Abelian varieties isogenous to a power of an elliptic curve

Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains,
Nicholas Shepherd-Barron and John T. Tate

Abstract

Let E be an elliptic curve over a field k. Let $R := \operatorname{End} E$. There is a functor $\mathscr{H}om_R(-, E)$ from the category of finitely presented torsion-free left R-modules to the category of abelian varieties isogenous to a power of E, and a functor $\operatorname{Hom}(-, E)$ in the opposite direction. We prove necessary and sufficient conditions on E for these functors to be equivalences of categories. We also prove a partial generalization in which E is replaced by a suitable higher-dimensional abelian variety over $\mathbb{F}_p$.

1. Introduction

Let E be an elliptic curve over a field k. Let $R := \operatorname{End} E$. We would like to classify all abelian varieties isogenous to a power of E. There is a functor $\mathscr{H}om_R(-, E)$ that takes as input a finitely presented (f.p.) left R-module M and produces a commutative group scheme. (This functor appears in articles by Giraud [Gir68, §1] and Waterhouse [Wat69, Appendix], and is attributed by the former to Serre and Tate; we will give a self-contained exposition in Section 4.1.) We will prove that when restricted to torsion-free modules, it becomes a fully faithful functor of additive categories

$$\begin{aligned}\mathscr{H}om_R(-, E)\colon &\{\text{f.p. torsion-free left } R\text{-modules}\}^{\text{opp}} \\ &\longrightarrow \{\text{abelian varieties isogenous to a power of } E\}.\end{aligned} \tag{1}$$

In the other direction, we have a functor

$$\begin{aligned}\operatorname{Hom}(-, E)\colon &\{\text{abelian varieties isogenous to a power of } E\} \\ &\longrightarrow \{\text{f.p. torsion-free left } R\text{-modules}\}^{\text{opp}}\end{aligned} \tag{2}$$

that provides the inverse on the essential image of (1). These are useful because the modules can be classified for each possible R.

We find necessary and sufficient conditions on E for (1) and (2) to be equivalences of categories. For simplicity, in this introduction we state the answer only for elliptic curves over finite fields.

Theorem 1.1. *Let E be an elliptic curve over a finite field $k = \mathbb{F}_q$. Let $R := \operatorname{End} E$. Let $\pi \in R$ be the q-power Frobenius endomorphism. Then* (1) *and* (2) *are equivalences of categories if and only if one of the following holds*:

2010 Mathematics Subject Classification Primary 14K15; Secondary 11G10, 14K02, 14K05
Keywords: abelian variety, elliptic curve, isogeny
B.P. was supported in part by National Science Foundation grants DMS-1069236 and DMS-1601946 and grants from the Simons Foundation (#340694, #402472, and #550033).

– *E is ordinary and $\mathbb{Z}[\pi] = R$;*

– *E is supersingular, $k = \mathbb{F}_p$, and $\mathbb{Z}[\pi] = R$; or*

– *E is supersingular, $k = \mathbb{F}_{p^2}$, and R is of rank 4 over $\mathbb{Z}$.*

Theorem 1.1 is close to many results in the literature. Waterhouse in [Wat69] proves many results relating the isogeny class of an elliptic curve E to the ideal classes of $\operatorname{End} E$, and he also considers such issues when E is replaced by an abelian variety. An analogue of Theorem 1.1 with the functors $\mathscr{H}om$ and $\operatorname{Hom}(-, E)$ replaced by similarly-defined functors $\otimes$ and $\operatorname{Hom}(E, -)$ is proved in Serre's appendix to [Lau02] in the case where $\mathbb{Z}[\pi]$ is the maximal order in an imaginary quadratic field (in this case, $R = \mathbb{Z}[\pi]$ necessarily). Other cases are handled in [SM74], [Lan75], [Sch92], and especially Kani's work [Kan11]; although these works do not define the functor $\mathscr{H}om$, they too classify all abelian varieties isogenous to a power of E in the case where E is ordinary and $\operatorname{rk} R = 2$ (see Theorems 1, 2, and 3 of [Kan11]). In fact, at one point (in the proof of our Theorem 4.8(a)), we make use of one of the easier results of [Kan11].

The category of all ordinary abelian varieties over a finite field is equivalent to the category of *Deligne modules* [Del69], which are f.p. torsion-free $\mathbb{Z}$-modules provided with an endomorphism that corresponds to the Frobenius. The ordinary case of Theorem 1.1 could be deduced from Deligne's equivalence. For a *prime* ground field $\mathbb{F}_p$, Yu [Yu12, Theorem 3.1] and (in a stronger form) Centeleghe and Stix [CS15] extended Deligne's equivalence to a category including most non-ordinary abelian varieties. For suitable abelian varieties B over $\mathbb{F}_p$, this leads to a classification of the quotients of powers of B; in particular, when B is simple, these quotients are the abelian varieties isogenous to a power of B. Centeleghe and Stix did not mention the functor $\mathscr{H}om_R(-, B)$, but in Section 8 we prove that a functor they used is isomorphic to $\mathscr{H}om_R(-, B)$. Combining their work with ours, we can rewrite their classification in terms of the functor $\mathscr{H}om_R(-, B)$. In particular, this yields a second proof of Theorem 1.1 in the case where the ground field k is $\mathbb{F}_p$. Our first proof, although only for elliptic curves, applies also to non-ordinary elliptic curves over $\mathbb{F}_{p^n}$ for $n > 1$ and to elliptic curves over infinite fields (see Theorems 7.1 and 7.7, for example). It includes the quaternionic endomorphism case, and also determines exactly when the functors above give an equivalence.

Let us now outline the rest of the paper. Section 2 introduces notation to be used. If R is the endomorphism ring of an elliptic curve, then R is $\mathbb{Z}$, an imaginary quadratic order, or a maximal quaternionic order; Section 3 reviews the classification of f.p. torsion-free left R-modules in each case, and in a little more generality. Section 4 introduces the two functors above and proves their basic properties; in particular it is shown that applying $\mathscr{H}om_R(-, E)$ to torsion-free modules produces abelian varieties isogenous to a power of E. Moreover, Section 4.3 relates duality of modules to duality of abelian varieties. Section 5 proves that when E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ with $\operatorname{rk} \operatorname{End} E = 4$, the functors (1) and (2) are equivalences of categories, so that there is a clean classification of abelian varieties isogenous to a power of E. In preparation for the other cases, Section 6 defines the notion of a kernel subgroup, and shows that the functors (1) and (2) are equivalences of categories if and only if every finite subgroup scheme of every power of E is a kernel subgroup. All this is combined in Section 7, which gives a complete answer to the question of when (1) and (2) are equivalences of categories. Section 8 contains the argument involving the work of Centeleghe and Stix for certain abelian varieties of higher dimension over $\mathbb{F}_p$.

