix a basis of K^r and fix an isomorphism $M \otimes K \simeq K^r$ for each $M \in \mathscr{B}(r)$. In particular this will allow us to represent morphisms (in a non-canonical way) in $\mathscr{B}(r)$ as matrices with entries in K.

Corollary 5.3 *Let $\mu : A \to B$ be a morphism of abelian varieties in* $\mathrm{AV}(h)$. *Put $\mathscr{F}(A) = M$, $\mathscr{F}(B) = N$ and $\mathscr{F}(\mu) = \Lambda : M \to N$ in $\mathscr{B}(r)$. Then μ is an isogeny if and only if* $\det \Lambda \in K^\times$. *Moreover, the dual morphism $\mu^\vee : B^\vee \to A^\vee$ corresponds via $\mathscr{F}$ to the morphism $\Lambda^\vee = \overline{\Lambda}^T : N^\vee \to M^\vee$, where $\overline{\Lambda}^T$ is the transpose of $\overline{\Lambda}$.*

Proof Put $(T, F) = \mathscr{F}^{\mathrm{ord}}(A)$, $(T', F') = \mathscr{F}^{\mathrm{ord}}(B)$ and $\mathscr{F}^{\mathrm{ord}}(\mu) = (T, F) \xrightarrow{\lambda} (T', F')$. Then μ is an isogeny if and only if the induced morphism $\lambda \otimes \mathbb{Q}$ is invertible. Let $\mathscr{G}$ be the functor defined in the proof of Theorem 4.1.(*a*). Observe that $\mathscr{G}(\lambda) = \Lambda$ and hence $\lambda \otimes \mathbb{Q}$ is invertible if and only if the matrix Λ is invertible over K.

Put $\mathscr{F}^{\mathrm{ord}}(\mu^\vee) = \lambda^\vee$ where $(T'^\vee, F'^\vee) \xrightarrow{\lambda^\vee} (T^\vee, F^\vee)$ is defined by $\lambda^\vee(\psi) = \psi \circ \lambda$ for every $\psi \in T'^\vee$. Using Proposition 5.1, we see that, if $\mathscr{G}(\lambda) = \Lambda$ then $\mathscr{G}(\lambda^\vee) = \overline{\Lambda}^T$. □

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 $\mathscr{M}^{\mathrm{ord}}(q)$. More precisely, put

$$\Phi = \left\{\varphi \in \mathrm{Hom}(K, \mathbb{C}) : v_p(\varphi(\alpha)) > 0\right\},$$

where v_p is the p-adic valuation induced by a fixed isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$. In [24] we give an algorithm to compute such a Φ. Recall that an element a in K is called *totally imaginary* if $\overline{a} = -a$. We say that a totally imaginary a is Φ-*non-positive* if $\Im(\varphi(a)) \leq 0$ for every φ in Φ.

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

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

Then there exists a unique K-sesquilinear form S on $T \otimes \mathbb{Q}$ such that $b = \mathrm{Tr}_{K/\mathbb{Q}} \circ S$ and, using [16, Proposition 4.9], we have that μ 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 Φ-non-positive.

Theorem 5.4 *Let A be an abelian variety in* $\mathrm{AV}(h)$ *and let $\mu : A \to A^\vee$ be an isogeny. Put $\mathscr{F}(\mu) = \Lambda : M \to M^\vee$. Then μ is a polarization if and only if*

- $\Lambda = -\overline{\Lambda}^T$ *and,*
- *for every column vector a in K^r, the element $a^T\overline{\Lambda}\overline{a}$ is Φ-non-positive.*

We have $\deg \mu = [M^\vee : \Lambda M]$.

Proof Put $\mathscr{F}^{\mathrm{ord}}(A) = (T, F)$. Using the functor $\mathscr{G}$ from the proof of Theorem 4.1.(a) we can identify $T \otimes_{\mathbb{Z}} \mathbb{Q}$ with K^r and, by abuse of notation, we will denote also by b and S the forms on M and $M \otimes \mathbb{Q}$ induced by $\mathscr{G}$. Let m be a (column) vector in M (seen as a submodule of K^r). Composing Λ with the inverse of the isomorphism ρ^{-1} introduced in the proof of Proposition 5.1, we obtain

$$\begin{aligned} M &\xrightarrow{\Lambda} M^\vee \xrightarrow{\rho^{-1}} \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) \\ m &\longmapsto \Lambda m \longmapsto \mathrm{Tr}((\overline{\Lambda m})^T, -) = \mathrm{Tr}(\overline{m^T \Lambda^T}, -). \end{aligned}$$

So we deduce that the bilinear form S is given by

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

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

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

for arbitrary a and a', which is equivalent to $\Lambda = -\overline{\Lambda}^T$.
The second condition follows directly from this description. The statement about the degree follows from [16, Proposition 4.14]. □

Let (M, Λ) and (M', Λ') 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 5.3. Denote by $\mathrm{Pol}(M)$ the set of polarizations of M.

