European Journal of Mathematics (2021) 7:1124–1136
https://doi.org/10.1007/s40879-021-00460-1

RESEARCH ARTICLE

The structure of the group of rational points of an abelian variety over a finite field

Caleb Springer[1]

Received: 14 June 2020 / Revised: 28 November 2020 / Accepted: 7 February 2021 /
Published online: 23 March 2021

Abstract

Let A be a simple abelian variety of dimension g defined over a finite field $\mathbb{F}_q$ with Frobenius endomorphism π. This paper describes the structure of the group of rational points $A(\mathbb{F}_{q^n})$, for all $n \geqslant 1$, as a module over the ring R of endomorphisms which are defined over $\mathbb{F}_q$, under certain technical conditions. If $[\mathbb{Q}(\pi):\mathbb{Q}] = 2g$ and R is a Gorenstein ring, then $A(\mathbb{F}_{q^n}) \cong R/R(\pi^n - 1)$. This includes the case when A is ordinary and has maximal real multiplication. Otherwise, if Z is the center of R and $(\pi^n - 1)Z$ is the product of invertible prime ideals in Z, then $A(\mathbb{F}_{q^n})^d \cong R/R(\pi^n - 1)$ where $d = 2g/[\mathbb{Q}(\pi):\mathbb{Q}]$. Finally, we deduce the structure of $A(\overline{\mathbb{F}}_q)$ as a module over R under similar conditions. These results generalize results of Lenstra for elliptic curves.

Keywords Abelian variety · Finite field · Endomorphism ring · Rational points

Mathematics Subject Classification 14K15 · 14G15 · 11G10 · 14G05

1 Introduction

Given an abelian variety A over a finite field $\mathbb{F}_q$, one may view the group of rational points $A(\mathbb{F}_q)$ as a module over the ring $\mathrm{End}_{\mathbb{F}_q}(A)$ of endomorphisms defined over $\mathbb{F}_q$. Lenstra completely described this module structure for elliptic curves over finite fields in the following theorem. In addition to being useful and interesting in its own right, this theorem also determines *a fortiori* the underlying abelian group structure of $A(\mathbb{F}_q)$ purely in terms of the endomorphism ring. The latter perspective has been leveraged for the sake of computational number theory and cryptography; see, for example, the

The author was partially supported by National Science Foundation award CNS-1617802.

✉ Caleb Springer
cks5320@psu.edu

[1] Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA

work of Galbraith [6, Lemma 1], Ionica and Joux [8, Section 2.3], and Kohel [12, Chapter 4]. The goal of this paper is to generalize Lenstra's theorem beyond elliptic curves to abelian varieties of arbitrary dimension.

Theorem 1.1 ([13, Theorem 1]) *Let E be an elliptic curve over $\mathbb{F}_q$. Write $R = \mathrm{End}_{\mathbb{F}_q}(E)$ and let $\pi \in R$ be the Frobenius endomorphism of E.*

(a) *Suppose that $\pi \notin \mathbb{Z}$. Then R has rank 2 over $\mathbb{Z}$ and there is an isomorphism of R-modules*

$$E(\mathbb{F}_{q^n}) \cong R/(\pi^n - 1)R.$$

(b) *Suppose that $\pi \in \mathbb{Z}$. Then R has rank 4 over $\mathbb{Z}$, we have*

$$E(\mathbb{F}_{q^n}) \cong \mathbb{Z}/\mathbb{Z}(\pi^n - 1) \oplus \mathbb{Z}/\mathbb{Z}(\pi^n - 1)$$

as abelian groups. Further, this group has up to isomorphism exactly one left R-module structure, and one has an isomorphism of R-modules

$$E(\mathbb{F}_{q^n}) \oplus E(\mathbb{F}_{q^n}) \cong R/R(\pi^n - 1).$$

Notice that E is supersingular in the second case, but not conversely. To prove the theorem, Lenstra notes that $E(\mathbb{F}_{q^n}) = E[\pi^n - 1]$, and $\pi^n - 1$ is a separable isogeny. For part (b), the abelian group structure is simply the well-known structure of the n-torsion of an elliptic curve for $n \in \mathbb{Z}$. The additional statements in part (b) follow from Morita equivalence and an isomorphism of rings, for integers n coprime to q, between R/Rn and the ring $\mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$ of 2×2 matrices with coefficients in $\mathbb{Z}/n\mathbb{Z}$.

For part (a) of the theorem, Lenstra uses the following proposition; see [13, Proposition 2.1].

Proposition 1.2 *Let E be an elliptic curve over $\mathbb{F}_q$, and let $R = \mathrm{End}_{\mathbb{F}_q} E$. If $[R : \mathbb{Z}] = 2$, then for every separable element $s \in R$ there is an isomorphism $E[s] \cong R/Rs$ of R-modules.*

Lenstra showed in his original paper that the preceding proposition does not immediately generalize to all "nice" abelian varieties of higher dimension, i.e., principally polarized ordinary abelian varieties; see [13, Proposition 6.4]. Although this means that a certain natural generalization is not correct, the examples that Lenstra produces must have very particular endomorphism rings. By inspecting Lenstra's theorem through two perspectives and imposing restrictions on the endomorphism ring, we can recover a natural generalization to certain abelian varieties of higher dimension.