2. Notation

Let R be a noetherian integral domain. Let $K = \operatorname{Frac} R$. The *torsion submodule* of an R-module M is

$$M_{\mathrm{tors}} := \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

Call M *torsion-free* if $M_{\mathrm{tors}} = 0$. Call a submodule N of M (or an injection $N \to M$) *saturated* if the cokernel of $N \to M$ is torsion-free. Given a f.p. R-module M, define its *rank* as $\operatorname{rk} M := \dim_K(K \otimes_R M)$. The notion of rank extends to f.p. left modules over a subring R in a division algebra K.

If k is a field, let $\overline{k}$ be an algebraic closure of k, let k_s be the separable closure of k in $\overline{k}$, and let $\mathcal{G}_k := \operatorname{Gal}(k_s/k)$. If G is a finite group scheme over a field k, its *order* is $\#G := \dim_k \Gamma(G, \mathscr{O}_G)$.

Let A be a commutative group scheme over a field k. Then $\operatorname{End} A$ denotes its endomorphism ring as a commutative group scheme over k, i.e., the ring of endomorphisms *defined over* k; an analogous convention applies to Hom. If $\lambda \in \operatorname{End} A$, then $A[\lambda] := \ker \lambda$ denotes the group scheme kernel of $A \xrightarrow{\lambda} A$. In particular, if $n \in \mathbb{Z}_{>0}$, then $A[n]$ is the group scheme kernel of $A \xrightarrow{n} A$. If ℓ is a prime not equal to $\operatorname{char} k$, then the ℓ-adic *Tate module* of A is

$$T_\ell A := \varprojlim_e A[\ell^e](k_s).$$

If X is a scheme over a field k of characteristic $p > 0$, and q is a power of p, let $\pi_{X,q} \colon X \to X^{(q)}$ be the q-power Frobenius morphism; if $k = \mathbb{F}_q$, then let π_X be $\pi_{X,q} \colon X \to X$.

Recall that the *essential image* of a functor $F \colon \mathcal{C} \to \mathcal{D}$ consists of the objects of $\mathcal{D}$ isomorphic to FC for some $C \in \mathcal{C}$; from now on, we call this simply the *image* of F.

3. Classifying torsion-free modules

3.1 Dedekind domains

Suppose that R is a Dedekind domain. Finitely presented (henceforth denoted f.p.) torsion-free R-modules can be completely classified, as is well known [Rei03, Theorem 4.13]. To describe the result, we need the notion of determinant of a module. Given a torsion-free R-module M of rank r, its *determinant* $\det M := \bigwedge^r M$ is a f.p. torsion-free R-module of rank 1; sometimes we identify $\det M$ with its class in $\operatorname{Pic} R$. For example, if $M = I_1 \oplus \cdots \oplus I_r$, where each I_j is a nonzero ideal of R, then $\operatorname{rk} M = r$ and

$$\det M \;\simeq\; I_1 \underset{R}{\otimes} \cdots \underset{R}{\otimes} I_r \;\simeq\; I_1 \cdots I_r \quad \text{(the product ideal in } R).$$

Theorem 3.1.

(a) *A f.p. R-module is torsion-free if and only if it is projective.*

(b) *Every f.p. projective R-module is isomorphic to a finite direct sum of invertible ideals.*

(c) *The isomorphism type of a f.p. projective R-module is determined by its rank and determinant.*

(d) *Every pair $(r, c) \in \mathbb{Z}_{>0} \times \operatorname{Pic} R$ arises as the rank and determinant of a nonzero f.p. projective R-module M; one representative is $M := R^{r-1} \oplus I$ where $[I] = c$.*

3.2 Quadratic orders

For a general order in a Dedekind domain, the structure theory of torsion-free f.p. modules is wild. Fortunately, for *quadratic* orders there is a theory that is only slightly more complicated than that for Dedekind domains. Recall that if $R_{\max}$ is the ring of integers in a quadratic field K, then every order in K is of the form $R_f := \mathbb{Z} + fR_{\max}$ for a positive integer f called the *conductor*. The orders containing R_f are the orders R_g for $g|f$.

Theorem 3.2. *Let R be a quadratic order, i.e., an order in a degree 2 extension K of $\mathbb{Q}$. Let M be a f.p. torsion-free R-module.*

(i) *There exists a unique chain of orders $R_1 \subseteq \cdots \subseteq R_n$ between R and K and invertible ideals $I_1, \ldots, I_n$ of $R_1, \ldots, R_n$, respectively, such that $M \simeq I_1 \oplus \cdots \oplus I_n$ as an R-module.*

(ii) *The I_i are not unique, but their product $I_1 \cdots I_n$ is an invertible R_n-ideal whose class $[M] \in \operatorname{Pic} R_n$ depends only on M.*

(iii) *The isomorphism type of M is uniquely determined by the chain $R_1 \subseteq \cdots \subseteq R_n$ and the class $[M] \in \operatorname{Pic} R_n$.*

Proof. See [BF60]. For generalizations to other integral domains, see [Bas63, Section 7], [BF65], [Lev85], and the survey article [Sal02]. □

3.3 Maximal orders in quaternion algebras

Let B be a quaternion division algebra over $\mathbb{Q}$. Let $\mathcal{O}$ be a maximal order in B. Suppose that M is a f.p. left $\mathcal{O}$-module. The abelian group $B \otimes_{\mathcal{O}} M$ inherits a left B-module structure from B; it is a *free* left B-module by [Bou70, II, §7, Théorème 1]. The nonnegative integer $\operatorname{rk} M$ is the dimension of the left B-vector space $B \otimes_{\mathcal{O}} M$; then $\operatorname{rk} M = \frac{1}{4} \operatorname{rk}_{\mathbb{Z}} M$. Call M *torsion-free* if the natural map $M \to B \otimes_{\mathcal{O}} M$ is an injection, or equivalently, if M is torsion-free as a $\mathbb{Z}$-module.

