International Journal of Number Theory
Vol. 18, No. 9 (2022) 1957–1974

DOI: 10.1142/S1793042122501007

Computing base extensions of ordinary abelian varieties over finite fields

Stefano Marseglia

Mathematisch Instituut, Universiteit Utrecht
Postbus 80010, 3508 TA Utrecht, The Netherlands
s.marseglia@uu.nl

Received 4 August 2021
Accepted 10 February 2022
Published 28 April 2022

We study base field extensions of ordinary abelian varieties defined over finite fields using the module theoretic description introduced by Deligne. As applications we give algorithms to determine the minimal field of definition of such a variety and to determine whether two such varieties are twists.

Keywords: Abelian varieties; finite fields; field extension.

Mathematics Subject Classification 2020: 14K15, 14G15, 11G25, 11G10

1. Introduction

Abelian varieties over $\mathbb{C}$ can easily be described in terms of tori. Indeed for a complex abelian variety A of dimension d we have an isomorphism $A(\mathbb{C}) \simeq \mathbb{C}^d/L$, where L is a $\mathbb{Z}$-lattice of rank $2d$. This association does not hold on the whole category of abelian varieties when we move to the wilder realms of positive characteristic. The reason is that there are objects such as the supersingular elliptic curves with quaternionic endomorphism algebra, which does not admit a two-dimensional representation over $\mathbb{Q}$.

Nevertheless, if we restrict our attention to the ordinary abelian varieties (that is, having p-torsion of maximal rank) over a finite field $\mathbb{F}_q$ of characteristic p, then we can still mimic the result from the complex world. More precisely, Deligne in [6] proved that the category $\mathrm{AV}^{\mathrm{ord}}(q)$ of ordinary abelian varieties over $\mathbb{F}_q$ is equivalent to the category $\mathcal{M}^{\mathrm{ord}}(q)$ of $\mathbb{Z}$-modules with a "Frobenius endomorphism". We recall the precise statement of Deligne's theorem in Sec. 2.

Fix an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$, which by Honda–Tate theory is uniquely determined by a q-Weil polynomial h. The subcategory $\mathcal{M}(h)$ of modules in $\mathcal{M}^{\mathrm{ord}}(q)$ whose characteristic polynomial of Frobenius is h, under some assumptions on h, becomes easy to describe in terms of categories of modules and

fractional ideals overorders in product of number fields. Such descriptions are given in [17, 19] and are recalled in Theorem 5.3.

In this paper, we use these module-theoretic descriptions and the related computational tools to study the functor associating to an abelian variety A in $\mathrm{AV}^{\mathrm{ord}}(q)$ its base extension $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ in $\mathrm{AV}^{\mathrm{ord}}(q^r)$, for a fixed positive integer r. In particular, if A is a simple abelian variety in $\mathrm{AV}^{\mathrm{ord}}(q)$ with characteristic polynomial of Frobenius h, then the characteristic polynomial of $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ will be of the form g^s for some irreducible q^r-Weil polynomial and positive integer s, as we recall in Sec. 3. See also Remark 4.3 for a generalization to non-simple abelian varieties.

Section 4 contains the main results of the paper, namely Theorem 4.1 and Corollary 4.2 which describe the functor $- \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} : \mathrm{AV}(h) \to \mathrm{AV}(g^s)$ in terms of a functor $\mathcal{E}_2$ defined on the category of modules. The definition of $\mathcal{E}_2$ is well suited for computations on the isomorphism level, as we explain in detail in Sec. 5. In particular, it allows us to explicitly compute twists of abelian varieties and their (minimal) fields of definition. These two applications are discussed in Secs. 6–8. The algorithms developed, which are available on the webpage of the author, allow us to compute explicit examples, which we include in the various sections of the paper. In particular, see Examples 5.5, 6.3, 6.4, 7.5, 8.1, 8.3–8.5.

It is worth mentioning that there are other descriptions of subcategories of the category of abelian varieties over finite fields in terms of modules with extra structure other than the one of Deligne. More precisely [3] deals only with abelian varieties over prime fields $\mathbb{F}_p$, while in [15, Appendix; 11, 12] discuss functors on categories of abelian varieties isogenous to powers of elliptic curves. Moreover, in [26] the author studies the behavior of the functor introduced in [11] in relation to Galois field extensions. An equivalence of categories for almost ordinary simple abelian varieties over finite fields of odd characteristic similar to one of Deligne has been described in [21]. We chose to work with Deligne's equivalence because it allows us to deduce results also about powers of abelian varieties of dimension greater than 1.

2. Preliminaries

Let $\mathrm{AV}^{\mathrm{ord}}(q)$ be the category of ordinary abelian varieties over $\mathbb{F}_q$. Consider the category $\mathcal{M}^{\mathrm{ord}}(q)$ consisting of pairs (T, F) where T is a finitely generated free $\mathbb{Z}$-module and F is an endomorphism of T such that

- $F \otimes \mathbb{Q}$ is semisimple with eigenvalues of complex absolute value $\sqrt{q}$.
- The characteristic polynomial h of F is ordinary, that is, exactly half of the roots of h are p-adic units and
- There exists an endomorphism V of T such that $FV = q$.

Theorem 2.1 ([6, Théorème]). *There is an equivalence of categories*

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

If $\mathcal{F}^{\mathrm{ord}}(A) = (T, F)$ *then* $\mathrm{rank}_{\mathbb{Z}}(T) = 2\dim(A)$ *and* F *corresponds to the Frobenius endomorphism of* A.

Let A be an abelian variety over $\mathbb{F}_q$. Denote by h_A the characteristic polynomial of Frobenius of A. Recall that h_A is a q-Weil polynomial, that is, a monic polynomial of even degree with integer coefficients and with complex roots of absolute value equal to $\sqrt{q}$. By Honda–Tate theory, the polynomial h_A uniquely determines the isogeny class of A, in the sense that, for an abelian variety B over $\mathbb{F}_q$,

$$A \sim_{\mathbb{F}_q} B \Leftrightarrow h_A = h_B,$$

where h_B is the characteristic polynomial of the Frobenius of B, see [24]. Moreover, by [8, 25], one can use q-Weil polynomials to list all isogeny classes of abelian varieties over $\mathbb{F}_q$ of given dimension.

Let h be the characteristic polynomial of Frobenius of an ordinary abelian variety over $\mathbb{F}_q$ and let $\mathrm{AV}(h)$ be the full subcategory of $\mathrm{AV}^{\mathrm{ord}}(q)$ consisting of abelian varieties in the isogeny class determined by h. Denote by $\mathcal{M}(h)$ the image of $\mathrm{AV}(h)$ under $\mathcal{F}^{\mathrm{ord}}$.

For a squarefree q-Weil polynomial $g \in \mathbb{Z}[x]$ we put $K_g = \mathbb{Q}[x]/(g)$ and $\alpha = x \bmod g$. Let R_g be the order $\mathbb{Z}[\alpha, q/\alpha]$ in K_g and denote by $\mathcal{B}(g, s)$ the category of torsion free R_g-modules M of rank s, that is, such that $M \otimes K_g \simeq K_g^s$. In what follows, we will always think of such a module as embedded in K_g^s. Note that the objects of the category $\mathcal{B}(g, 1)$ are just fractional R_g-ideals.