Theorem 5.5 *There is a degree-preserving action of* $\mathrm{Aut}(M)$ *on the set* $\mathrm{Pol}(M)$ *given by*

$$\begin{aligned} \mathrm{Aut}(M) \times \mathrm{Pol}(M) &\longrightarrow \mathrm{Pol}(M) \\ (U, \Lambda) &\longmapsto \overline{U}^T \Lambda U \end{aligned}$$

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 Λ on M, we have

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

Proof Let Λ be a polarization of M and U an automorphism of M. Observe that the first condition of Theorem 5.4 is satisfied for $\overline{U}^T \Lambda U$, since

$$-(\overline{\overline{U}^T \Lambda U})^T = -(U^T \overline{\Lambda U})^T = -\overline{U}^T (U^T \overline{\Lambda})^T = -\overline{U \Lambda}^T U = \overline{U} \Lambda U,$$

where the last equality holds because $-\overline{\Lambda}^T = \Lambda$. Note that given $a \in K^r$ we have that

$$a^T \overline{\overline{U}^T \Lambda U \overline{a}} = (Ua)^T \overline{\Lambda \overline{(Ua)}}$$

which is then Φ-non-negative, since U is also an automorphism of K^r. Hence the second condition of Theorem 5.4 holds as well and $\overline{U}^T \Lambda U$ is a polarization of M. The statement on the degree follows from the existence of R-linear isomorphisms

$$\frac{M^\vee}{(\overline{U}^T \Lambda U)M} \simeq \frac{(\overline{U}^T)^{-1} M^\vee}{(\Lambda U)M} \simeq \frac{M^\vee}{\Lambda M}.$$

□

Remark 5.6 Let $\mathrm{Pol}^1(M)$ be the subset of $\mathrm{Pol}(M)$ consisting of principal polarizations. Since the action of $\mathrm{Aut}(M)$ on $\mathrm{Pol}(M)$ is degree-preserving, we get an induced action on $\mathrm{Pol}^1(M)$. Recall that an abelian variety defined over a finite field admits only finitely many non-isomorphic principal polarizations, or, in other words, the quotient

$$Q = {}^{\mathrm{Pol}^1(M)}\!/_{\mathrm{Aut}(M)}$$

is finite. Moreover, the action of $\mathrm{Aut}(M)$ on $\mathrm{Pol}^1(M)$ can be extended to the set $\mathrm{Isom}(M, M^\vee)$ of isomorphisms from M to $M^\vee$. In particular, by fixing an element A_0 in $\mathrm{Isom}(M, M^\vee)$, we get

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

This suggests that a good understanding of $\mathrm{Aut}(M)$ will most likely allow us to handle Q, but if $r > 1$, then $\mathrm{Aut}(M)$ 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, μ) is called *decomposable* if there are proper subvarieties B_1 and B_2 of A, admitting polarizations β_1 and β_2, respectively, such that

$$(A, \mu) \simeq (B_1 \times B_2, \mu_1 \times \mu_2).$$

Corollary 5.7 *Let (M, Λ) in $\mathscr{B}(r)$ correspond to a polarized abelian variety (A, μ). Then (A, μ) is decomposable if and only if there are an integer $m > 1$ and polarized modules $(M_i, \Lambda_i) \in \mathscr{B}(r_i)$ for $i = 1, \ldots, m$ with $r_1 + \cdots + r_m = r$ and an isomorphism*

$$P : M_1 \oplus \cdots \oplus M_m \to M$$

satisfying

$$\overline{P}^T (\Lambda_1 \oplus \cdots \oplus \Lambda_m) P = \Lambda.$$

Proof Let $\mathscr{F}(A, \mu) = (M, \Lambda)$ and $\mathscr{F}(B_i, \mu_i) = (M_i, \Lambda_i)$ for $i = 1, \ldots, m$. Then there exists a polarized isomorphism $f : \prod_i (B_i, \mu_i) \to (A, \mu)$ if and only if there exists an R-linear map P as in the statement of the corollary. □

Remark 5.8 Assume that R is Bass and that $r > 1$. For simplicity, let us assume that g is irreducible and let (A, μ) be a polarized abelian variety in $\mathrm{AV}(g^r)$. By Corollary 4.3 we know that A is isomorphic to the product of r simple abelian varieties. Hence Corollary 5.7 tells us that the obstruction for (A, μ) to be decomposable is a property of the polarization μ.