1.1 First perspective: Gorenstein rings

First, consider part (a) of Lenstra's theorem, or more generally, Proposition 1.2. In this case, the endomorphism ring of the elliptic curve is commutative, specifically an order in an imaginary quadratic number field. In general, a simple abelian variety A

of dimension g over $\mathbb{F}_q$ with Frobenius endomorphism π has commutative endomorphism ring exactly when $[\mathbb{Q}(\pi):\mathbb{Q}] = 2g$, and in this case, $\mathrm{End}_{\mathbb{F}_q}(A)$ is an order in the field $\mathbb{Q}(\pi)$ [21, Theorem 8]. In fact, if π is an ordinary Weil q-integer, then the rings which arise as the endomorphism rings of abelian varieties in the corresponding isogeny class over $\mathbb{F}_q$ are precisely the orders of $\mathbb{Q}(\pi)$ which contain the minimal order $\mathbb{Z}[\pi, \overline{\pi}]$ [20, Theorem 7.4]. Since every order in a quadratic number field is Gorenstein, restricting to the Gorenstein case for abelian varieties of arbitrary dimension provides us with our first natural generalization.

Proposition 2.1 *Let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g with Frobenius endomorphism π. If $[\mathbb{Q}(\pi):\mathbb{Q}] = 2g$ and $R = \mathrm{End}_{\mathbb{F}_q}(A)$ is a Gorenstein ring, then there is an isomorphism of R-modules*

$$A[s] \cong R/Rs$$

for every separable $s \in R$.

This proposition will be proved in Sect. 2 by using properties of finite local Gorenstein rings. To see examples where the proposition applies, note that $\mathrm{End}_{\mathbb{F}_q}(A)$ is guaranteed to be Gorenstein if A has *maximal real multiplication*, i.e., if $\mathrm{End}_{\mathbb{F}_q}(A)$ contains the ring of integers of the maximal totally real subfield of $\mathbb{Q}(\pi)$; see [3, Lemma 4.4]. Many recent results in the algorithmic study of abelian varieties over finite fields have productively focused on the case of maximal real multiplication, including results on point counting [1,7], isogeny graphs [3,9,15], and endomorphism ring computation [19]. At the other extreme, Centeleghe and Stix have shown that the minimal order $\mathbb{Z}[\pi, \overline{\pi}]$ is also always Gorenstein, where π is a Weil integer [4, Theorem 11].

1.2 Second perspective: modules over the center

Now consider part (b) of Lenstra's theorem, where E is a supersingular elliptic curve over $\mathbb{F}_q$ with all endomorphisms defined. Before describing the group of rational points $E(\mathbb{F}_{q^n})$ as a module over the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(E)$, Lenstra first identifies $E(\mathbb{F}_{q^n})$ as an abelian group, i.e., a module over $\mathbb{Z}$. Importantly, $\mathbb{Z}$ is the center of the endomorphism ring in this case.

Following this point of view, given a simple abelian variety A over $\mathbb{F}_q$ with Frobenius endomorphism π, we will first consider the structure of $A(\mathbb{F}_{q^n})$ as a module of the center of $\mathrm{End}_{\mathbb{F}_q}(A)$. Recall that the center of the endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is the field $\mathbb{Q}(\pi)$ [21, Theorem 8]. More generally, we can study $A[s]$ as a module over the center of the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$ for any separable endomorphism s in the center, which leads us to the following result.

Proposition 3.1 *Let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g, and let Z be the center of $R = \mathrm{End}_{\mathbb{F}_q}(A)$. If s is a separable element of Z for which sZ is the product of invertible prime ideals in Z, then there is an isomorphism of Z-modules*

$$A[s] \cong (Z/Zs)^d$$

where $d = 2g/[\mathbb{Q}(\pi) : \mathbb{Q}]$. Moreover, this Z-module has exactly one R-module structure, up to isomorphism. The unique R-module structure comes from the isomorphism of rings $R/Rs \cong \mathrm{M}_d(Z/Zs)$, and there is an isomorphism

$$A[s]^d \cong R/Rs$$

as R-modules.

This proposition will be proved in Sect. 3 through the study of kernel ideals. The latter parts of this proposition will follow from Morita equivalence, similarly to Theorem 1.1 (b). Notice that we must require that sZ is the product of invertible prime ideals, which is automatically true when Z is a maximal order. For example, let A be an abelian surface defined over $\mathbb{F}_p$ in the isogeny class corresponding to the Weil polynomial $(t^2 - p)^2$ for a prime $p \not\equiv 1 \bmod 4$. This Weil polynomial corresponds to the Weil restriction of a supersingular elliptic curve over $\mathbb{F}_{p^2}$, and A is simple over $\mathbb{F}_p$. The endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(A)$ is a noncommutative ring whose center is $\mathbb{Z}[\sqrt{p}]$, which is a maximal order by construction because $p \not\equiv 1 \bmod 4$. Hence the proposition automatically applies in this case for any separable $s \in \mathbb{Z}[\sqrt{p}]$.

1.3 Main result

Combining the perspectives outlined above, we have the following main result.