Theorem 2.2 ([17, Theorem 4.1]). *Assume that* $h = g^s$ *for some squarefree polynomial* g. *There is an equivalence of categories*

$$\mathcal{G}_h : \mathcal{M}(h) \to \mathcal{B}(g, s).$$

We briefly describe the functor $\mathcal{G}_h$. Given a pair $(T, F) \in \mathcal{M}(h)$ we have a natural identification between R_g and $\mathbb{Z}[F, V]$ given by $\alpha \mapsto F$, which induces an R_g-module structure on T. Denote by M this module and set $\mathcal{G}_h((T, F)) = M$.

Definition 2.3. The functor $\mathcal{F}_h : \mathrm{AV}(h) \to \mathcal{B}(g, s)$ is defined as the composition $\mathcal{G}_h \circ \mathcal{F}^{\mathrm{ord}}$.

3. Isogeny Classes and Field Extensions

Let A be an abelian variety over $\mathbb{F}_q$ of dimension g, let $h = h_A$ be the characteristic polynomial of Frobenius of A. Let r be a positive integer and put $A_r = A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ and denote by h_r the characteristic polynomial of Frobenius of A_r. Explicitly, if $\dim(A) = d$ and

$$h = (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_{2d})$$

over the complex numbers, then

$$h_r = (x - \alpha_1^r) \cdot \cdots \cdot (x - \alpha_{2d}^r).$$

One has $h_r \in \mathbb{Z}[x]$ and, in particular, h_r is a q^r-Weil polynomial of degree $2d$. All these results are well known, see, for example, [23, Theorem 5.1.15].

Recall that an abelian variety A is isotypic if A is isogenous to B^n for some simple abelian variety B and positive integer n.

Proposition 3.1 ([4, Proposition 1.2.6.1]). *If A is isotypic then A_r is isotypic for every $r \geq 1$.*

The statement does not hold over an arbitrary field, see [4, Example 1.2.6]. Also, the converse does not hold: if A_r is isotypic then A does not need to be so, as the next example shows.

Example 3.2. If A is an abelian surface over $\mathbb{F}_{31}$ with characteristic polynomial

$$h_A = (x^2 - 3x + 31)(x^2 + 3x + 31)$$

then A is isogenous to the product of two non-isogenous elliptic curves E_1 and E_2. On the other hand E_1 and E_2 become isogenous over $\mathbb{F}_{31^2}$ and indeed the characteristic polynomial of $A_2 = A \otimes \mathbb{F}_{31^2}$ is

$$h_{A_2} = (x^2 + 53x + 961)^2.$$

An isotypic abelian variety A over $\mathbb{F}_q$ has characteristic polynomial of Frobenius of the form $h = g^s$, where g is an irreducible q-Weil polynomial. The next result is well known and we include a proof for completeness.

Proposition 3.3. *Let h be the characteristic polynomial of Frobenius of a simple ordinary abelian variety A over $\mathbb{F}_q$. Then for every $r > 0$ we have $h_r = g^s$ for some irreducible polynomial g and some positive integer s, both depending on r. Moreover, $s = 1$ if and only if A_r is simple.*

Proof. Recall that a simple ordinary abelian variety has an irreducible characteristic polynomial, see [9, Theorem 3.3]. By Proposition 3.1, the extension A_r is isotypic, which is isogenous to B^s for some positive integer s and some simple ordinary abelian variety B over $\mathbb{F}_{q^r}$. Let g be the characteristic polynomial of Frobenius of B. Note that g is irreducible. Then $h_r = g^s$, as required. The last statement follows immediately. □

4. Isomorphism Classes and Field Extensions

Let h be the characteristic polynomial of a simple ordinary abelian variety A over $\mathbb{F}_q$ and h_r the characteristic polynomial of $A_r = A \otimes \mathbb{F}_{q^r}$. By Proposition 3.3, we know that $h_r = g^s$ for some irreducible polynomial g. Put $K_g = \mathbb{Q}[x]/(g)$ and $K_h = \mathbb{Q}[x]/(h)$, and denote by α_g and α_h the classes of x modulo g and modulo h, respectively. Define

$$R_g = \mathbb{Z}[\alpha_g, q^r/\alpha_g] \subset K_g \quad \text{and} \quad R_h = \mathbb{Z}[\alpha_h, q/\alpha_h] \subset K_h.$$

Since h is irreducible, by Theorem 2.2 the abelian varieties isogenous to A correspond via the functor $\mathcal{F}_h$ to the fractional ideals of the order R_h and the abelian varieties isogenous to A_r functorially correspond to the modules in $\mathcal{B}(g,s)$. We want to understand how the functor $-\otimes_{\mathbb{F}_q}\mathbb{F}_{q^r}$ acts on these categories.

The field K_g is naturally a subfield of K_h where the inclusion is given by $\alpha_g \mapsto \alpha_h^r$. Equivalently, we have that K_h is a field extension of degree

$$[K_h : K_g] = \frac{\deg(h)}{\deg(g)} = s.$$

So in particular there exists a polynomial $l \in K_g[y]$ of degree s such that

$$\begin{array}{ccc} K_g & \hookrightarrow & K_h \\ & \searrow & \uparrow \simeq \varphi \\ & & \dfrac{K_g[y]}{(l)} \end{array}$$

where the isomorphism φ is given by

$$\begin{aligned} \overline{y} &\mapsto \alpha_h, \\ \alpha_g &\mapsto \alpha_h^r, \end{aligned}$$

where $\overline{y} = y \bmod l$. Observe that

$$\frac{K_g[y]}{(l)} = K_g \oplus \overline{y}K_g \oplus \cdots \oplus \overline{y}^{s-1}K_g$$

and that there is a natural isomorphism of R_g-modules

$$\begin{aligned} \psi : K_g \oplus \overline{y}K_g \oplus \cdots \oplus \overline{y}^{s-1}K_g &\xrightarrow{\sim} \overbrace{K_g \times \cdots \times K_g}^{s\text{-times}} \\ \sum_{i=0}^{s-1} b_i \overline{y}^i &\mapsto (b_0, \ldots, b_{s-1}). \end{aligned}$$

Consider the functors

$$\begin{aligned} \mathcal{E}_1 : \mathcal{M}(h) &\to \mathcal{M}(h_r) \\ (T, F) &\mapsto (T, F^r) \end{aligned}$$

and

$$\begin{aligned} \mathcal{E}_2 : \mathcal{B}(h,1) &\to \mathcal{B}(g,s) \\ I &\mapsto \psi(\varphi^{-1}(I)), \end{aligned}$$

the action on morphisms being the obvious one. Let $\mathcal{G}_h : \mathcal{M}(h) \to \mathcal{B}(h,1)$ and $\mathcal{G}_{h_r} : \mathcal{M}(h_r) \to \mathcal{B}(g,s)$ be defined as in Theorem 2.2.