The classification of f.p. torsion-free left $\mathcal{O}$-modules is similar to the classification over a Dedekind domain, and even simpler in ranks at least 2.

Theorem 3.3.

(a) *A f.p. left $\mathcal{O}$-module is torsion-free if and only if it is projective.*

(b) *Every f.p. projective left $\mathcal{O}$-module is isomorphic to a finite direct sum of ideals.*

(c) *A f.p. projective left $\mathcal{O}$-module of rank at least 2 is free.*

Proof.

(a) See [Rei03, Corollary 21.5].

(b) This follows from the final statement of [Rei03, Corollary 21.5].

(c) This is a classical result due to Eichler [Eic38]; see also [Shi79, Theorem 3.5]. □

4. Categorical constructions

4.1 A functor to an abelian category

We recall the following general construction (cf. [Gir68, §1], [Wat69, Appendix], or [Ser85, pp. 50–51]). Fix an abelian category $\mathcal{C}$, an object $E \in \mathcal{C}$, a ring R, and a ring homomorphism $R \to \operatorname{End} E$. For each f.p. left R-module M, choose a presentation

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0. \tag{3}$$

If we view R^m and R^n as spaces of row vectors, then the R-module homomorphism $R^m \to R^n$ is represented by right-multiplication by some matrix $X \in \mathrm{M}_{m,n}(R)$. Since R acts on E, left-multiplication by X defines a morphism $E^n \to E^m$, whose kernel we call A:

$$0 \longrightarrow A \longrightarrow E^n \longrightarrow E^m. \tag{4}$$

For any $C \in \mathcal{C}$, applying $\operatorname{Hom}(C,-)$ yields an exact sequence

$$0 \longrightarrow \operatorname{Hom}(C,A) \longrightarrow \operatorname{Hom}(C,E)^n \longrightarrow \operatorname{Hom}(C,E)^m.$$

On the other hand, applying $\operatorname{Hom}_R(-,\operatorname{Hom}(C,E))$ to (3) yields an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(M,\operatorname{Hom}(C,E)) \longrightarrow \operatorname{Hom}(C,E)^n \longrightarrow \operatorname{Hom}(C,E)^m.$$

Comparing the previous two sequences yields an isomorphism

$$\operatorname{Hom}(C,A) \simeq \operatorname{Hom}_R(M,\operatorname{Hom}(C,E)),$$

and it is functorial in C. This gives a presentation-independent description of A up to isomorphism as an object of $\mathcal{C}$ representing the functor $\operatorname{Hom}_R(M,\operatorname{Hom}(-,E))\colon \mathcal{C} \to \mathbf{Sets}$. Define $\mathscr{H}om_R(M,E) := A$.

An R-module homomorphism $M \to M'$ induces a homomorphism

$$\operatorname{Hom}_R(M',\operatorname{Hom}(C,E)) \longrightarrow \operatorname{Hom}_R(M,\operatorname{Hom}(C,E))$$

for each $C \in \mathcal{C}$, functorially in C, so by Yoneda's lemma it induces also a morphism between the representing objects $\mathscr{H}om_R(M',E) \to \mathscr{H}om_R(M,E)$. Thus we obtain a functor

$$\mathscr{H}om_R(-,E)\colon \{\text{f.p. left } R\text{-modules}\}^{\text{opp}} \longrightarrow \mathcal{C}. \tag{5}$$

If $0 \to M_1 \to M_2 \to M_3$ is an exact sequence of f.p. left R-modules, then for each $C \in \mathcal{C}$,

$$0 \longrightarrow \operatorname{Hom}_R(M_1,\operatorname{Hom}(C,E)) \longrightarrow \operatorname{Hom}_R(M_2,\operatorname{Hom}(C,E)) \longrightarrow \operatorname{Hom}_R(M_3,\operatorname{Hom}(C,E))$$

is exact. This implies that the sequence of representing objects

$$0 \longrightarrow \mathscr{H}om_R(M_1,E) \longrightarrow \mathscr{H}om_R(M_2,E) \longrightarrow \mathscr{H}om_R(M_3,E)$$

is exact. That is, the functor $\mathscr{H}om_R(-,E)$ is left exact.

Remark 4.1. Following Serre's appendix to [Lau02], one can also define a functor

$$-\otimes_R E\colon \{\text{f.p. right } R\text{-modules}\} \longrightarrow \mathcal{C}.$$

Namely, given a f.p. right R-module M, choose a presentation

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0,$$

and define $M \otimes_R E$ as the cokernel of $E^m \longrightarrow E^n$.

4.2 The functor for an elliptic curve produces abelian varieties

The category of commutative proper group schemes over a field k is an abelian category (the hardest part of this statement is the existence of cokernels, which is [Gro61, Corollaire 7.4]). From now on, we assume that $\mathcal{C}$ is this category.

Proposition 4.2. *Let M be an R-module. Let $A := \mathscr{H}om_R(M,E)$. For every k-algebra L, we have $A(L) \simeq \operatorname{Hom}_R(M,E(L))$.*

Proof. Taking L-points of (4) yields an exact sequence

$$0 \longrightarrow A(L) \longrightarrow E(L)^n \longrightarrow E(L)^m.$$

On the other hand, applying $\operatorname{Hom}_R(-, E(L))$ to (3) yields an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(M, E(L)) \longrightarrow E(L)^n \longrightarrow E(L)^m.$$

The maps $E(L)^n \longrightarrow E(L)^m$ in both sequences are the same, so the result follows. □

PROPOSITION 4.3. *Let E be an abelian variety over a field k. Let R be a domain that is f.p. as a $\mathbb{Z}$-module. Let $R \to \operatorname{End} E$ be a ring homomorphism. Let M be a f.p. left R-module. Let $A := \mathscr{H}om_R(M, E)$. Then $\dim A = (\operatorname{rk} M)(\dim E)$.*

Proof. For any $n \geqslant 1$, the presentation $R \xrightarrow{n} R \to R/nR \to 0$ shows that $\mathscr{H}om_R(R/nR, E) \simeq E[n]$. If M is torsion, then it is a quotient of $(R/nR)^m$ for some $m, n \geqslant 1$; then $A \subseteq E[n]^m$, so A is finite.