Theorem 1.3 *For $g \geqslant 1$, let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g with Frobenius endomorphism π. Write $K = \mathbb{Q}(\pi)$ and $R = \mathrm{End}_{\mathbb{F}_q}(A)$, and let Z be the center of R.*

(a) *If $[K : \mathbb{Q}] = 2g$ and R is a Gorenstein ring, then*

$$A(\mathbb{F}_{q^n}) \cong R/R(\pi^n - 1).$$

(b) *If $(\pi^n - 1)Z$ is the product of invertible prime ideals in Z, then there is an isomorphism of Z-modules*

$$A(\mathbb{F}_{q^n}) \cong (Z/Z(\pi^n - 1))^d,$$

where $d = 2g/[K : \mathbb{Q}]$. Moreover, this Z-module has exactly one left R-module structure, up to isomorphism. This R-module structure comes from the isomorphism of rings $R/R(\pi^n - 1) \cong \mathrm{M}_d(Z/Z(\pi^n - 1))$, and there is an isomorphism of R-modules

$$A(\mathbb{F}_{q^n})^d \cong R/R(\pi^n - 1).$$

Notice that parts (a) and (b) of the theorem provide the same answer in the case when all hypotheses are simultaneously satisfied, e.g. when A is a simple ordinary abelian variety with maximal endomorphism ring. The theorem follows immediately from the propositions above, given that $A(\mathbb{F}_{q^n}) = A[\pi^n - 1]$ and $\pi^n - 1$ is a separable isogeny,

as in the elliptic curve case. Propositions 2.1 and 3.1 will be proved in Sects. 2 and 3, respectively, which completes the proof of our main theorem. Finally, in Sect. 4, we stitch together all of the isomorphisms described above to understand the structure of $A(\overline{\mathbb{F}}_q)$ as a module of the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$.

2 Gorenstein rings

The goal of this section is to prove the following generalization of Proposition 1.2, as outlined in the introduction.

Proposition 2.1 *Let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g with Frobenius endomorphism π. If $[\mathbb{Q}(\pi):\mathbb{Q}] = 2g$ and $R = \mathrm{End}_{\mathbb{F}_q}(A)$ is a Gorenstein ring, then there is an isomorphism of R-modules*

$$A[s] \cong R/Rs$$

for every separable $s \in R$.

In order to prove this proposition, we will follow a strategy that is largely similar to the proof of Theorem 1.1 (a) in Lenstra's original paper. Our approach differs from Lenstra by working directly with finite local Gorenstein rings, rather than using duality. Background for Gorenstein rings can be found in Matsumura's book [16, Chapter 18].

Lemma 2.2 *Let R be a Gorenstein domain and s a nonzero element of R. If the quotient $S = R/Rs$ is finite, then every faithful S-module M contains a submodule that is free of rank 1 over S.*

Proof Notice that S is Gorenstein because R is Gorenstein; see [16, Exercise 18.1]. Additionally, the fact that S is finite implies that it is an Artinian ring. In particular, it is canonically isomorphic to a finite product of its localizations $S = S_1 \times \cdots \times S_r$. Thus every S-module M has the form $M \cong M_1 \times \cdots \times M_r$ where M_i is an S_i-module for each $1 \leqslant i \leqslant r$. This lemma therefore reduces to the following lemma. □

Lemma 2.3 *Let $(T, \mathfrak{m})$ be a finite local Artinian ring that is Gorenstein.*

(a) *Every nonzero ideal $J \subseteq T$ contained in $\mathfrak{m}$ contains a nonzero element that is killed by all elements of $\mathfrak{m}$.*
(b) *Every faithful T-module N contains a submodule that is free of rank 1 over T.*

Proof To prove part (a), list the elements of the maximal ideal $\mathfrak{m} = \{a_1, \ldots, a_d\}$. Define $J_0 = J$, and for each $1 \leqslant i \leqslant d$, let J_i be the set of elements of J which are annihilated by $\{a_1, \ldots, a_i\}$. In other words, for each $1 \leqslant i \leqslant d$, the ideal J_i is the kernel of the map $f_i : J_{i-1} \to J_{i-1}$ defined by $x \mapsto a_i x$. All elements of $\mathfrak{m}$ are nilpotent, and therefore the kernel J_i of the map f_i is nontrivial precisely when $J_{i-1} \neq 0$. Since $J_0 \neq 0$ by hypothesis, it is clear by induction that $J_i \neq 0$ for all $1 \leqslant i \leqslant d$. In particular, there are nonzero elements in $J_d \subseteq J$ which are annihilated by every element of $\mathfrak{m}$.

For part (b), let $k = T/\mathfrak{m}$ be the residue field of T. Because T is a zero-dimensional Gorenstein ring, the k-vector space $\mathrm{Ext}^0_T(k, T) = \mathrm{Hom}_T(k, T)$ is one-dimensional;

see [16, Theorem 18.1]. Thus the annihilator of $\mathfrak{m}$ in T is a principal ideal $I = tT$ where $t = \phi(1)$ for some nonzero $\phi\colon k \to T$. Because N is a faithful module, there is some $n \in N$ such that $tn \neq 0$. Let $\mathrm{Ann}(n)$ be the annihilator of n, which is an ideal contained in $\mathfrak{m}$.

If $\mathrm{Ann}(n) = 0$, then the submodule $Tn \subseteq N$ is free of rank 1 and we are done. If $\mathrm{Ann}(n) \neq 0$, then part (a) implies that $\mathrm{Ann}(n)$ contains a nonzero element x which is killed by all elements of $\mathfrak{m}$. Since I is the annihilator of $\mathfrak{m}$, this means that $x \in \mathrm{Ann}(n)$ is also a nonzero element of I. However, I is a principal ideal that can be viewed as a module over the field $k = T/\mathfrak{m}$, hence every nonzero element of I is a generator. In particular, $xn \neq 0$ because $t \in I = xT$ and $tn \neq 0$. This contradiction completes the proof. □

We are now ready to prove the key proposition.