Theorem 4.1. *We have a commutative diagram of functors*:

$$\begin{array}{ccccc}
 & & \overset{\mathcal{F}_h}{\frown} & & \\
\mathrm{AV}(h) & \xrightarrow[\mathcal{F}^{\mathrm{ord}}]{} & \mathcal{M}(h) & \xrightarrow[\mathcal{G}_h]{} & \mathcal{B}(h,1) \\
{\scriptstyle -\otimes\mathbb{F}_{q^r}}\downarrow & & \downarrow{\scriptstyle \mathcal{E}_1} & & \downarrow{\scriptstyle \mathcal{E}_2} \\
\mathrm{AV}(h_r) & \xrightarrow{\mathcal{F}^{\mathrm{ord}}} & \mathcal{M}(h_r) & \xrightarrow{\mathcal{G}_{h_r}} & \mathcal{B}(g,s) \\
 & & \underset{\mathcal{F}_{h_r}}{\smile} & &
\end{array}$$

Proof. Let A be an abelian variety in $\mathrm{AV}(h)$ and put $\mathcal{F}^{\mathrm{ord}}(A) = (T, F)$. As usual denote $A \otimes \mathbb{F}_{q^r}$ by A_r. Then $\mathcal{F}^{\mathrm{ord}}(A_r) = (T, F^r)$ which proves the commutativity of the left square of the diagram. The commutativity of the right square follows from the above discussion. □

A straightforward generalization of the previous result leads to the following corollary.

Corollary 4.2. *Let t be a positive integer. We have a commutative diagram of functors*:

$$\begin{array}{ccccc}
 & & \overset{\mathcal{F}_{h^t}}{\frown} & & \\
\mathrm{AV}(h^t) & \xrightarrow[\mathcal{F}^{\mathrm{ord}}]{} & \mathcal{M}(h^t) & \xrightarrow[\mathcal{G}_{h^t}]{} & \mathcal{B}(h,t) \\
{\scriptstyle -\otimes\mathbb{F}_{q^r}}\downarrow & & \downarrow{\scriptstyle \mathcal{E}_1} & & \downarrow{\scriptstyle \mathcal{E}_2} \\
\mathrm{AV}(h_r^t) & \xrightarrow{\mathcal{F}^{\mathrm{ord}}} & \mathcal{M}(h_r^t) & \xrightarrow{\mathcal{G}_{h_r^t}} & \mathcal{B}(g,ts) \\
 & & \underset{\mathcal{F}_{h_r^t}}{\smile} & &
\end{array}$$

Remark 4.3. In this section, and in the following ones, we assume that the q-Weil polynomial h is irreducible, that is, that $\mathrm{AV}(h)$ is a simple isogeny class. If we relax this assumption and instead assume that h is squarefree then the extension $\mathrm{AV}(h_r)$ might fail to be a "pure power". More precisely, if $A \in \mathrm{AV}(h)$ has isogeny decomposition

$$A \sim_{\mathbb{F}_q} B_1 \times \cdots \times B_t,$$

where $B_1, \ldots, B_t$ are simple abelian varieties over $\mathbb{F}_q$, then

$$A_r \sim_{\mathbb{F}_{q^r}} C_1^{s_1} \times \cdots \times C_{t'}^{s_{t'}}, \qquad (*)$$

where $C_1, \ldots, C_{t'}$ are simple abelian varieties over $\mathbb{F}_{q^r}$ and $s_1, \ldots, s_{t'}$ are positive integers, not necessarily equal. Nevertheless, we can still apply all the results developed in this section and in the following ones if we assume that $h_r = g^s$ for a squarefree q^r-Weil polynomial, that is, in $(*)$ we have $s_1 = \cdots = s_{t'} = s$.

5. Computations in $\mathcal{B}(g, s)$

Let the notation be as in Sec. 4. In this section, first, we describe how to compute representatives of the isomorphism classes of $\mathcal{B}(g, s)$ and the functor $\mathcal{E}_2$ in the cases when h_r is irreducible or the order R_g is Bass, see Secs. 5.1 and 5.2, respectively. In practice, most isogeny classes $\mathrm{AV}(h_r)$ fall into one of these two cases.

Second, in Sec. 5.3, we focus on the problem of determining when two modules in $\mathcal{B}(g, s)$ are isomorphic. We present efficient solutions to the problem in the cases described in Secs. 5.1 and 5.2. Moreover, we describe a general method to solve the isomorphism problem for modules in $\mathcal{B}(g, s)$, which in practice turns out to be slower than the previous two, and cannot be used to list the representatives of the isomorphism classes.

Finally, in Sec. 5.4, we give examples of computations of base field extension of abelian varieties.

5.1. *Isomorphism classes when h_r is irreducible*

Assume that the polynomial h_r is irreducible, that is, $h_r = g$ or equivalently $s = 1$. We fix once and for all an isomorphism $K_h \simeq K_g$. This allows us to identify R_g with a finite index order contained in R_h and consequently we can identify the objects of the category $\mathcal{B}(g, 1)$ with fractional R_g-ideals. Moreover, the operation of ideal multiplication induces the structure of a commutative monoid on $\mathcal{B}(g, 1)$. The set of ideal classes inherits such a structure: we call it the *ideal class monoid* of R_g and denote it by $\mathrm{ICM}(R_g)$. In [18], we give an effective algorithm to compute $\mathrm{ICM}(R_g)$. Moreover, it is easy to determine if two fractional R_g-ideals I_1 and I_2 define the same class in $\mathrm{ICM}(R_g)$. Recall the definition of *colon ideal*

$$(I_1 : I_2) = \{a \in K_g : aI_2 \subseteq I_1\}.$$

Theorem 5.1 ([18, Corollary 4.5]). *The fractional R_g-ideals I_1 and I_2 are isomorphic if and only if the following two conditions hold*:

(1) $1 \in (I_1 : I_2)(I_2 : I_1)$;
(2) *The fractional ideal $(I_1 : I_2)$ is a principal $(I_1 : I_1)$-ideal.*

If Part (1) of Theorem 5.1 is satisfied then $(I_1 : I_2)$ is an invertible fractional $(I_1 : I_1)$-ideal, and there are well-known algorithms to check whether it is principal. See also [18, Algorithm 5].

Remark 5.2. Observe that the ideal class monoid of the maximal order coincides with the class group. In particular, if $R_g = \mathcal{O}_{K_g}$ then the number of isomorphism classes of abelian varieties in $\mathrm{AV}(g)$ is just the class group of K_g.

5.2. *Isomorphism classes when R_g is Bass*

Recall that an order S in a number field K is *Bass* if every overorder is Gorenstein, or equivalently, if the maximal order $\mathcal{O}_K$ has cyclic index in S, that is, the

finite S-module $\mathcal{O}_K/S$ is cyclic. For the proofs of these statements and other equivalent definitions, see, for instance, [16, Theorem 2.1]. Examples of Bass orders are maximal orders and orders in quadratic number fields.

If the order R_g is Bass, the modules in $\mathcal{B}(g,s)$ can be written up to R_g-linear isomorphism as a direct sum of fractional R_g-ideals. More precisely, we have the following theorem, see [1] or [2].