The next example shows that a polarized module (M, Λ) can be decomposable even if there is no way to put Λ into a block diagonal matrix by the action of an element of $\mathrm{Aut}(M)$.

Example 5.9 Let $K = \mathbb{Q}(F)$ be the number field generated by the 4-Weil polynomial $h = x^2 - x + 4$. The order $\mathcal{O} = \mathbb{Z}[F, 4/F] = \mathbb{Z} + F\mathbb{Z}$ 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 $\mathcal{O}$-ideal I is not principal and hence represents the non-trivial ideal class of $\mathcal{O}$. The previous discussion implies that there are 2 isomorphism classes of elliptic curves, corresponding to $\mathcal{O}$ 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 $\mathcal{O}$ and I, respectively, that is, $y\mathcal{O} = \overline{\mathcal{O}}^t$ and $zI = \overline{I}^t$. Now consider the abelian surfaces $\mathcal{O} \oplus \mathcal{O}$ and $I \oplus I$ and the following matrices

$$P_0 = \begin{pmatrix} 1 & \frac{-3-3F}{2} \\ \frac{-3-3F}{2} & \frac{-13+13F}{2} \end{pmatrix}, \quad M = \begin{pmatrix} 4 & 2\overline{F} - 1 \\ 2F - 1 & 4 \end{pmatrix},$$
$$D = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}, \quad D' = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}.$$

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

$$I \oplus I \to \mathcal{O} \oplus \mathcal{O},$$

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

One can verify by using results contained in [10] that the polarization DM is not the pullback of the product polarization D of $\mathcal{O} \oplus \mathcal{O}$, that is, there is no matrix $B \in \mathrm{GL}_2(\mathcal{O})$ such that

$$\overline{B}^T DMB = D.$$

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

$$(\overline{AP_0})^T DMAP_0 = D',$$

for

$$A = \begin{pmatrix} 7 - 10F & -3 - 2F \\ -23 + 3F & -4 + 3F \end{pmatrix} \in GL_2(\mathcal{O}).$$

Again, the matrix A has been computed using results from [10].

6 Examples

With the previous results we can create effective algorithms to compute examples of different phenomena of abelian varieties over finite fields that are isogenous to powers.

Example 6.1 In this example we compute all the isomorphism classes in the isogeny class $\mathrm{AV}(g^3)$ where $g = x^6 - x^5 + 2x^4 - 2x^3 + 4x^2 - 4x + 8$. Note that g corresponds to a simple isogeny class of abelian varieties over $\mathbb{F}_2$. Define $K = \mathbb{Q}[x]/(g)$ and $\alpha = x \bmod g$ and put $R = \mathbb{Z}[\alpha, \overline{\alpha}]$. The only over-order of R is the maximal order $\mathcal{O}_K$ of K and, since R is Gorenstein by [7, Theorem 11] we get that R is Bass. 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 $\mathscr{O}_K$ is a principal ideal domain. Using Theorem 4.1(b) we can count the isomorphism classes in $\mathrm{AV}(g^3)$, which are functorially represented by the following R-modules in $\mathscr{B}(3)$:

$$\begin{aligned} M_1 &= R \oplus R \oplus R \\ M_2 &= R \oplus R \oplus I \\ M_3 &= R \oplus R \oplus I^2 \\ M_4 &= R \oplus R \oplus \mathscr{O}_K \\ M_5 &= R \oplus \mathscr{O}_K \oplus \mathscr{O}_K \\ M_6 &= \mathscr{O}_K \oplus \mathscr{O}_K \oplus \mathscr{O}_K. \end{aligned}$$

Using Proposition 2.4 we can recover the endomorphism rings of the abelian varieties by their (functorial) representations as endomorphism rings of the modules M_i. For example, $\mathrm{End}(M_1)$ is the ring of 3×3 matrices over R, while $\mathrm{End}(M_2)$ is the matrix ring