Proof of Proposition 2.1 Put $S = R/Rs$ and $M = A[s]$ for ease of notation. Notice that M is a *faithful* S-module: Any $r \in R$ such that $rM = rA[s] = 0$ factors as $r = ts$ for some $t \in R$, i.e., $r \in Rs$. Indeed, this follows immediately from the universal property of quotients; see [11, Remark 7 (c)].

Therefore, Lemma 2.2 implies that M contains a free S-submodule of rank 1. Now, we can count the cardinalities of these sets:

$$\#M = \deg s = N_{K/\mathbb{Q}}s = \#R/Rs = \#S.$$

The first equality comes from the separability of s, and the second equality above is a well-known theorem [17, Proposition IV.12.12]. Therefore, $M \cong S$ as an S-module because their cardinalities are the same. This proves Proposition 2.1. □

3 Using kernel ideals

In this section, A is a simple abelian variety over $\mathbb{F}_q$ with Frobenius endomorphism π. Then the endomorphism algebra $D = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a division algebra with center $K = \mathbb{Q}(\pi)$ [21, Theorem 8]. Write $R = \mathrm{End}_{\mathbb{F}_q}(A)$, and let Z be the center of the endomorphism ring. Our goal in this section is to prove the following result.

Proposition 3.1 *If s is a separable element of Z for which sZ is the product of invertible prime ideals in Z, then there is an isomorphism of Z-modules*

$$A[s] \cong (Z/Zs)^d$$

where $d = 2g/[\mathbb{Q}(\pi) : \mathbb{Q}]$. Moreover, this Z-module has exactly one R-module structure, up to isomorphism. This R-module structure comes from the isomorphism of rings $R/Rs \cong \mathrm{M}_d(Z/Zs)$, and there is an isomorphism

$$A[s]^d \cong R/Rs$$

as R-modules.

To prove this proposition, we will inspect the isogenies associated to (left) ideals, inspired by Waterhouse [20]; see also [11, Section 2] for additional background. In the construction of Waterhouse, a nonzero ideal $I \subseteq R$ is associated to an isogeny whose kernel is $A[I] = \bigcap_{\alpha \in I} A[\alpha]$, where $A[\alpha]$ is the kernel of the endomorphism α. In other words, if I is generated by the elements $\alpha_1, \ldots, \alpha_m$, then the abelian variety $A/A[I]$ is isomorphic to the image of the map $(\alpha_1, \ldots, \alpha_m) \colon A \to A^m$.

Similarly, we can also associate a finite subgroup scheme H of A to a left ideal $I(H) \subseteq R$, given by

$$I(H) = \{\alpha \in R : H \subseteq A[\alpha]\}.$$

Given a nonzero ideal $I \subseteq R$, we always have $I \subseteq I(A[I])$. If equality holds, then I is called a *kernel ideal*. Every nonzero ideal I is contained in a kernel ideal J such that $A[I] = A[J]$.

For our purposes, we will be concerned with isogenies that are associated to ideals contained in the center $I_0 \subseteq Z$. For convenience, we will write $A[I_0]$ in place of $A[I_0 R]$. The goal of this section is to describe $A[s]$ in terms of $A[\mathfrak{p}_j^{e_j}]$ where $sZ = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ is the factorization of s into invertible prime ideals in Z, which will allow us to prove Proposition 3.1.

3.1 Basics of invertible ideals

First, we recall some basic key properties about invertible ideals in algebraic number theory. Within this section, let L denote a number field and let $\mathcal{O} \subseteq L$ be an order. The *conductor ideal* of $\mathcal{O}$ is defined to be $\mathfrak{f}_\mathcal{O} = \{a \in L : a\mathcal{O}_L \subseteq \mathcal{O}\}$. The following lemmas show the connection between the conductor ideal and the invertibility of ideals.

Lemma 3.2 *If $\mathfrak{p} \subseteq \mathcal{O}$ is a nonzero prime ideal, then the following are equivalent:*

- *$\mathfrak{p}$ is invertible, i.e., $\mathfrak{p}I = a\mathcal{O}$ for some ideal $I \subseteq \mathcal{O}$ and some $a \in \mathcal{O}$;*
- *$\mathfrak{p}$ is regular, i.e., the localization $\mathcal{O}_\mathfrak{p}$ is integrally closed;*
- *$\mathfrak{p}$ is coprime to the conductor ideal $\mathfrak{f}_\mathcal{O}$, i.e., $\mathfrak{p} + \mathfrak{f}_\mathcal{O} = \mathcal{O}$.*

Moreover, when these equivalent conditions hold, the localization $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring.

Proof The prime ideal $\mathfrak{p}$ is invertible if and only if it is regular by [18, Exercise I.12.5], which is true if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}_\mathcal{O}$ [18, Proposition 12.10]. To obtain the last equivalent condition, observe that $\mathcal{O}$ is a one-dimensional Noetherian integral domain [18, Proposition I.12.2], so any nonzero prime ideal of $\mathcal{O}$ is maximal. In particular, $\mathfrak{p} \not\supseteq \mathfrak{f}_\mathcal{O}$ is equivalent to $\mathfrak{p} + \mathfrak{f}_\mathcal{O} = \mathcal{O}$.