Theorem 5.3. *Assume that R_g is a Bass order and let M be in $\mathcal{B}(g,s)$. Then there are fractional R_g-ideals $J_1,\dots,J_s$ satisfying*

$$(J_1 : J_1) \subseteq \cdots \subseteq (J_s : J_s)$$

and elements $v_1,\dots,v_s$ in M such that

$$M = J_1 v_1 \oplus \cdots \oplus J_s v_s.$$

Moreover, given another module N in $\mathcal{B}(g,s)$ with decomposition

$$N = I_1 u_1 \oplus \cdots \oplus I_s u_s,$$

we have that M and N are R_g-isomorphic if and only if

$$(J_k : J_k) = (I_k : I_k)$$

for each k and

$$J_1 \cdot \cdots \cdot J_s \simeq I_1 \cdot \cdots \cdot I_s.$$

Let M be in $\mathcal{B}(g,s)$, with R_g Bass. We can explicitly compute a decomposition

$$M = J_1 v_1 \oplus \cdots \oplus J_s v_s$$

by following the proof of [2, Lemma 7]. For completeness we briefly recall the method. We start with a $\mathbb{Z}$-basis of M

$$M = a_1\mathbb{Z} \oplus \cdots \oplus a_l\mathbb{Z},$$

where $l = \deg h_r = \dim_{\mathbb{Q}} K_g^s$. Let S be the multiplicator ring of M in K_g, that is,

$$S = \{a \in K_g : aM \subseteq M\}.$$

By [2, Lemma 6], there exists $\phi \in \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ such that $a\phi \notin \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ for every $a \in \mathcal{O}_{K_g} \backslash S$. Let $e_1,\dots,e_s$ be the orthogonal idempotents of K_g^s and define v_i in K_g^s to be the dual basis with respect to ϕ, that is, $(e_i\phi)(v_j) = 1$ if $i = j$ and 0 otherwise. Put $v = v_1 + \cdots + v_s$. Now, each element w of M in K_g^s can be written in a unique way as

$$w = \xi v + y$$

for $\xi \in K_g$ and y orthogonal to v. Let I be the subset of coefficients ξ in K_g when w runs over all elements of M. Observe that I is a fractional R_g-ideal and one can

prove that the multiplicator ring of I is S. We then have a decomposition

$$M = Iv \oplus M_1,$$

where M_1 is an object of $\mathcal{B}(g, s-1)$ with multiplicator ring containing S. We can then proceed recursively to obtain the whole decomposition of M.

5.3. *Isomorphism testing*

Let M_1 and M_2 be two modules in $\mathcal{B}(g, s)$. If $s = 1$ we can use [18, Algorithm 5] to check if they are isomorphic. If R_g is Bass, for any $s \geq 1$, we can use the algorithm described in Sec. 5.2 to compute the decompositions of M_1 and M_2 and then conclude by using Theorem 5.3 together with [18, Algorithm 5].

If $s > 1$ and R_g is not Bass we can use the following method. Observe that M_1 and M_2 are isomorphic as R_g-modules if and only if they are so as $\mathbb{Z}[\alpha_g]$-modules, since $\mathbb{Z}[\alpha_g]$ has finite index in R_g. Let m_1 (respectively, m_2) be the matrix that represents multiplication by α_g with respect to any $\mathbb{Z}$-basis of M_1 (respectively, M_2). Observe that m_1 and m_2 are $N \times N$ matrices with integer entries and the same characteristic polynomial g^s and minimal polynomial g, where $N = s \deg(g)$.

Theorem 5.4. *The modules M_1 and M_2 are isomorphic in $\mathcal{B}(g, s)$ if and only if m_1 and m_2 are conjugate over the integers, that is, if there exists a matrix U in $\mathrm{GL}_N(\mathbb{Z})$ such that*

$$m_1 = U m_2 U^{-1}.$$

Proof. The theorem is a direct consequence of generalizations of [14]. Such generalizations can be found in [18, Theorem 8.1] and in [10]. □

The algorithm described in [7] allows us to test whether m_1 and m_2 are conjugate over $\mathbb{Z}$. Such an algorithm has the advantage of being very general, at the cost of being slower than the methods described above for the particular cases when $s = 1$ or R_g is Bass.

5.4. *Applications to abelian varieties*

The algorithms described above allow us to explicitly compute base field extensions of abelian varieties as we show in the next example.

Example 5.5. Consider the polynomial $h = x^6 - x^3 + 8$ corresponding to an isogeny class of ordinary abelian three-folds over $\mathbb{F}_2$. Denote by K_h the number field $\mathbb{Q}[x]/(h)$ and by α_h the class of x in K_h. It turns out that the order $R_h = \mathbb{Z}[\alpha_h, 2/\alpha_h]$ is maximal and has Picard group of order 3 generated by the prime ideal $\mathfrak{p}_h = 2R_h + \alpha_h R_h$. So in particular, by Remark 5.2, there are three isomorphism classes of abelian varieties in this isogeny class, corresponding to R_h, $\mathfrak{p}_h$ and $\mathfrak{p}_h^2$.

We now extend the isogeny class to the field $\mathbb{F}_{2^6}$, which means that we look at the polynomial

$$h_6 = x^6 + 45x^5 + 867x^4 + 9135x^3 + 55488x^2 + 184320x + 262144.$$

Observe that $h_6 = g^3$, where

$$g = x^2 + 15x + 64.$$

Put $K_g = \mathbb{Q}[x]/(g)$, $\alpha_g = x \bmod g$ and $R_g = \mathbb{Z}[\alpha_g, 64/\alpha_g]$. Note that R_g is the maximal order of K_g and that it has a Picard group of order 3 generated by $\mathfrak{p}_g = 2R_g + \alpha_g R_g$. Since R_g is Bass, using Theorem 5.3, we can see that the isomorphism classes of abelian varieties in the isogeny class determined by h_6 correspond to the direct sums in $\mathcal{B}(g, 3)$

$$M_1 = R_g \oplus R_g \oplus R_g,$$

$$M_2 = R_g \oplus R_g \oplus \mathfrak{p}_g,$$

$$M_3 = R_g \oplus R_g \oplus \mathfrak{p}_g^2.$$

Moreover, using the same notation as in Theorem 2.2, we can verify that

$$\mathcal{E}_2(R_h) = M_1,$$

$$\mathcal{E}_2(\mathfrak{p}_h) = M_2,$$

$$\mathcal{E}_2(\mathfrak{p}_h^2) = M_3.$$

6. Twists

Recall that two abelian varieties A and A' over $\mathbb{F}_q$ are twists of each other if there exists some $r > 1$ such that $A_r \simeq_{\mathbb{F}_{q^r}} A'_r$. If this is the case we say that A and A' are r-twists. We say that A' is a trivial twist of A if $A \simeq_{\mathbb{F}_q} A'$.

Assume now that A and A' are simple and ordinary. A necessary condition for A and A' to be r-twists is $h_{A_r} = h_{A'_r}$. For simplicity of exposition we assume that A and A' are isogenous, say both in $\mathrm{AV}(h)$. See Remark 6.2 for an explanation about how to adapt the method descried to the general case.

Proposition 6.1. *Let A and A' be simple and ordinary abelian varieties, both in the isogeny class $\mathrm{AV}(h)$. Let $r > 1$ and write $h_r = g^s$, with g irreducible.*

(1) *The abelian varieties A_r and A'_r are isomorphic if and only if $\mathcal{F}_{h_r}(A_r)$ and $\mathcal{F}_{h_r}(A'_r)$ are isomorphic in $\mathcal{B}(g, s)$.*
(2) *Moreover, if $s = 1$, that is, h_r is irreducible then A_r and A'_r are isomorphic if and only if A and A' are.*

Proof. Part (1) follows from Theorem 4.1. To prove (2) observe that if $h_r = g$ then the inclusion $K_g \hookrightarrow K_h$ given by $\alpha_g \mapsto \alpha_h^r$ (discussed in Sec. 4) is an isomorphism.