In general, let $r = \operatorname{rk} M$. There is an exact sequence

$$0 \to R^r \to M \to T \to 0$$

for some torsion module T; this yields

$$0 \to \mathscr{H}om_R(T, E) \to A \to E^r. \tag{6}$$

By the previous paragraph, $\mathscr{H}om_R(T, E)$ is finite, so $\dim A \leqslant r \dim E$. There exists a nonzero $\rho \in R$ such that $\rho T = 0$. Since R is f.p. as a $\mathbb{Z}$-module, it follows that there exists a positive integer n such that $nT = 0$. Then $R^r \xrightarrow{n} R^r$ factors as $R^r \hookrightarrow M \to R^r$, which induces $E^r \to A \to E^r$ whose composition is multiplication by n, which is surjective. Thus $A \to E^r$ is surjective, so $\dim A \geqslant r \dim E$. Hence $\dim A = r \dim E$. □

If E is an elliptic curve, and I is a subset of $\operatorname{End} E$, let $E[I] := \bigcap_{\alpha \in I} \ker \alpha$.

THEOREM 4.4. *Let E be an elliptic curve over a field k. Let R be a saturated subring of $\operatorname{End} E$ (saturated as a $\mathbb{Z}$-module). Let M be a torsion-free f.p. left R-module. Let $A := \mathscr{H}om_R(M, E)$. Then*

(a) *The group scheme A is an abelian variety isogenous to a power of E.*
(b) *The functor $\mathscr{H}om_R(-, E)$ is exact.*
(c) *If $f : E^r \to E^s$ is a homomorphism arising from applying $\mathscr{H}om_R(-, E)$ to an R-homomorphism $g : R^s \to R^r$, then the image of f is isomorphic to $\mathscr{H}om_R(N, E)$ for some f.p. torsion-free R-module $N \subseteq R^r$. (Moreover, if $R = \operatorname{End} E$, then every homomorphism $f : E^r \to E^s$ arises from some g.)*
(d) *If I is a nonzero left R-ideal, then $\mathscr{H}om_R(R/I, E) \simeq E[I]$ and $\mathscr{H}om_R(I, E) \simeq E/E[I]$.*
(e) *If T is an R-module that is finite as a set, then $\mathscr{H}om_R(T, E)$ is a finite group scheme of order $(\#T)^{2/\operatorname{rk} R}$.*
(f) *If $n \in \mathbb{Z}_{>0}$, then $A[n] \simeq \mathscr{H}om_R(M, E[n])$, where the latter is defined by using the induced ring homomorphism $R \to \operatorname{End} E[n]$.*
(g) *If ℓ is a prime not equal to $\operatorname{char} k$, then $T_\ell A \simeq \operatorname{Hom}_R(M, T_\ell E)$.*

Proof.

(a) Let $r = \operatorname{rk} M = \dim A$. The proof of Proposition 4.3 shows that A admits a surjection to E^r with finite kernel, so if A is an abelian variety, it is isogenous to E^r.
The ring R is either $\mathbb{Z}$, a quadratic order, or a maximal quaternionic order. In the first and third cases, M is projective of rank r over R (the quaternionic case is Theorem 3.3(a)); in

other words, M is a direct summand of R^n for some n; thus A is a direct factor of E^n, so A is an abelian variety.
So suppose that R is a quadratic order. Let c be the conductor, i.e., the index of R in its integral closure. Let ℓ denote a prime. If $\ell \nmid c$, then the semi-local ring $R \otimes \mathbb{Z}_{(\ell)}$ is a Dedekind domain, but a semi-local Dedekind domain is a principal ideal domain, so $M \otimes \mathbb{Z}_{(\ell)}$ is free of rank r over $R \otimes \mathbb{Z}_{(\ell)}$, and $M/\ell M$ is free of rank r over $R/\ell R$.
We claim that A is smooth. This is automatic if $\operatorname{char} k = 0$. So suppose that $\operatorname{char} k = p > 0$. By [Wat69, Theorem 4.2], we have $p \nmid c$, so by the above, M/pM is free of rank r over R/pR. By Proposition 4.2, applying $\operatorname{Hom}_R(M, -)$ to

$$0 \longrightarrow \operatorname{Lie} E \longrightarrow E(k[\epsilon]/(\epsilon^2)) \longrightarrow E(k) \longrightarrow 0$$

yields

$$0 \longrightarrow \operatorname{Hom}_R(M, \operatorname{Lie} E) \longrightarrow A(k[\epsilon]/(\epsilon^2)) \longrightarrow A(k) \longrightarrow 0.$$

Thus

$$\operatorname{Lie} A \simeq \operatorname{Hom}_R(M, \operatorname{Lie} E) \simeq \operatorname{Hom}_{R/pR}(M/pM, \operatorname{Lie} E) \simeq (\operatorname{Lie} E)^r.$$

In particular, $\dim \operatorname{Lie} A = r$, so A is smooth.
Since A is also proper, it is an extension of a finite étale commutative group scheme Φ by an abelian variety B. The constructed surjection $A \to E^r$ with finite kernel restricts to a homomorphism $B \to E^r$ with finite kernel, and it must still be surjective since E^r does not have algebraic subgroups of finite index; thus B is isogenous to E^r. Since $B(\overline{k})$ is divisible, the extension splits over $\overline{k}$. In particular, for each prime ℓ,

$$\#A(\overline{k})[\ell] = \#E(\overline{k})[\ell]^r \#\Phi[\ell]. \tag{7}$$

On the other hand, Proposition 4.2 implies

$$A(\overline{k})[\ell] = \operatorname{Hom}_R(M, E(\overline{k})[\ell]) = \operatorname{Hom}_{R/\ell R}(M/\ell M, E(\overline{k})[\ell]). \tag{8}$$