Finally, if $\mathfrak{p}$ is regular, then the localization $\mathcal{O}_\mathfrak{p}$ is equal to the localization of the ring of integers $\mathcal{O}_L$ at the prime ideal $\hat{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_L$ [18, Proposition 12.10], and the latter localization $\mathcal{O}_{L,\hat{\mathfrak{p}}}$ is known to be a discrete valuation ring [18, Proposition I.11.5]. □

While the preceding lemma focuses on prime ideals, the following result shows the connection between invertibility and the conductor ideal in general. In particular, we see that Proposition 3.1 can be rephrased to require that sZ is coprime to the conductor ideal $\mathfrak{f}_Z$ of Z instead of requiring that sZ is the product of invertible ideals.

Lemma 3.3 ([14, Proposition 3.2]) *If $\mathfrak{a} \subseteq \mathcal{O}$ is any ideal coprime to the conductor $\mathfrak{f}_{\mathcal{O}}$, then $\mathfrak{a}$ is invertible and is uniquely factored into (invertible) prime ideals.*

Recall that the *Picard group* $\mathrm{Pic}(\mathcal{O})$ is defined to be the quotient of the set of invertible fractional ideals of $\mathcal{O}$ by the set of principal fractional ideals. We refer readers to [18, Section I.12] and [14] for additional background.

Lemma 3.4 *Every class of ideals in $\mathrm{Pic}(\mathcal{O})$ contains infinitely many prime ideals.*

Proof The extension and contraction of ideals provides a natural bijection between the set of invertible prime ideals of $\mathcal{O}$ and the set of prime ideals of $\mathcal{O}_L$ which are coprime to the conductor ideal $\mathfrak{f}_{\mathcal{O}}$ [14, Lemma 3.3]. Using this bijection, there is a natural isomorphism of groups that allows us to interpret the Picard group $\mathrm{Pic}(\mathcal{O})$ in terms of fractional ideals of $\mathcal{O}_L$ which are coprime to the ideal $\mathfrak{f}_{\mathcal{O}}$ [14, Theorem 3.11]. This reduces the claim to a question concerning ideals in $\mathcal{O}_L$, and a generalization of the Dirichlet density theorem immediately shows that there are infinitely many suitable prime ideals [18, Theorem VII.13.2]. □

3.2 Isogenies associated to ideals

Now we focus our attention on the invertible ideals of the center Z of the endomorphism ring R, and investigate the corresponding isogenies.

Lemma 3.5 *If $I_0 \subseteq Z$ is an invertible ideal, then I_0R is an invertible two-sided ideal of R. In particular, I_0R is a kernel ideal.*

Proof Clearly I_0R is naturally a right ideal, and RI_0 is naturally a left ideal, and these two sets are equal as $I_0 \subseteq Z$ is in the center. Thus, I_0R is a two-sided ideal.

Because I_0 is invertible, there is a fractional ideal J_0 of Z such that $I_0J_0 = Z$. Since Z is the center of R, it also follows that

$$(I_0R)(J_0R) = (J_0R)(I_0R) = R.$$

Moreover, if J is any fractional two-sided ideal of R such that $J \cdot (I_0R) = (I_0R) \cdot J = R$, then $J_0R = (J_0R)(I_0R)J = J$. This proves that J_0R is the unique two-sided fractional ideal of R with this property, which we denote $(I_0R)^{-1}$. It follows immediately from uniqueness that $((I_0R)^{-1})^{-1} = I_0R$.

Now for any ideal I of R, define $(R : I) = \{x \in D : xI \subseteq R\}$. Then we have

$$(R : I_0R) = \{x \in D : xI_0 \subseteq R\} = \{x \in D : I_0x \subseteq R\}$$

because $xI_0R \subseteq R$ if and only if $xI_0 \subseteq R$, and $xI_0 = I_0x$ for all $x \in D$ because I_0 is contained in the center Z. In particular, $(R : I_0R)$ is a two-sided fractional ideal and it is easy to verify that $(R : I_0R) = (I_0R)^{-1}$. Indeed, the containments

$$R \supseteq (R : I_0R) \cdot I_0R \supseteq (I_0R)^{-1} \cdot (I_0R) = R$$

show that $(R : I_0R) \cdot I_0R = R$, and similarly $I_0R \cdot (R : I_0R) = R$. Therefore, we have

$$(R : (R : I_0R)) = ((I_0R)^{-1})^{-1} = I_0R.$$

By [11, Remark 7 (d)], we know that

$$I(A[I_0R]) \subseteq \bigcap_{Rf \supseteq I_0} Rf$$

where the intersection is taken over all elements $f \in D$.

A routine verification shows that

$$\begin{aligned}(R : (R : I_0R)) &= \{x \in D : x \cdot (R : I_0R) \subseteq R\} \\ &= \left\{x \in D : \forall y \in D, \text{ if } I_0y \subseteq R, \text{ then } xy \in R\right\} \\ &= \left\{x \in D : \forall y \in D \setminus \{0\}, \text{ if } I_0 \subseteq Ry^{-1}, \text{ then } x \in Ry^{-1}\right\} \\ &= \bigcap_{Ry^{-1} \supseteq I_0R} \{x \in D : x \in Ry^{-1}\} \\ &= \bigcap_{Ry^{-1} \supseteq I_0R} Ry^{-1} = \bigcap_{Rf \supseteq I_0R} Rf\end{aligned}$$

where the final equality comes from simply reindexing the intersection with $f = y^{-1}$.