This implies that the functor $\mathcal{E}_2 : \mathcal{B}(h,1) \to \mathcal{B}(h_r,1)$ from Theorem 4.1 is fully faithful and hence

$$\mathrm{Hom}_{\mathbb{F}_q}(A, A') \simeq \mathrm{Hom}_{\mathbb{F}_{q^r}}(A_r, A'_r). \qquad \square$$

We can use the results contained in Sec. 5.3 in order to test the isomorphisms of Proposition 6.1, that is, we have an algorithm to test whether two abelian varieties given as modules in the appropriate category $\mathcal{B}(h,1)$ are r-twists, for a fixed $r > 0$. The implementation of such an algorithm is available on the author's webpage.

Remark 6.2. The assumption that A and A' are isogenous is made to simplify the exposition. If A and A' are r-twists but not necessarily isogenous, say $A \in \mathrm{AV}(h)$ and $A' \in \mathrm{AV}(h')$ with $h_r = h'_r$, then we can still use the theory developed in the previous sections to explicitly compute the corresponding modules and isomorphisms, but we will have to work with the two functors $\mathcal{F}_{h_r} : \mathrm{AV}(h_r) \to \mathcal{B}(g,s)$ and $\mathcal{F}_{h'_r} : \mathrm{AV}(h'_r) \to \mathcal{B}(g,s)$. The implementation of our algorithms includes this case and it is demonstrated in Example 7.5.

In the reminder of this section, we give examples of concrete computations.

Example 6.3. Let $h = x^4 - 205x^2 + 103^2$ and consider the isogeny class of ordinary simple abelian surfaces $\mathrm{AV}(h)$ over $\mathbb{F}_{103}$. Note that R_h is maximal. Hence by Remark 5.2, in $\mathrm{AV}(h)$ there are 12 isomorphism classes which are represented by the fractional R_h-ideals

$$\mathfrak{p}_3^i \mathfrak{p}_5^j$$

for $i = 0, 1$ and $j = 0, \ldots, 5$, where $\mathfrak{p}_3$ is the unique prime of R_h above 3 and $\mathfrak{p}_5 = (5, 1 + \alpha_h)$. Observe that $h_2 = g^2$, where $g = x^2 - 205x + 103^2$. Moreover, by looking at the square roots of the roots of h_2 one can easily verify that there is no 103-Weil polynomial other than h whose extension gives h_2. The order R_g is maximal and has cyclic Picard group of order 6, generated by the class of $\mathfrak{P} = (5, -1 + \alpha_g)$. In particular, the objects of $\mathcal{B}(g,2)$ can be represented by

$$R_g \oplus \mathfrak{P}^k \quad \text{for } k = 0, \ldots, 5.$$

Using the methods described in Sec. 5.3 we compute

$$\mathcal{E}_2(\mathfrak{p}_5^j) \simeq \mathcal{E}_2(\mathfrak{p}_3\mathfrak{p}_5^j) \simeq R_g \oplus \mathfrak{P}^j \quad \text{for } j = 0, \ldots, 5.$$

This tells us that for each $j = 0, \ldots, 5$ the only nontrivial two-twist of the abelian variety corresponding to $\mathfrak{p}_5^j$ is the abelian variety corresponding to $\mathfrak{p}_3\mathfrak{p}_5^j$. In other words, if we denote by $A_{i,j}$ the abelian variety such that $\mathcal{F}_h(A_{i,j}) = \mathfrak{p}_3^i\mathfrak{p}_5^j$ then we have

$$A_{0,j} \otimes_{\mathbb{F}_{103}} \mathbb{F}_{103^2} \simeq A_{1,j} \otimes_{\mathbb{F}_{103}} \mathbb{F}_{103^2}.$$

Example 6.4. Let $h = x^4 - 18x^2 + 169$ and $g = x^2 - 18x + 169$. The isogeny class $\mathrm{AV}(h)$ of abelian surfaces over $\mathbb{F}_{13}$ extends to the isogeny class $\mathrm{AV}(g^2)$. By

looking at the complex roots of the polynomial g, one can easily check that h is the only 13-Weil polynomial for which this happens. The order R_h is not Bass and it has three proper overorders:

$$S := R_h + \left(\frac{1+\alpha_h^2}{2} + \frac{\alpha_h^2 - 5}{26}\alpha_h\right)R_h,$$

$$T := R_h + \frac{\alpha_h^2 - 5}{26}\alpha_h R_h,$$

and the maximal order $\mathcal{O}_{K_h}$. Among these orders, the only non-Gorenstein one is S. One computes using the methods described in Sec. 5.1 that the 12 isomorphism classes of $\mathcal{B}(h,1)$ are represented by the following set of ideals:

$$\left\{R_h, I, I^2, I^3, S, IS, S^t, IS^t, T, IT, \mathcal{O}_{K_h}, I\mathcal{O}_{K_h}\right\},$$

where I is a generator of $\mathrm{Pic}(R_h) \simeq \mathbb{Z}/4\mathbb{Z}$ and S^t is the trace dual ideal of S, that is,

$$S^t = \left\{z \in K_h : \mathrm{Tr}_{K_h/\mathbb{Q}}(zS) \subseteq \mathbb{Z}\right\}.$$

The order R_g is Bass and has only one proper overorder, the maximal order $\mathcal{O}_{K_g}$. Observe that by [17, Corollary 4.3] we have that each abelian variety in $\mathrm{AV}(g^2)$ is isomorphic to a product of isogenous elliptic curves. We have $\mathrm{Pic}(R_g) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We denote by $\mathfrak{I}$ the generator isomorphic to any of the two prime ideals above 47 and by $\mathfrak{A}$ the other generator. The isomorphism classes of modules in $\mathcal{B}(g,s)$ are represented by

$$M_1 = R_g \oplus R_g, \quad M_2 = R_g \oplus \mathfrak{I},$$

$$M_3 = R_g \oplus \mathfrak{A}, \quad M_4 = R_g \oplus \mathfrak{I}\mathfrak{A},$$

$$M_5 = R_g \oplus \mathcal{O}_{K_g}, \quad M_6 = R_g \oplus \mathfrak{I}\mathcal{O}_{K_g},$$

$$M_7 = \mathcal{O}_{K_g} \oplus \mathcal{O}_{K_g}, \quad M_8 = \mathcal{O}_{K_g} \oplus \mathfrak{I}\mathcal{O}_{K_g}.$$

We compute that the following isomorphisms of R_g-modules hold:

$$M_2 \simeq \mathcal{E}_2(I) \simeq \mathcal{E}_2(I^3), \quad M_3 \simeq \mathcal{E}_2(R_h) \simeq \mathcal{E}_2(I^2),$$

$$M_5 \simeq \mathcal{E}_2(IS^t) \simeq \mathcal{E}_2(IS), \quad M_6 \simeq \mathcal{E}_2(S^t) \simeq \mathcal{E}_2(S),$$

$$M_7 \simeq \mathcal{E}_2(IT) \simeq \mathcal{E}_2(\mathcal{O}_{K_h}), \quad M_8 \simeq \mathcal{E}_2(T) \simeq \mathcal{E}_2(I\mathcal{O}_{K_h}),$$

which allows us to identify the two-twists in the isogeny class $\mathrm{AV}(h)$.