We claim that

$$\#A(\overline{k})[\ell] = \#E(\overline{k})[\ell]^r. \tag{9}$$

If $\ell \nmid c$, then $M/\ell M$ is free of rank r over $R/\ell R$, so (9) holds. Now suppose that $\ell | c$; in particular, $\ell \neq p$. Then $R/\ell R \simeq \mathbb{F}_\ell[e]/(e^2)$. Every $(R/\ell R)$-module is a direct sum of copies of $\mathbb{F}_\ell$ and $\mathbb{F}_\ell[e]/(e^2)$. Since R is saturated in $\operatorname{End} E$ and $\ell \neq p$, the homomorphisms

$$\frac{R}{\ell R} \longrightarrow \frac{\operatorname{End} E}{\ell(\operatorname{End} E)} \longrightarrow \operatorname{End} E(\overline{k})[\ell]$$

are injective. On the other hand, $\#E(\overline{k})[\ell] = \ell^2 = \#(R/\ell R)$. The previous three sentences imply that $E(\overline{k})[\ell]$ is free of rank 1 over $R/\ell R$. The equality $\#\operatorname{Hom}_{R/\ell R}(N, R/\ell R) = \#N$ holds for $N = \mathbb{F}_\ell$ and $N = \mathbb{F}_\ell[e]/(e^2)$, so it holds for every finite $(R/\ell R)$-module N, and in particular for $M/\ell M$. Thus (8) implies

$$\#A(\overline{k})[\ell] = \#(M/\ell M) = \#(R/\ell R)^r = \#E(\overline{k})[\ell]^r;$$

the middle equality holds since M and R^r are torsion-free $\mathbb{Z}$-modules of the same rank. Hence (9) holds for all ℓ.
Comparing (7) and (9) shows that $\#\Phi[\ell] = 1$ for all ℓ, so Φ is trivial. Thus $A = B$, an abelian variety.

(b) By Lemma 4.5 below, it suffices to show that if $M \to P$ is an injection of modules with P

projective, then $\mathscr{H}om_R(P,E) \to \mathscr{H}om_R(M,E)$ is surjective. We have an exact sequence

$$0 \longrightarrow \mathscr{H}om_R(P/M,E) \longrightarrow \mathscr{H}om_R(P,E) \longrightarrow \mathscr{H}om_R(M,E).$$

By (a), $\mathscr{H}om_R(P,E)$ and $\mathscr{H}om_R(M,E)$ are abelian varieties, so the image I of $\mathscr{H}om_R(P,E) \to \mathscr{H}om_R(M,E)$ is an abelian subvariety of $\mathscr{H}om_R(M,E)$. By Proposition 4.3,

$$\dim \mathscr{H}om_R(P,E) = \dim \mathscr{H}om_R(P/M,E) + \dim \mathscr{H}om_R(M,E),$$

so $\dim I = \dim \mathscr{H}om_R(M,E)$. Thus $I = \mathscr{H}om_R(M,E)$; i.e., $\mathscr{H}om_R(P,E) \to \mathscr{H}om_R(M,E)$ is surjective.

(c) Since $\mathscr{H}om_R(-,E)$ is exact, it transforms the co-image of g into the image of f. (Co-image equals image in any abelian category, though the proof above does not need this.)

(d) The proof of [Wat69, Proposition A.2] shows that $\mathscr{H}om_R(R/I,E) \simeq E[I]$ (there R is *equal* to $\operatorname{End} E$, but this is not used). The proof of [Wat69, Proposition A.3] shows that $E/E[I]$ is the connected component of $\mathscr{H}om_R(I,E)$, but $\mathscr{H}om_R(I,E)$ is already connected, by (a).

(e) The function $(\#T)^{2/\operatorname{rk} R}$ of T is multiplicative in short exact sequences. So is $\# \mathscr{H}om_R(T,E)$, since $\mathscr{H}om_R(-,E)$ is exact. Thus we may reduce to the case in which T is simple, i.e., $T \simeq R/I$ for some maximal ideal I. Then $\mathscr{H}om_R(T,E) = E[I]$ by (d). We have $I \supseteq \ell R$ for some prime ℓ. If $I = \ell R$, then $E[I] = E[\ell]$, which has order $\ell^2 = \#(R/I)^{2/\operatorname{rk} R}$.
Now suppose that $I \neq \ell R$. If R has rank 2, then $\#(R/I) = \ell$; if R has rank 4, then $\#(R/I) = \ell^2$. Choose $f \in I \setminus \ell R$; then f does not kill $E[\ell]$, so $E[I] \subsetneq E[\ell]$. Thus $\#E[I] \leqslant \ell = \#(R/I)^{2/\operatorname{rk} R}$. Thus $\# \mathscr{H}om_R(T,E) \leqslant (\#T)^{2/\operatorname{rk} R}$ holds for each Jordan–Hölder factor of $R/\ell R$, but for $T = R/\ell R$ equality holds, so all the inequalities must have been equalities.

(f) Start with the exact sequence

$$0 \to E[n] \to E \xrightarrow{n} E.$$

Given $S \in \mathcal{C}$, apply the left exact functors $\operatorname{Hom}_{\mathcal{C}}(S,-)$ and then $\operatorname{Hom}_R(M,-)$; taken for all S, this produces an exact sequence of representable functors

$$0 \longrightarrow \mathscr{H}om_R(M,E[n]) \longrightarrow \mathscr{H}om_R(M,E) \xrightarrow{n} \mathscr{H}om_R(M,E).$$

Hence $\mathscr{H}om_R(M,E[n]) \simeq A[n]$.

(g) We have

$$\begin{aligned} T_\ell A &:= \varprojlim_e A[\ell^e](k_s) \\ &\simeq \varprojlim_e \mathscr{H}om_R(M,E[\ell^e])(k_s) && \text{(by (f))} \\ &\simeq \varprojlim_e \operatorname{Hom}_R(M,E[\ell^e](k_s)) && \text{(by Proposition 4.2 with E replaced by $E[\ell^e]$)} \\ &\simeq \operatorname{Hom}_R(M, \varprojlim_e E[\ell^e](k_s)) \\ &=: \operatorname{Hom}_R(M,T_\ell E). \end{aligned}$$

□

The following was used in the proof of Theorem 4.4(b).