Combining all of the containments above, we see that

$$I_0R \subseteq I(A[I_0R]) \subseteq \bigcap_{Rf \supseteq I} Rf = (R : (R : I_0R)) = I_0R$$

which shows that I_0R is a kernel ideal by definition. □

The lemma above is useful because it shows that the prime ideals appearing in Proposition 3.1 are actually kernel ideals, which gives us the following important information. We will write $|H|$ for the rank of a finite subgroup scheme H of A, or equivalently, the degree of the isogeny $\pi_H : A \to A/H$.

Proposition 3.6 *If $I_0 \subseteq Z$ is an invertible ideal, then*

$$\mathrm{End}_{\mathbb{F}_q}(A/A[I_0]) = \mathrm{End}_{\mathbb{F}_q}(A) = R.$$

Moreover,

$$|A[I_0]| = N_{K/\mathbb{Q}}(I_0)^{2g/[K:\mathbb{Q}]}.$$

Proof For convenience, write $B = A/A[I_0]$. Because I_0R is a kernel ideal by Lemma 3.5, the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(B)$ is equal to the right order of I_0R [20, Proposition 3.9], which we denote by

$$\mathcal{O}_r(I_0R) = \{x \in D : (I_0R) \cdot x \subseteq I_0R\}.$$

Since I_0R is a two-sided ideal, clearly $R \subseteq \mathcal{O}_r(I_0R)$. Conversely, let $x \in \mathcal{O}_r(I_0R)$. Then

$$Rx = (I_0R)^{-1}(I_0R)x \subseteq (I_0R)^{-1}I_0R = R$$

because I_0R is an invertible ideal. Therefore, $x \in R$ and $\mathrm{End}_{\mathbb{F}_q}(B) = \mathcal{O}_r(I_0R) = R$.

To prove the second claim, first assume that $I_0 = \alpha Z$ is a principal ideal. Then $A[I_0] = A[\alpha]$ and $|A[I_0]| = \deg \alpha$, so the claim is known [17, Proposition V.12.12].

Now suppose I_0 is not principal. Because I_0 is an invertible ideal of Z, we can pick an ideal $J_0 \subseteq Z$ such that $I_0J_0 = \lambda Z$ and $N_{K/\mathbb{Q}}(J_0)$ is coprime to $|A[I_0]|$. Indeed, there are only finitely many prime factors of $|A[I_0]|$, while there are infinitely many prime ideals in the equivalence class $[I_0]^{-1} \in \mathrm{Pic}(Z)$ by Lemma 3.4. Multiplication of ideals corresponds to composition of isogenies [20, Proposition 3.12], and therefore

$$\begin{aligned} |A[I_0]| \cdot |B[J_0]| &= |A[I_0J_0]| = |A[\lambda]| \\ &= N_{K/\mathbb{Q}}(\lambda)^{2g/[K:\mathbb{Q}]} = N_{K/\mathbb{Q}}(I_0)^{2g/[K:\mathbb{Q}]} N_{K/\mathbb{Q}}(J_0)^{2g/[K:\mathbb{Q}]}. \end{aligned}$$

Now the fact that the rank of $A[I_0]$ is coprime to $N_{K/\mathbb{Q}}(J_0)$ means that $|A[I_0]|$ divides $N_{K/\mathbb{Q}}(I_0)^{2g/[K:\mathbb{Q}]}$. But the same must be true for J_0, so $|B[J_0]|$ divides $N_{K/\mathbb{Q}}(J_0)^{2g/[K:\mathbb{Q}]}$ as well. Therefore, equality must hold, as claimed. □

Because we are ultimately only concerned with separable isogenies, we will restrict our attention to this case now. Recall that the kernel of a separable isogeny $\phi\colon A \to A'$ can be identified with a finite subgroup of $A(\overline{\mathbb{F}}_q)$ of cardinality $\deg \phi$.

Lemma 3.7 *If $r \geqslant$, and $\mathfrak{p} \subseteq Z$ is an invertible prime ideal which corresponds to a separable isogeny, then*

$$A[\mathfrak{p}^r] \cong (Z/\mathfrak{p}^r)^{2g/[K:\mathbb{Q}]}$$

is an isomorphism of Z-modules.

Proof First, $A[\mathfrak{p}]$ is a $Z/\mathfrak{p}$-module. But $Z/\mathfrak{p}$ is a field, so $A[\mathfrak{p}]$ is a vector space, and therefore $A[\mathfrak{p}] \cong (Z/\mathfrak{p})^m$ for some m. We have $m = 2g/[K:\mathbb{Q}]$ by counting the cardinality of each side with Proposition 3.6.

Now we proceed by induction. Given $r \geqslant 2$, we know that $A[\mathfrak{p}^r]$ is a finitely generated module over $Z/\mathfrak{p}^r \cong Z_\mathfrak{p}/\mathfrak{p}^r Z_\mathfrak{p}$. Because $Z_\mathfrak{p}$ is a discrete valuation ring by Lemma 3.2, we can apply the structure theorem for finitely generated modules [5, Theorem 12.1.6] to deduce that $A[\mathfrak{p}^r]$ is the direct sum of modules of the form $Z_\mathfrak{p}/\mathfrak{p}^i Z_\mathfrak{p} \cong Z/\mathfrak{p}^i$ for $1 \leqslant i \leqslant r$.

Further, $A[\mathfrak{p}^r]$ contains $A[\mathfrak{p}^{r-1}]$, which is of the form $(Z/\mathfrak{p}^{r-1})^{2g/[K:\mathbb{Q}]}$ by assumption. Thus, writing $A[\mathfrak{p}^r] \cong Z/\mathfrak{p}^{r_1} \times \cdots \times Z/\mathfrak{p}^{r_s}$ implies that $s = 2g/[K:\mathbb{Q}]$. By counting the cardinality, we must have $r_j = r$ for all $1 \leqslant j \leqslant s$. □

3.3 Proof of main result

Now we are ready to prove the main result of this section.