Remark 6.5. In Example 6.4, we notice several interesting behaviors. Since the order S is the unique non-Gorenstein overorder of R_g we deduce that it must be CM-conjugate stable, that is, $\overline{S} = S$ and in particular, we have that $\overline{S^t} = S^t$ is not isomorphic to S. This tells us that the abelian variety corresponding to S is not isomorphic to its own dual, which corresponds to $\overline{S^t}$ and in particular, it is not principally polarizable. But the extension $\mathcal{E}_2(S) \simeq M_6$ corresponds to a product of two elliptic curves which has the product principal polarization.

Moreover, since S is not Gorenstein, S^t and S are not even weakly equivalent, that is, there exist a prime $\mathfrak{p}$ of S such that $S^t_{\mathfrak{p}} \not\simeq S_{\mathfrak{p}}$. The notion of weak equivalence was introduced in [5] and in [18] we give effective algorithms to check whether two fractional ideals are weakly equivalent. Since $\mathcal{E}_2(S) \simeq \mathcal{E}_2(S^t)$ we deduce that the weak equivalence class of an abelian variety does not correspond to a geometric invariant of the corresponding abelian varieties.

Also, the abelian varieties corresponding to IT and $\mathcal{O}_{K_h}$ which have, respectively, endomorphism rings isomorphic to T and $\mathcal{O}_{K_h}$ are two-twists.

7. Galois Cohomology

In this section, we explain the connection between the set of isomorphism classes of twists of a given abelian variety and its torsion automorphisms. In the square-free ordinary case, this connection can be made explicit by use of the machinery developed in the previous section, see Corollary 7.4 and Example 7.5.

Put $K = \overline{\mathbb{F}}_p$ and $G = \mathrm{Gal}(K/\mathbb{F}_q)$. Write Fr for the Frobenius element of G. Let A be an abelian variety over $\mathbb{F}_q$ and put $A_K := A \otimes K$. Observe that Fr acts on $\mathrm{Aut}_K(A)$ by the following rule: given $\tau \in \mathrm{Aut}_K(A)$ write ${}^{\mathrm{Fr}}\tau$ for the twisted automorphism of A_K defined by

$$ {}^{\mathrm{Fr}}\tau = (\mathrm{id}_A \otimes \mathrm{Fr}) \circ \tau \circ (\mathrm{id}_A \otimes \mathrm{Fr}^{-1}). $$

Such an action turns $\mathrm{Aut}_K(A)$ into a topological G-module. Recall that a *cocycle* of G with values in $\mathrm{Aut}_K(A)$ is a G-linear map $\varepsilon : G \to \mathrm{Aut}_K(A)$ such that

$$ \varepsilon(g_1 g_2) = \varepsilon(g_1)({}^{g_2}\varepsilon(g_1)), $$

for every $g_1, g_2 \in G$. We denote by $Z^1(G, \mathrm{Aut}_K(A))$ the set of cocycles of G with values in $\mathrm{Aut}_K(A)$. We say that $\varepsilon_1, \varepsilon_2 \in Z^1(G, \mathrm{Aut}_K(A))$ are *cohomologous* if there exists $\sigma \in \mathrm{Aut}_K(A)$ such that

$$ \varepsilon_1(g) = \sigma \varepsilon_2(g) \sigma^{-1}, $$

for every $g \in G$. Observe that being cohomologous defines an equivalence relation on $Z^1(G, \mathrm{Aut}_K(A))$. The corresponding set of equivalence classes is denoted $H^1(G, \mathrm{Aut}_K(A))$.

Denote by $\Theta(A/\mathbb{F}_q)$ the set of $\mathbb{F}_q$-isomorphism classes of twists A' (over $\mathbb{F}_q$) of A. The class of A' in $\Theta(A/\mathbb{F}_q)$ is represented by a geometric isomorphism $\phi : A_K \to A'_K$. Given such $\phi : A_K \to A'_K$ define the map $\varepsilon_\phi : G_{\mathbb{F}_q} \to \mathrm{Aut}_K(A)$ by

$$ \varepsilon_\phi : \alpha \mapsto \phi^{-1} \circ {}^{\alpha}\phi. $$

It is an easy verification that $\varepsilon_\phi \in Z^1(G, \mathrm{Aut}_K(A))$.

Two automorphisms $\tau_1, \tau_2 \in \mathrm{Aut}_K(A)$ are called Fr-*conjugate* if there exists $\sigma \in \mathrm{Aut}_K(A)$ such that

$$ \tau_1 = \sigma^{-1} \tau_2 ({}^{\mathrm{Fr}}\sigma). $$

Being Fr-conjugate is an equivalence relation. Let $\mathcal{S}$ be the set of automorphisms $\tau \in \mathrm{Aut}_K(A)$ such that there exists n for which

(i) ${}^{\mathrm{Fr}^n}\tau = \tau$ and
(ii) $(\tau \cdot {}^{\mathrm{Fr}}\tau \cdots {}^{\mathrm{Fr}^{n-1}}\tau)$ has finite order.

Observe that (i) is equivalent to saying that τ lies in $\mathrm{Aut}_{\mathbb{F}_{q^n}}(A)$ and that the set $\mathcal{S}$ contains $\mathrm{Tors}(\mathrm{Aut}_K(A))$. Denote by $\overline{\mathcal{S}}$ the set of Fr-conjugacy classes of elements of $\mathcal{S}$.

Proposition 7.1. *The maps $\phi \mapsto \varepsilon_\phi$ and $\varepsilon \mapsto \varepsilon(\mathrm{Fr}_q)$ yield bijections*:

$$\Theta(A, \mathbb{F}_q) \to H^1(G_{\mathbb{F}_q}, \mathrm{Aut}_K(A)) \to \overline{\mathcal{S}}.$$

Proof. By [22, Proposition 5, §1.3, Chap. III], the map $\phi \mapsto \varepsilon_\phi$ induces a bijection

$$\Theta(A, \mathbb{F}_q) \to H^1(G_{\mathbb{F}_q}, \mathrm{Aut}_K(A)).$$

Moreover, by [22, §5.1, Chap. I], the map $\varepsilon \mapsto \varepsilon(\mathrm{Fr})$ induces a bijection

$$H^1(G_{\mathbb{F}_q}, \mathrm{Aut}_K(A)) \to \overline{\mathcal{S}}.$$

□

Remark 7.2. Compare Proposition 7.1 with [13, Proposition 3.5; 20, Propositions 5 and 9], where there are analogous results for principally polarized abelian varieties and curves over finite fields, respectively. The main difference with our result is that since we consider unpolarized abelian varieties the automorphism groups are infinite if $\dim(A) > 1$.

Corollary 7.3. *Let A be an abelian variety over $\mathbb{F}_q$ such that $\mathrm{Aut}_K(A) = \mathrm{Aut}_{\mathbb{F}_q}(A)$. Let $\tau \in \mathrm{Tors}(\mathrm{Aut}_{\mathbb{F}_q}(A))$. Assume that τ lies in the center of $\mathrm{Aut}_K(A)$ and has order r. Then there exists a twist $\phi : A_r \to A'_r$ such that if we denote by π and π' the Frobenius endomorphisms of A and A', respectively, we have*

$$\phi^{-1} \circ \pi' \circ \phi = \pi \circ \tau^{-1}. \tag{7.1}$$

In particular, $\pi \circ \tau^{-1}$ and π' have the same characteristic polynomial.