Lemma 4.5. *Let $\mathcal{C}$ be an abelian category with enough projectives. Let $F\colon \mathcal{C}^{\text{opp}} \to \mathcal{D}$ be a left exact functor. Suppose that for each monomorphism $M \to P$ with P projective, the morphism $FP \to FM$ is an epimorphism. Then F is exact.*

Proof. Given $A \in \mathcal{C}$, choose an epimorphism $P \to A$ with P projective, and let K be the kernel. The sequence $0 \to K \to P \to A \to 0$ yields

$$0 \to FA \to FP \to FK \to (R^1F)A \to (R^1F)P = 0,$$

and the hypothesis implies that $FP \to FK$ is surjective, so $(R^1F)A = 0$. This holds for all A, so F is exact. $\square$

Remark 4.6. The hypothesis that R is saturated in Theorem 4.4 cannot be dropped. For example, if E is an elliptic curve over $\mathbb{C}$ with $\operatorname{End} E = \mathbb{Z}[i]$, and R is the subring $\mathbb{Z}[2i]$, then the R-module $\mathbb{Z}[i]$ has a presentation

$$R \xrightarrow{\begin{pmatrix} 2i \\ -2 \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} 1 & i \end{pmatrix}} \mathbb{Z}[i] \longrightarrow 0,$$

so by definition,

$$\mathscr{H}\!om_R(\mathbb{Z}[i], E) \;\simeq\; \ker\left(E^2 \xrightarrow{\begin{pmatrix} 2i & -2 \end{pmatrix}} E \right) \;\simeq\; E \times E[2],$$

which is not an abelian variety. Moreover, applying $\mathscr{H}\!om_R(-, E)$ to the injection $\mathbb{Z}[i] \xrightarrow{2} R$ yields a homomorphism $E \to E \times E[2]$, which is not surjective, so $\mathscr{H}\!om_R(-, E)$ is not exact. Finally, $\mathbb{Z}[i]$ is isomorphic as R-module to the R-ideal $I := 2\mathbb{Z}[i]$, so $\mathscr{H}\!om_R(I, E)$ is not an abelian variety.

4.3 Duality of abelian varieties

Let E be an elliptic curve over a field k. Let $R := \operatorname{End} E$. The *Rosati involution*, sending an endomorphism to its dual, is an isomorphism $R \to R^{\mathrm{opp}}$. If M is a left R-module, then $M^* := \operatorname{Hom}_R(M, R)$ (the group of homomorphisms of left R-modules) is a *right* R-module: Given $f \in M^*$ and $r \in R$, let $f \cdot r$ be the composition $M \xrightarrow{f} R \xrightarrow{r} R$, where $R \xrightarrow{r} R$ is right-multiplication by r. In other words, M^* is a left R^{opp}-module, which we may reinterpret as a left R-module by using the Rosati involution. Moreover, if M is f.p., then it is finite over $\mathbb{Z}$, and then so is M^*. Also, M^* is torsion-free.

Given an abelian variety A, let $A^\vee$ be the dual abelian variety. The following lets us understand the duals of abelian varieties arising from modules.

Theorem 4.7. *Given a f.p. torsion-free left R-module M, we have*

$$\mathscr{H}\!om_R(M, E)^\vee \simeq \mathscr{H}\!om_R(M^*, E),$$

functorially in M.

Proof. Let M be a f.p. torsion-free left R-module. Choose a presentation as in (3),

$$R^m \xrightarrow{X} R^n \longrightarrow M \longrightarrow 0, \tag{10}$$

in which the first homomorphism is right-multiplication by some $X \in \mathrm{M}_{m\times n}(R)$ on row vectors. Apply $\mathscr{H}\!om_R(-, E)$ to obtain

$$0 \longrightarrow A \longrightarrow E^n \xrightarrow{X} E^m,$$

in which X now acts on the left. Taking dual abelian varieties yields

$$E^m \xrightarrow{X^\dagger} E^n \longrightarrow A^\vee \longrightarrow 0, \tag{11}$$

where $X^\dagger \in \mathrm{M}_{n\times m}(R)$ is obtained from X by taking the transpose and applying the Rosati involution entrywise.

On the other hand, applying $\operatorname{Hom}_R(-,R)$ to (10) yields an exact sequence of right R-modules

$$0 \longrightarrow M^* \longrightarrow R^n \xrightarrow{X} R^m$$

involving left-multiplication by X on column vectors. This may be reinterpreted via the Rosati involution as an exact sequence of left R-modules

$$0 \longrightarrow M^* \longrightarrow R^n \xrightarrow{X^\dagger} R^m$$

involving right-multiplication by $X^\dagger$ on row vectors. Applying the exact functor $\mathscr{H}\!om_R(-,E)$ yields

$$E^m \xrightarrow{X^\dagger} E^n \longrightarrow \mathscr{H}\!om_R(M^*,E) \longrightarrow 0.$$

Comparing with (11) yields an isomorphism

$$\mathscr{H}\!om_R(M^*,E) \simeq A^\vee = \mathscr{H}\!om_R(M,E)^\vee. \tag{12}$$

Given a homomorphism of f.p. torsion-free left R-modules $M \xrightarrow{f} N$, we can build a commutative diagram

$$\begin{array}{ccccccc}
R^n & \longrightarrow & R^m & \longrightarrow & M & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle f} & & \\
R^i & \longrightarrow & R^j & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

and apply the constructions above to show that (12) is functorial in M. $\square$

4.4 The other Hom functor

Under the assumptions of Theorem 4.4(b), we have a functor of additive categories

$$\begin{aligned}\mathscr{H}\!om_R(-,E)\colon &\{\text{f.p. torsion-free left } R\text{-modules}\}^{\mathrm{opp}} \\ &\longrightarrow \{\text{abelian varieties isogenous to a power of } E\},\end{aligned}$$

as promised in the introduction. From now on, $\mathscr{H}\!om_R(-,E)$ denotes this functor, restricted to f.p. *torsion-free* left R-modules.

Given an abelian variety A over the same field as E, the abelian group $\operatorname{Hom}(A,E)$ (the group of homomorphisms of abelian varieties) is a left $(\operatorname{End} E)$-module, and hence also a left R-module, and it is f.p. because it is f.p. over $\mathbb{Z}$ [Mum70, p. 178, Corollary 1]. In fact, we get a functor in the opposite direction:

$$\begin{aligned}\operatorname{Hom}(-,E)\colon &\{\text{abelian varieties isogenous to a power of } E\} \\ &\longrightarrow \{\text{f.p. torsion-free left } R\text{-modules}\}^{\mathrm{opp}}.\end{aligned}$$

For which elliptic curves E are $\mathscr{H}\!om_R(-,E)$ and $\operatorname{Hom}(-,E)$ inverse equivalences of categories? If we start with the R-module R and apply $\mathscr{H}\!om_R(-,E)$ and then $\operatorname{Hom}(-,E)$, we obtain $\operatorname{End} E$, so we should have $R \simeq \operatorname{End} E$ as R-modules; then the only R-module endomorphisms of $\operatorname{End} E$ are given by multiplication by elements of R, but multiplication by elements of $\operatorname{End} E$ also give endomorphisms, so $R = \operatorname{End} E$. Thus we assume from now on that $R = \operatorname{End} E$.