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

Example 6.2 Let $g = (x^2 - 3x + 13)(x^2 + 6x + 13)$. Define $K = \mathbb{Q}[x]/(g)$ and $\alpha = x \bmod g$ and put $R = \mathbb{Z}[\alpha, \overline{\alpha}]$. Using the algorithm described in [25] we can compute the 6 over-orders of R and verify that they are all Gorenstein, that is, that R is a Bass order. We apply Theorem 4.1 to compute the number of isomorphism classes of abelian varieties in the isogeny class determined by g^r as r increases and collect the results for $1 \leq r \leq 10$ in the following table.

r	1	2	3	4	5	6	7	8	9	10
$\#\left(\mathrm{AV}(g^r)/_{\simeq}\right)$	62	97	144	206	286	387	512	664	846	1061

Example 6.3 In this example we will prove that certain isomorphism classes in the isogeny class $\mathrm{AV}(g^2)$, with $g = x^4 - 2x^3 - 7x^2 - 22x + 121$ are not principally polarizable. Note that g is irreducible and it corresponds to an ordinary isogeny class of abelian surfaces over $\mathbb{F}_{11}$. Define $K = \mathbb{Q}[x]/(g)$ and $\alpha = x \bmod g$ and put $R = \mathbb{Z}[\alpha, \overline{\alpha}]$. The only over-order of R is the maximal order $\mathscr{O}_K$ of K and, since R is Gorenstein by [7, Theorem 11] we get that R is Bass. We computed that $\mathrm{Pic}(R) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Pic}(\mathscr{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$. One can verify that the classes of

$$I = 31R + (7 + 12\alpha - \alpha^2)R \text{ and } J = 6734R + (2053 - \alpha - \alpha^2)R$$

generate $\mathrm{Pic}(R)$ and that the class of $J\mathcal{O}_K$ is the generator of $\mathrm{Pic}(\mathcal{O}_K)$. Using Theorem 4.1 we can list the 8 isomorphism classes of module in $\mathscr{B}(2)$:

$$M_1 = R \oplus R \qquad M_5 = R \oplus \mathcal{O}_K$$
$$M_2 = R \oplus I \qquad M_6 = R \oplus J\mathcal{O}_K$$
$$M_3 = R \oplus J \qquad M_7 = \mathcal{O}_K \oplus \mathcal{O}_K$$
$$M_4 = R \oplus IJ \qquad M_8 = \mathcal{O}_K \oplus J\mathcal{O}_K$$

Again using Theorem 4.1 one can verify that all modules but M_3 and M_4 are self-dual, that is, isomorphic to their own dual. Hence we can deduce that the abelian varieties corresponding via $\mathscr{F}$ to M_3 and M_4 are not principally polarizable and hence cannot be Jacobian of curves. By [16, Theorem 1.3] the isogeny class $\mathrm{AV}(g)$ is not principally polarizable, hence the abelian varieties in $\mathrm{AV}(g^2)$ do not admit a product polarization of degree 1. On the other hand, in view of the fact that $\mathrm{AV}(g^2)$ becomes a 4-th power of an elliptic curve over $\mathbb{F}_{11^2}$, the modules M_i for $i \neq 3, 4$ might still admit a principal polarization. As mentioned in the introduction, the behavior of the machinery developed with respect to field extensions will be investigated in a forthcoming paper.

Example 6.4 For all primes $p \leq 29$ and integers $0 < r \leq 10$ we compute the number $N_{r,p}$ of isomorphism classes of abelian varieties over $\mathbb{F}_p$ that are isogenous to the r-th power of an elliptic curve over $\mathbb{F}_p$. Note that a characteristic polynomial h of such an isogeny class cannot have real roots. Indeed if h has a real roots then $x^2 - p$ divides h and hence an abelian surface with characteristic polynomial $(x^2 - p)^2$, which is necessarily simple, would appear as an isogeny factor.

p	2	3	5	7	11	13	17	19	23	29
$N_{1,p}$	5	8	12	18	22	32	36	42	46	60
$N_{2,p}$	5	9	14	23	25	44	44	55	53	74
$N_{3,p}$	5	10	16	28	28	58	54	68	60	90
$N_{4,p}$	5	11	18	33	31	74	66	81	67	108
$N_{5,p}$	5	12	20	38	34	92	80	94	74	128
$N_{6,p}$	5	13	22	43	37	112	96	107	81	150
$N_{7,p}$	5	14	24	48	40	134	114	120	88	174
$N_{8,p}$	5	15	26	53	43	158	134	133	95	200
$N_{9,p}$	5	16	28	58	46	184	156	146	102	228
$N_{10,p}$	5	17	30	63	49	212	180	159	109	258