Proof of Proposition 3.1 We factor $(s) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Notice that for any nonzero $I, J \subseteq R$, we have $A[I] \cap A[J] = A[I + J]$ by definition because $I + J$ is generated by $I \cup J$. Thus, coprime ideals correspond to subgroups with trivial intersection, and we conclude that we have an isomorphism of Z-modules:

$$A[s] \cong A[\mathfrak{p}_1^{e_1}] \times \cdots \times A[\mathfrak{p}_r^{e_r}].$$

For each $1 \leqslant i \leqslant r$, we see that $A[\mathfrak{p}_i^{e_i}] \cong (Z/\mathfrak{p}_i^{e_i})^{2g/[K:\mathbb{Q}]}$ by the proposition above. By the Chinese Remainder Theorem, we conclude that

$$A[s] \cong (Z/Zs)^{2g/[K:\mathbb{Q}]}$$

as desired.

Now write $d = 2g/[K : \mathbb{Q}]$ for convenience. To prove the second claim, we notice that the endomorphism ring of the Z-module $A[s] \cong (Z/Zs)^d$ is the ring of $d \times d$ matrices over Z/Zs, which we write as $\mathrm{End}_Z(A[s]) = \mathrm{M}_d(Z/Zs)$. As in the proof of Proposition 2.1, we see that $A[s]$ is a faithful R/Rs-module, so the map $R/Rs \to \mathrm{End}_Z(A[s])$ induced by the natural R-module structure on $A[s]$ is injective. Moreover, s defines a linear map on the lattice $R \subseteq D$, so we have

$$\#(R/Rs) = N_{D/\mathbb{Q}}(s) = N_{K/\mathbb{Q}}(N_{D/K}(s)) = N_{K/\mathbb{Q}}(s)^{[D:K]},$$

where $N_{D/\mathbb{Q}}(s)$ and $N_{D/K}(s)$ denote the determinants of $s\colon D \to D$ as a linear map over $\mathbb{Q}$ and K, respectively. On the other hand, it is clear that

$$\#\,\mathrm{M}_d(Z/Zs) = N_{K/\mathbb{Q}}(s)^{d^2} = N_{K/\mathbb{Q}}(s)^{[D:K]}$$

because $d^2 = [D : K]$; see [21, Theorem 8]. Therefore, R/Rs and $\mathrm{M}_d(Z/Zs)$ have the same cardinality, so the injective ring map $R \to \mathrm{M}_d(Z/Zs)$ is an isomorphism.

Therefore, to prove that $A[s]$ has exactly one R-module structure, it suffices to show that $(Z/Zs)^d$ has exactly one $\mathrm{M}_d(Z/Zs)$-module structure. Morita equivalence states that every $\mathrm{M}_d(Z/Zs)$-module M' is isomorphic to M^d for some Z/Zs-module M, where M^d is given the natural left $\mathrm{M}_d(Z/Zs)$-module structure defined by applying matrices to column vectors; see [10, Proposition 1.4]. Thus we simply need to know that if a Z-module M satisfies $M^d \cong (Z/Zs)^d$, then $M \cong Z/Zs$. But, as above, s is the product of invertible primes, so M must be of the desired form.

Finally, we notice that $\mathrm{M}_d(Z/Zs)$ is isomorphic to $((Z/Zs)^d)^d$ as a module over itself, which proves the final claim. □

4 Considering the algebraic closure

Now that we have considered the module structure of the group of rational points of a simple abelian variety over a finite field $\mathbb{F}_q$, we turn our attention towards the algebraic closure $\overline{\mathbb{F}}_q$. Because $\overline{\mathbb{F}}_q$ is the union of all its finite subfields, we can stitch together the isomorphisms from Propositions 2.1 and 3.1 to recover the following theorem.

As before, given a simple abelian variety A of dimension g over $\mathbb{F}_q$, we write $R = \mathrm{End}_{\mathbb{F}_q}(A)$ and define Z to be the center of R. Let $[Z:\mathbb{Z}]$ denote the rank of Z as a $\mathbb{Z}$-module. Write $S \subseteq Z$ for the set of separable isogenies in Z, and R_S (resp. Z_S) for the left R-submodule (resp. Z-submodule) of the endomorphism algebra $R \otimes \mathbb{Q}$ generated by the set $\{s^{-1} : s \in S\}$. Equivalently, these can be recognized as localizations by the set S.

Theorem 4.1 *For $g \geqslant 1$, let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g. Let $R = \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$, and let Z be the center of R.*

(a) *If $[\mathbb{Q}(\pi):\mathbb{Q}] = 2g$ and R is a Gorenstein ring, then*

$$A(\overline{\mathbb{F}}_q) \cong R_S/R$$

is an isomorphism of R-modules.

(b) *If Z is a maximal order, then*

$$A(\overline{\mathbb{F}}_q) \cong (Z_S/Z)^d$$

is an isomorphism of Z-modules where $d = 2g/[Z:\mathbb{Z}]$. Moreover, this Z-module has exactly one left R-module structure, up to isomorphism, and there is an isomorphism

$$A(\overline{\mathbb{F}}_q)^d \cong R_S/R$$

as R-modules.