Theorem 4.8. *Let E be an elliptic curve over a field. Let $R := \operatorname{End} E$. Then*

(a) *The functor $\mathscr{H}\!om_R(-,E)$ is fully faithful.*

(b) *The functor* $\operatorname{Hom}(-,E)$ *on the image of* $\mathscr{H}om_R(-,E)$ *is an inverse to* $\mathscr{H}om_R(-,E)$.

(c) *The image of* $\mathscr{H}om_R(-,E)$ *consists exactly of the products of elliptic curves of the form* $\mathscr{H}om_R(I,E)$ *for a nonzero left* R*-ideal* I.

Proof.

(a) The ring R is $\mathbb{Z}$, a quadratic order, or a maximal quaternionic order. By Theorem 3.1, Theorem 3.2(i), or Theorem 3.3(b), respectively, every f.p. torsion-free left R-module is a finite direct sum of nonzero left R-ideals. Thus, (a) follows if for any two nonzero R-ideals I and J, the natural map

$$\operatorname{Hom}_R(J,I) \longrightarrow \operatorname{Hom}(\mathscr{H}om_R(I,E), \mathscr{H}om_R(J,E))$$

is an isomorphism. If $R=\mathbb{Z}$, this is trivial. If R is a quadratic order, this is the elliptic curve case of the isomorphism given in (48) in [Kan11, Proposition 17]. If R is a maximal quaternionic order, then by Theorem 3.3(a) all f.p. torsion-free left R-modules are projective, i.e., direct summands of f.p. free left R-modules; since $\mathscr{H}om_R(-,E)$ is fully faithful when restricted to free modules, it is also fully faithful on projective modules.

(b) Let M be a f.p. torsion-free left R-module. Then

$$\operatorname{Hom}(\mathscr{H}om_R(M,E),E) = \operatorname{Hom}(\mathscr{H}om_R(M,E), \mathscr{H}om_R(R,E)) = \operatorname{Hom}_R(R,M) = M$$

since $E = \mathscr{H}om_R(R,E)$ and $\mathscr{H}om_R(-,E)$ is fully faithful by (a).

(c) As remarked in the proof of (a), every f.p. torsion-free left R-module is a finite direct sum of nonzero left R-ideals I. $\square$

5. Maximal abelian varieties over $\mathbb{F}_{p^2}$

Fix a prime p. Call an abelian variety A over $\mathbb{F}_{p^2}$ *maximal* if A has the maximum possible number of $\mathbb{F}_{p^2}$-points for its dimension, namely $(p+1)^{2\dim A}$.

PROPOSITION 5.1. *Let A be a g-dimensional abelian variety over $\mathbb{F}_{p^2}$. Let ℓ be a prime not equal to p. The following are equivalent*:

(a) *The abelian variety A is maximal; i.e., $\#A(\mathbb{F}_{p^2}) = (p+1)^{2g}$.*

(b) *The characteristic polynomial of π_A on $T_\ell A$ equals $(x+p)^{2g}$.*

(c) *We have $\pi_A = -p$.*

(d) *We have $A(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^{2g}$ as abelian groups.*

If E is a fixed maximal elliptic curve over $\mathbb{F}_{p^2}$, then the following also is equivalent to the above:

(e) *The abelian variety A is isogenous to E^g.*

Proof.

(a)⇒(b): Let $\lambda_1,\dots,\lambda_{2g} \in \overline{\mathbb{Q}}$ be the eigenvalues of π_A acting on $T_\ell A$. Then $|\lambda_i| = p$ and $\#A(\mathbb{F}_{p^2}) = \prod(1-\lambda_i) = \prod|1-\lambda_i| \leqslant (p+1)^{2g}$; if equality holds, then $\lambda_i = -p$ for all i. Thus the characteristic polynomial is $(x+p)^{2g}$.

(b)⇒(c): Since π_A is determined by its action on $T_\ell A$, which is semisimple [Mum70, pp. 203–206], we obtain $\pi_A = -p$.

(c)⇒(d): We have

$$A(\mathbb{F}_{p^2}) = \ker(\pi_A - 1)(\overline{\mathbb{F}}_p) = \ker(-p-1)(\overline{\mathbb{F}}_p) = A[p+1](\overline{\mathbb{F}}_p) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^{2g}.$$

(d) ⇒(a): Trivial.

(e) ⇔(b): By (a)⇒(b), the characteristic polynomial of π_E is $(x+p)^2$, so the characteristic polynomial of π_{E^g} is $(x+p)^{2g}$. Two abelian varieties over a finite field are isogenous if and only if their characteristic polynomials are equal [Tat66, Theorem 1(c)]. □

Lemma 5.2. *If A and B are maximal abelian varieties over $\mathbb{F}_{p^2}$, then any homomorphism $A_{\overline{\mathbb{F}}_p} \to B_{\overline{\mathbb{F}}_p}$ is the base extension of a homomorphism $A \to B$.*

Proof. Any homomorphism respects the p^2-power Frobenius endomorphisms (both are equal to $-p$), and hence descends to $\mathbb{F}_{p^2}$. □

Every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ admits a unique model over $\mathbb{F}_{p^2}$ that is maximal: the existence is [BGGP05, Lemma 3.21], and uniqueness follows from Lemma 5.2. In particular, maximal elliptic curves over $\mathbb{F}_{p^2}$ exist. If E is any such curve, then E is supersingular, and Lemma 5.2 implies that $\operatorname{End} E = \operatorname{End} E_{\overline{\mathbb{F}}_p}$, which is a maximal order $\mathcal{O}$ in a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Also, the kernel of the p-power Frobenius morphism $E \to E^{(p)}$ is isomorphic to $\boldsymbol{\alpha}_p$.