Example 6.5 Consider the Klein quartic $\mathscr{K}$ over $\mathbb{F}_2$, which can be represented by the model

$$\mathscr{K} : (X^2 + XZ)^2 + (X^2 + XZ)(Y^2 + YZ) + (Y^2 + YZ)^2 + Z^4 = 0.$$

This model is equation (1.22) in [9] reduced modulo 2. It is known, see for example [9, Sect. 3.3], that $\mathscr{K}$ is isogenous to E^3, where E is an elliptic curve in the isogeny class determined by the Weil polynomial

$$h = x^2 - x + 2.$$

Note that $\mathbb{Z}[x]/h$ is the maximal order of $K = \mathbb{Q}[x]/h$ and that K has class number one. We deduce that E is *super-isolated*, that is, its isogeny class consists of only one isomorphism class. From Theorem 4.1 we deduce that also E^3 is super-isolated and we conclude that the Jacobian $J(\mathscr{K})$ is isomorphic to E^3 (as an unpolarized abelian variety). Explicitly, E is given by

$$E : Y^2 + (X+1)Y = X^3 + 1.$$

The fact that $J(\mathscr{K})$ is isomorphic to the cube of an elliptic curve could also be deduced, with some work, from the discussion on [14, pp. 414-415]. Clearly, such isomorphism is not compatible with the canonical principal polarization of $J(\mathscr{K})$, which is indecomposable, and the product principal polarization of E^3.

Example 6.6 In this example we are able to list all principally polarized abelian varieties in a particular isogeny class of surfaces together with their automorphisms. Consider the isogeny class of elliptic curves over $\mathbb{F}_3$ determined by the Weil polynomial

$$h = x^2 + 2x + 3.$$

The number field $K = \mathbb{Q}[x]/h$ has class number one and the order $\mathbb{Z}[x]/h$ is maximal. We deduce that the isogeny class $\mathrm{AV}(h)$ is super-isolated. We now consider the isogeny class $\mathrm{AV}(h^2)$ which is also super-isolated by Theorem 4.1. From [26, Table 3] we find that $\mathrm{AV}(h^2)$ contains the Jacobian of the hyperelliptic curve

$$\mathscr{H} : Y^2 = X^6 + X^4 + X^2 + 1.$$

From data on curves of genus at most three computed by Jonas Bergström in connection with the article [4] we can deduce that there are only two isomorphism classes of principally polarized abelian varieties in $\mathrm{AV}(h^2)$. The two isomorphism classes are represented by the Jacobian $J(\mathscr{H})$ which has 48 (polarized) automorphisms and the square of the elliptic curve

$$E : Y^2 = X^3 + X^2 + 2$$

together with the product principal polarization, which has exactly 8 polarized automorphisms (the canonical involutions on both factors and the involution coming from swapping the factors).

Authors' contributions

The author would like to thank Jonas Bergström for helpful discussions and for sharing the data used to compute Example 6.6. We are also grateful to Rachel Newton and Christophe Ritzenthaler for comments on a previous version of the paper, which is part of the author's Ph.D thesis [23]. We express our gratitude to the anonymous reviewers of Research in Number Theory for their useful comments and suggestions.

Author details

[1] Matematiska institutionen, Stockholms universitet, 106 91 Stockholm, Sweden, [2] Present address: Mathematisch Instituut, Universiteit Utrecht, P.O. Box 80010, 3508 TA Utrecht, The Netherlands.

Received: 11 January 2019 Accepted: 18 October 2019 Published online: 1 November 2019

References

1. Bass, H.: Torsion free and projective modules. Trans. Am. Math. Soc. **102**, 319–327 (1962)
2. Bass, H.: On the ubiquity of Gorenstein rings. Math. Z. **82**, 8–28 (1963)
3. Borevič, Z.I., Faddeev, D.K.: Representations of orders with a cyclic index. Proc. Steklov Inst. Math. **80**, 56–72 (1968); translation from Trans. Mater. Inst. Steklov **80** 51–65 (1965)