Proof. Since all automorphisms are defined over the base field, Fr-conjugacy coincides with usual conjugacy. Moreover, the conjugacy class of τ contains only τ. By the bijections described in Proposition 7.1, the automorphism τ defines a twist $\phi : A_K \to A'_K$. Since τ is defined over $\mathbb{F}_q$ then for every positive integer n we have

$$\tau \cdot {}^{\mathrm{Fr}}\tau \cdot {}^{\mathrm{Fr}^2}\tau \cdots {}^{\mathrm{Fr}^{n-1}}\tau = \tau^n$$

and hence by [13, Remark 3.7] the twist $\phi : A_K \to A'_K$ is defined over $\mathbb{F}_{q^r}$. Moreover, by [13, Proposition 3.9] the twist $\phi : A_r \to A'_r$ satisfies

$$\phi^{-1} \circ \pi' \circ \phi = \pi \circ \tau^{-1},$$

as required. □

Corollary 7.4. *Let A be a squarefree ordinary abelian variety over $\mathbb{F}_q$. If the simple isogeny factors of A are absolutely simple, then the association*

$$\begin{aligned} \mathrm{Tors}(\mathrm{Aut}_{\mathbb{F}_q}(A)) &\longrightarrow \Theta(A, \mathbb{F}_q), \\ \tau &\longmapsto \phi \end{aligned}$$

of Corollary 7.3 *is a bijection.*

Proof. By the hypothesis on A we have that $\mathrm{Aut}_{\mathbb{F}_q}(A)$ lies in the center of $\mathrm{End}_K(A)$ and $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_K(A)$. Moreover, the set $\overline{\mathcal{S}}$ equals $\mathrm{Tors}(\mathrm{Aut}_{\mathbb{F}_q}(A))$. Proposition 7.1 and Corollary 7.3 yield the desired bijection. □

Corollary 7.4 allow us to identify which twist is induced by τ by means of the relation (7.1), as we show in Example 7.5.

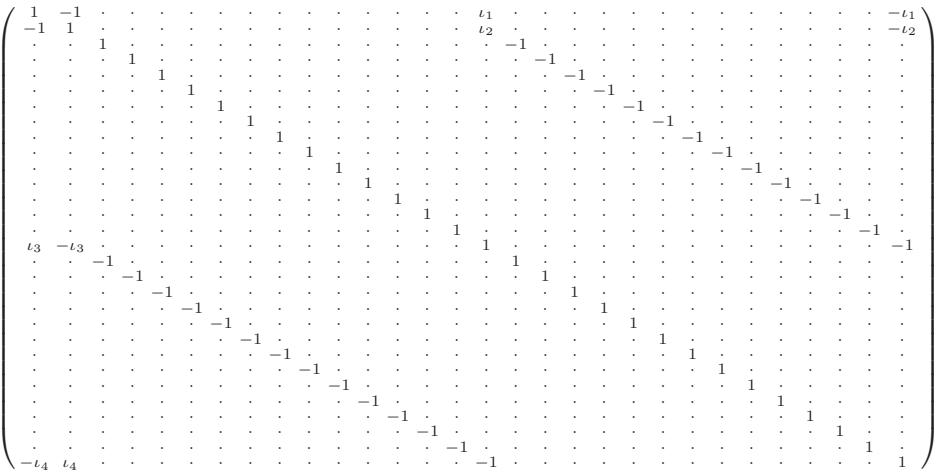
Example 7.5. Consider the 5^4-Weil polynomial

$$h_4 = x^6 - 112x^5 + 5872x^4 - 184786x^3 + 5872 \cdot 5^4 x^2 - 112 \cdot 5^8 x + 5^{12}.$$

The corresponding isogeny class $\mathrm{AV}(h_4)$ can be attained as base field extension of 4 primitive (see the beginning of Sec. 8 for the definition) absolutely simple isogeny classes determined by the following 5-Weil polynomials:

$$\begin{aligned} h^{(1)} &= x^6 + 4x^5 + 12x^4 + 36x^3 + 60x^2 + 100x + 125, \\ h^{(2)} &= x^6 - 4x^5 + 12x^4 - 36x^3 + 60x^2 - 100x + 125, \\ h^{(3)} &= x^6 - 4x^4 - 2x^3 - 20x^2 + 125, \\ h^{(4)} &= x^6 - 4x^4 + 2x^3 - 20x^2 + 125. \end{aligned}$$

The isogeny classes $\mathrm{AV}(h^{(1)}), \mathrm{AV}(h^{(2)}), \mathrm{AV}(h^{(3)})$ and $\mathrm{AV}(h^{(4)})$ contain 1, 1, 14 and 14 isomorphism classes of abelian varieties, respectively. Each isogeny class $\mathrm{AV}(h^{(i)})$ contains a single abelian variety with four distinct torsion automorphisms, which we will denote by $1, -1, \iota_i$ and $-\iota_i$, with orders $1, 2, 4, 4$, respectively. All the other 26 isomorphism classes have only two torsion automorphisms, namely 1 and -1. We do not add a pedix to the automorphisms 1 and -1 since all abelian varieties considered have only one automorphism of order 1, the identity, and one automorphism or order 2, so no confusion can arise. In the following 30×30 matrix in the entry (i, j) we write "$\cdot$" if the ith and jth isomorphism classes are not four-twists and, otherwise, $1, -1$, ι_i or $-\iota_i$ for the torsion automorphism of the ith abelian variety which induces the twist.



8. Field of Definition

Let A be an abelian variety over $\mathbb{F}_q$ and k be a subfield of $\mathbb{F}_q$. We say that A is *defined* over k if there exists an abelian variety A' over k such that $A' \otimes_k \mathbb{F}_q$ is isomorphic to A over $\mathbb{F}_q$. We say that an abelian variety A over $\mathbb{F}_q$ is *primitive* if there is no proper subfield k of $\mathbb{F}_q$ such that A is defined over k. Moreover, for a q-Weil polynomial h, we say that isogeny class $\mathrm{AV}(h)$ is *primitive* if every abelian variety A in $\mathrm{AV}(h)$ is so.

Let h be an irreducible ordinary q-Weil polynomial. By looking at the complex roots of h it is easy to list all q_0-Weil polynomials h_0, with $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$, that give h after a base field extension to $\mathbb{F}_q$. Observe that each such h_0 is irreducible and for any subfield $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$ there might be more than one q_0-Weil polynomial that extends to h.

Example 8.1. The isogeny class of elliptic curves over $\mathbb{F}_{16}$ determined by $h_{16} = x^2 - x + 16$ is not primitive and can be attained as a base extension of the primitive isogeny classes $h_4 = x^2 - 3x + 4$ over $\mathbb{F}_4$ and of both $h_{2,1} = x^2 + x + 2$ and $h_{2,2} = x^2 - x + 2$ over $\mathbb{F}_2$.

Corollary 8.2. *Let h be an irreducible ordinary q-Weil polynomial. Let t be some positive integer. For A in $\mathrm{AV}(h^t)$, consider the R_h-module $M = \mathcal{F}_{h^t}(A)$ in $\mathcal{B}(h,t)$. Let h_0 be a q_0-Weil polynomial that extends to h. The abelian variety A can be defined over $\mathbb{F}_{q_0}$ if and only if M is an R_{h_0}-module, that is, there exists M_0 in $\mathcal{B}(h_0,t)$ such that $\mathcal{E}_2(M_0) \simeq M$.*

Proof. This is a consequence of Corollary 4.2. □

Example 8.3. Using the same notation as in Example 8.1, we fix isomorphisms between $K_{h_{16}}$, K_{h_4}, $K_{h_{2,1}}$ and $K_{h_{2,2}}$ so that we can work in $K_{h_{16}}$, which we will denote by K.