Proof Notice that, in any case, we have

$$A(\overline{\mathbb{F}}_q) = \bigcup_{s \in S} A[s] = \bigcup_{n \geqslant 1} A[\pi^n - 1] = \bigcup_{n \geqslant 1} A(\mathbb{F}_{q^n})$$

where π denotes the Frobenius endomorphism of A over $\mathbb{F}_q$. Indeed, it is clear that each term contains the next, and the final term equals the first. This allows us to deduce the theorem after describing only $A[s]$ for $s \in S$.

For part (a), the hypotheses allow us to apply Proposition 2.1 to obtain isomorphisms $A[s] \cong R/Rs \cong s^{-1}R/R$ for every separable $s \in R$. In other words, for each $s \in S$, the set W_s of isomorphisms between $A[s]$ and $s^{-1}R/R$ is nonempty. Moreover, if s and t are two separable endomorphisms such that s divides t, then the isomorphism $A[t] \xrightarrow{\sim} t^{-1}R/R$ maps the submodule $A[s]$ isomorphically to $s^{-1}R/R$. Thus the set $\{W_s\}_{s \in S}$ forms a projective system of nonempty finite sets, and the projective limit of this system is nonempty [2, Section 7.4, Théorème 1]. In particular, there exists a simultaneous choice of isomorphisms $A[s] \to s^{-1}R/R$ for all $s \in S$ that commutes with the natural inclusions of sets, and the result follows by taking the union over all $s \in S$.

Part (b) follows similarly. Indeed, for each $s \in S$, Proposition 3.1 provides an isomorphism $A[s] \cong (Z/Zs)^d \cong (s^{-1}Z/Z)^d$. By the same projective limit argument

given for part (a), we obtain the desired isomorphism $A(\overline{\mathbb{F}}_q) \cong (Z_S/Z)^d$. Similarly, we obtain the isomorphism $A(\overline{\mathbb{F}}_q)^d \cong R_S/R$.

Finally, any two R-module structures on $(Z_S/Z)^d$ give rise to two R-module structures on $(s^{-1}Z/Z)^d$ for each $s \in S$. Since this structure is known to be unique by Proposition 3.1, we obtain compatible isomorphisms for all $s \in S$, and yet again obtain the desired isomorphism through the projective limit construction. □

Acknowledgements The author thanks Kirsten Eisenträger and Stefano Marseglia for their helpful comments, and thanks Yuri Zarhin for suggesting a simplified approach to Lemma 2.2.

References

1. Ballentine, S., Guillevic, A., Lorenzo García, E., Martindale, C., Massierer, M., Smith, B., Top, J.: Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In: Howe, E.W., et al. (eds.) Algebraic Geometry for Coding Theory and Cryptography, Association for Women in Mathematics Series, vol. 9, pp. 63–94. Springer, Cham (2017)
2. Bourbaki, N.: Éléments de Mathématique. Théorie des Ensembles. Hermann, Paris (1970)
3. Brooks, E.H., Jetchev, D., Wesolowski, B.: Isogeny graphs of ordinary abelian varieties. Res. Number Theory **3**, # 28 (2017)
4. 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)
5. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. John Wiley, Hoboken (2004)
6. Galbraith, S.D.: Constructing isogenies between elliptic curves over finite fields. LMS J. Comput. Math. **2**, 118–138 (1999)
7. Gaudry, P., Kohel, D., Smith, B.: Counting points on genus 2 curves with real multiplication. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology-ASIACRYPT 2011. Lecture Notes in Computer Science, vol. 7073, pp. 504–519. Springer, Heidelberg (2011)
8. Ionica, S., Joux, A.: Pairing the volcano. Math. Comp. **82**(281), 581–603 (2013)
9. Ionica, S., Thomé, E.: Isogeny graphs with maximal real multiplication. J. Number Theory **207**, 385–422 (2020)
10. Jacobson, N.: Basic Algebra. II, 2nd edn. W.H. Freeman and Company, New York (1989)
11. Kani, E.: Products of CM elliptic curves. Collect. Math. **62**(3), 297–339 (2011)
12. Kohel, D.R.: Endomorphism Rings of Elliptic Curves over Finite Fields. PhD Thesis, University of California (1996)
13. Lenstra, H.W., Jr.: Complex multiplication structure of elliptic curves. J. Number Theory **56**(2), 227–241 (1996)
14. Lv, C., Deng, Y.: On orders in number fields: Picard groups, ring class fields and applications. Sci. China Math. **58**(8), 1627–1638 (2015)
15. Martindale, C.: Isogeny Graphs, Modular Polynomials, and Applications. PhD Thesis, University of Leiden (2018)
16. Matsumura, H.: Commutative Ring Theory. Cambridge Studies in Advanced Mathematics, vol. 8. Cambridge University Press, Cambridge (1986)
17. Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.) Arithmetic Geometry, pp. 103–150. Springer, New York (1986)
18. Neukirch, J.: Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften, vol. 322. Springer, Berlin (1999)
19. Springer, C.: Computing the endomorphism ring of an ordinary abelian surface over a finite field. J. Number Theory **202**, 430–457 (2019)
20. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. **2**, 521–560 (1969)
21. Waterhouse, W.C., Milne, J.S.: Abelian varieties over finite fields. In: Lewis, D.J. (ed.) 1969 Number Theory Institute. Proceedings of Symposia in Pure Mathematics, vol. 20, pp. 53–64. American Mathematical Society, Providence (1971)