4. Bergström, J., Faber, C., van der Geer, G.: Siegel modular forms of degree three and the cohomology of local systems. Sel. Math. **20**(1), 83–124 (2014)
5. Buchmann, J., Lenstra Jr., H.W.: Approximating rings of integers in number fields. J. Théor. Nr. Bordx. **6**(2), 221–260 (1994)
6. Cohen, H.: Advanced Topics in Computational Number Theory. Graduate Texts in Mathematics, vol. 193. Springer, New York (2000)
7. Centeleghe, T.G., Stix, J.: Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$. Algebra Number Theory **9**(1), 225–265 (2015)
8. Deligne, P.: Variétés abéliennes ordinaires sur un corps fini. Invent. Math. **8**, 238–243 (1969)
9. Elkies, N.D.: The Klein Quartic in Number Theory. The Eightfold Way. Mathematical Sciences Research Institute Publications, pp. 51–101. Cambridge University Press, Cambridge (1999)
10. Gélin, A., Howe, E.W., Ritzenthaler, C.: Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$, ANTS-XIII (Renate Scheidler and Jonathan Sorenson, eds.), vol. 2. In: Proceedings of the Thirteenth Algorithmic Number Theory Symposium, no. 1, pp. 257–274. Mathematical Sciences Publishers, Berkeley (2019)
11. Haefner, J.: Local orders whose lattices are direct sums of ideals. Trans. Am. Math. Soc. **321**(2), 717–740 (1990)
12. Haloui, S.: The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. J. Number Theory **130**(12), 2745–2752 (2010)
13. Haefner, J., Levy, L.S.: Commutative orders whose lattices are direct sums of ideals. J. Pure Appl. Algebra **50**(1), 1–20 (1988)
14. Detlev, W.: Hoffmann, on positive definite Hermitian forms. Manuscr. Math. **71**(4), 399–429 (1991)
15. Honda, Taira: Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Jpn. **20**, 83–95 (1968)
16. Everett, W.: Howe, principally polarized ordinary abelian varieties over finite fields. Trans. Am. Math. Soc. **347**(7), 2361–2401 (1995)
17. Haloui, S., Singh, V.: The Characteristic Polynomials of Abelian Varieties of Dimension 4 Over Finite Fields. Arithmetic, Geometry, Cryptography and Coding Theory. Contemporary Mathematics, pp. 59–68. American Mathematical Society, Providence, RI (2012)
18. Jordan, B.W., Keeton, A.G., Poonen, B., Rains, E.M., Shepherd-Barron, N., Tate, T.: Abelian varieties isogenous to a power of an elliptic curve. Compos. Math. **154**(5), 934–959 (2018)
19. Kani, E.: Products of CM elliptic curves. Collect. Math. **62**(3), 297–339 (2011)
20. Klüners, J., Pauli, S.: Computing residue class rings and Picard groups of orders. J. Algebra **292**(1), 47–64 (2005)
21. Lauter, K.: The maximum or minimum number of rational points on genus three curves over finite fields. Compos. Math. **134**(1), 87–111 (2002). With an appendix by Jean-Pierre Serre
22. Lawrence, S.: Levy and Roger Wiegand, Dedekind-like behavior of rings with 2-generated ideals. J. Pure Appl. Algebra **37**(1), 41–58 (1985)
23. Marseglia, S.: Computing abelian varieties over finite fields. Stockholm University, Stockholm (2018)
24. Marseglia, S.: Computing isomorphism classes of square-free polarized abelian varieties over finite fields. arXiv:1805.10223 (2018)
25. Marseglia, S.: Ideal class monoid of an order and conjugacy classes of integral matrices. arXiv:1805.09671 (2018)
26. Maisner, D., Nart, E.: Abelian surfaces over finite fields as Jacobians. Exp. Math. **11**(3), 321–337 (2002). With an appendix by Everett W. Howe
27. Nazarova, L.A., Roĭter, A.V.: A sharpening of a theorem of Bass. Dokl. Akad. Nauk SSSR **176**, 266–268 (1967)
28. Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent. Math. **2**, 134–144 (1966)
29. The LMFDB Collaboration, The l-functions and modular forms database. http://www.lmfdb.org, (2013). Accessed Sept 16, 2013
30. Waterhouse, W.C., Milne, J.S.: Abelian varieties over finite fields. 1969 Number Theory Institute. In: Proceedings of Symposium Pure Mathematics, Vol. XX, State University New York, Stony Brook, 1969, pp. 53–64. American Mathematics Society, Providence, RI (1971)

Publisher's Note