The order $R_{h_{16}}$ has index 3 in the maximal order $\mathcal{O}_K$. Moreover, the images in K of the orders R_{h_4}, $R_{h_{2,1}}$ and $R_{h_{2,2}}$ all equal the maximal order $\mathcal{O}_K$. Since the Picard group of $R_{h_{16}}$ has order 4 and $\mathcal{O}_K$ is a principal ideal domain, we see that there are five isomorphism classes of elliptic curves in $\mathrm{AV}(h_{16})$. The first four have endomorphism ring isomorphic to $R_{h_{16}}$ and so by Corollary 8.2 cannot be defined over any proper subfield of $\mathbb{F}_{16}$. On the other hand, the unique isomorphism class with maximal endomorphism ring can be defined over $\mathbb{F}_4$ or over $\mathbb{F}_2$. It is not hard to determine equations of the representatives of these classes. Write $\mathbb{F}_{16} = \mathbb{F}_2(T)$ and $\mathbb{F}_4 = \mathbb{F}_2(S)$, for $T^4+T+1=0$ and $S^2+S+1=0$. Consider the elliptic curves

$$\begin{aligned} E_{16,i} &: y^2 + xy = x^3 + T^{2i} \in \mathrm{AV}(h_{16}) \quad \text{for } i = 0,1,2,3,4, \\ E_{2,1} &: y^2 + xy = x^3 + 1 \in \mathrm{AV}(h_{2,1}), \\ E_{2,2} &: y^2 + xy + y = x^3 + 1 \in \mathrm{AV}(h_{2,2}), \\ E_4 &: y^2 + xy + Sy = x^3 + S \in \mathrm{AV}(h_4). \end{aligned}$$

We have that $E_{16,0}$ is isomorphic to $E_{2,1} \otimes_{\mathbb{F}_2} \mathbb{F}_{16}$, $E_{2,2} \otimes_{\mathbb{F}_2} \mathbb{F}_{16}$ and $E_4 \otimes_{\mathbb{F}_4} \mathbb{F}_{16}$. We deduce that $E_{16,0}$ has maximal endomorphism ring, while $E_{16,i}$ for $i = 1, \ldots, 4$ represent the isomorphism classes with endomorphism ring isomorphic to R_{16}.

Example 8.4. Consider the situation of Example 6.3. From the computations described, we see that the six isomorphism classes of abelian varieties in $\mathrm{AV}(h_2)$ are extensions of abelian varieties from $\mathrm{AV}(h)$, that is, they can all be defined over $\mathbb{F}_{103}$.

Example 8.5. Consider Example 6.4. Here, we see that not all isomorphism classes in $\mathrm{AV}(h_2)$ are extensions. Indeed the varieties corresponding to the modules M_1 and M_4 cannot be defined over the prime field $\mathbb{F}_{13}$.

Acknowledgments

The author thanks the anonymous referee for carefully reading the paper. The author is grateful to Jonas Bergström and Valentijn Karemaker for their suggestions, and to Christophe Ritzenthaler and Rachel Newton for comments on a preliminary version of the paper, which was included in the author's Ph.D. thesis written at Stockholm University. Part of the research was supported by the Dutch Research Council (NWO), Grant 613.001.651.

References

[1] H. Bass, On the ubiquity of Gorenstein rings, *Math. Z.* **82** (1963) 8–28.
[2] Z. I. Borevič and D. K. Faddeev, Representations of orders with a cyclic index, *Proc. Steklov Inst. Math.* **80** (1968) 56–72; translation from *Tr. Mat. Inst. Steklov* **80** (1965) 51–65.
[3] T. G. Centeleghe and J. Stix, Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$, *Algebra Number Theory* **9**(1) (2015) 225–265.

[4] C.-L. Chai, B. Conrad and F. Oort, *Complex Multiplication and Lifting Problems*, Mathematical Surveys and Monographs, Vol. 195 (American Mathematical Society, Providence, RI, 2014).
[5] E. C. Dade, O. Taussky and H. Zassenhaus, On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field, *Math. Ann.* **148** (1962) 31–64.
[6] P. Deligne, Variétés abéliennes ordinaires sur un corps fini, *Invent. Math.* **8** (1969) 238–243.
[7] B. Eick, T. Hofmann and E. A. O'Brien, The conjugacy problem in $\mathrm{GL}(n, \mathbb{Z})$, *J. Lond. Math. Soc.* (*2*) **100**(3) (2019) 731–756.
[8] T. Honda, Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968) 83–95.
[9] E. W. Howe, Principally polarized ordinary abelian varieties over finite fields, *Trans. Amer. Math. Soc.* **347**(7) (1995) 2361–2401.
[10] D. Husert, Similarity of integer matrices, Ph.D. thesis, University of Paderborn (2016).
[11] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron and J. T. Tate, Abelian varieties isogenous to a power of an elliptic curve, *Compos. Math.* **154**(5) (2018) 934–959.
[12] E. Kani, Products of CM elliptic curves, *Collect. Math.* **62**(3) (2011) 297–339.
[13] V. Karemaker and R. Pries, Fully maximal and fully minimal abelian varieties, *J. Pure Appl. Algebra* **223**(7) (2019) 3031–3056.
[14] C. G. Latimer and C. C. MacDuffee, A correspondence between classes of ideals and classes of matrices, *Ann. of Math.* (*2*) **34**(2) (1933) 313–316.
[15] K. Lauter, The maximum or minimum number of rational points on genus three curves over finite fields, *Compos. Math.* **134**(1) (2002) 87–111. With an appendix by Jean-Pierre Serre.
[16] L. S. Levy and R. Wiegand, Dedekind-like behavior of rings with 2-generated ideals, *J. Pure Appl. Algebra* **37**(1) (1985) 41–58.
[17] S. Marseglia, Computing abelian varieties over finite fields isogenous to a power, *Res. Number Theory* **5**(4) (2019) Paper No. 35.
[18] S. Marseglia, Computing the ideal class monoid of an order, *J. Lond. Math. Soc.* (*2*) **101**(3) (2020) 984–1007.
[19] S. Marseglia, Computing squarefree polarized abelian varieties over finite fields, *Math. Comp.* **90**(328) (2021) 953–971.
[20] S. Meagher and J. Top, Twists of genus three curves over finite fields, *Finite Fields Appl.* **16**(5) (2010) 347–368.
[21] A. Oswal and A. N. Shankar, Almost ordinary abelian varieties over finite fields, *J. Lond. Math. Soc.* (*2*) **101**(3) (2020) 923–937.
[22] J.-P. Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Engl. edition (Springer-Verlag, Berlin, 2002). Translated from the French by Patrick Ion and revised by the author.
[23] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edition, Graduate Texts in Mathematics, Vol. 254 (Springer-Verlag, Berlin, 2009).
[24] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966) 134–144.
[25] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), in *Séminaire Bourbaki. Vol. 1968/69*: *Exposés 347–363*, Lecture Notes in Mathematics, Vol. 175 (Springer, Berlin, 1971), pp. 95–110.
[26] I. Vogt, Abelian varieties isogenous to a power of an elliptic curve over a Galois extension, *J. Théor. Nombres Bordeaux* **31**(1) (2019) 205–213.