By Proposition 5.1(a)⇒(e), any maximal abelian variety A over $\mathbb{F}_{p^2}$ is isogenous to a power of E. The main result of this section strengthens this as follows:

Theorem 5.3.

(a) *Every maximal abelian variety A over $\mathbb{F}_{p^2}$* is isomorphic *to a product of maximal elliptic curves over $\mathbb{F}_{p^2}$.*

(b) *Fix a maximal elliptic curve E over $\mathbb{F}_{p^2}$. Let $\mathcal{O} := \operatorname{End} E$. Then the functors $\mathscr{H}om_{\mathcal{O}}(-, E)$ and $\operatorname{Hom}(-, E)$ are inverse equivalences of categories. Also, the categories involved can be rewritten so that $\mathscr{H}om_{\mathcal{O}}(-, E)$ becomes*

$$\mathscr{H}om_{\mathcal{O}}(-, E)\colon \{\text{f.p. projective left } \mathcal{O}\text{-modules}\}^{\mathrm{opp}} \xrightarrow{\sim} \{\text{maximal abelian varieties}/\mathbb{F}_{p^2}\}.$$

(c) *Fix a maximal elliptic curve E over $\mathbb{F}_{p^2}$. Let $g \geqslant 2$. Every g-dimensional maximal abelian variety over $\mathbb{F}_{p^2}$ is isomorphic to E^g. In particular, any product of g maximal elliptic curves over $\mathbb{F}_{p^2}$ is isomorphic to any other.*

The analogous results hold if maximal is replaced by minimal; *i.e., we consider abelian varieties A over $\mathbb{F}_{p^2}$ such that $\#A(\mathbb{F}_{p^2}) = (p-1)^{2\dim A}$.*

We need a few lemmas for the proof of Theorem 5.3.

Lemma 5.4. *There exists an elliptic curve E over $\mathbb{F}_p$ such that $E_{\mathbb{F}_{p^2}}$ is maximal.*

Proof. There exists an elliptic curve E over $\mathbb{F}_p$ with $p+1$ points [Wat69, Theorem 4.1(5)(i)]. The p-power Frobenius endomorphism π_E of E satisfies $\pi_E^2 = -p$, so $E_{\mathbb{F}_{p^2}}$ satisfies condition (c) in Proposition 5.1. □

Lemma 5.5. *If E and E' are maximal elliptic curves over $\mathbb{F}_{p^2}$, there exists a separable isogeny $E \to E'$.*

Proof. For elliptic curves E and E', write $E \sim E'$ if there exists an isogeny $E \to E'$ of degree prime to p. The relation $\sim$ is an equivalence relation: reflexive because of the identity, symmetric because of the dual isogeny (which has the same degree), and transitive because of composition of isogenies.

Any isogeny $\phi\colon E \to E'$ factors as $f \circ \lambda$ where $\deg f = p^n$ for some $n \geqslant 1$, and $p \nmid \deg \lambda$. Here λ is separable. On the other hand, f is a factor of $[p^n]$, which is purely inseparable if E is maximal. Thus, assuming that E is maximal, ϕ is separable if and only if $p \nmid \deg \phi$.

Let E_0 be the maximal elliptic curve over $\mathbb{F}_{p^2}$ in Lemma 5.4. Since $\#E_0(\mathbb{F}_{p^2}) = \#E(\mathbb{F}_{p^2})$, there exists an isogeny $E_0 \to E$, which factors as $E_0 \xrightarrow{f} E_0 \xrightarrow{\lambda} E$, where f is a power of the p-power Frobenius morphism (which goes from E_0 to itself since E_0 is definable over $\mathbb{F}_p$), and λ is separable. By the previous paragraph, $p \nmid \deg \lambda$. Thus $E_0 \sim E$. Similarly, $E_0 \sim E'$, so $E \sim E'$. Thus there exists an isogeny $E \to E'$ of degree prime to p. Any such isogeny is separable. $\square$

Remark 5.6. Even better, if E and E' are maximal elliptic curves over $\mathbb{F}_{p^2}$, there exists an isogeny of ℓ-power degree for any prime $\ell \neq p$: for an argument due to Serre, see [Mes86, p. 223].

Lemma 5.7. *If A is a maximal abelian variety over $\mathbb{F}_{p^2}$, then every finite étale subgroup scheme of $A_{\overline{\mathbb{F}}_p}$ is defined over $\mathbb{F}_{p^2}$.*

Proof. The p^2-power Frobenius field automorphism acts on (prime-to-p) torsion points of $A_{\overline{\mathbb{F}}_p}$ as $-p$, so it preserves any finite subgroup of order prime to p. $\square$

Corollary 5.8. *If A is a maximal abelian variety over $\mathbb{F}_{p^2}$, and G is a nonzero finite étale subgroup scheme of A, then G contains a subgroup scheme of prime order.*

Proof. Choose a prime-order subgroup of $G(\overline{\mathbb{F}}_p)$. The corresponding finite étale subgroup scheme of $G_{\overline{\mathbb{F}}_p}$ is defined over $\mathbb{F}_{p^2}$ by Lemma 5.7. $\square$

Lemma 5.9. *Let A be a supersingular abelian variety over a field k of characteristic p. Every p-power order subgroup scheme $G \subseteq A$ is an iterated extension of copies of $\boldsymbol{\alpha}_p$.*

Proof. By induction, it suffices to show that if $G \neq 0$, then G contains a copy of $\boldsymbol{\alpha}_p$. The *a-number* $\dim_k \operatorname{Hom}(\boldsymbol{\alpha}_p, G)$ is unchanged by field extension [LO98, Section 1.5], so we may assume that k is algebraically closed. Then A is isogenous to a power E^r of a supersingular elliptic curve. The group scheme $E[p]$ is an extension of $\boldsymbol{\alpha}_p$ by $\boldsymbol{\alpha}_p$, so all Jordan–Hölder factors of $E[p^n]$ are isomorphic to $\boldsymbol{\alpha}_p$. The image of $E[p^N]$ under the isogeny $E^r \to A$ contains $A[p^n]$ if N is sufficiently large relative to n, and $A[p^n]$ contains G if n is large enough. Thus all Jordan–Hölder factors of G are isomorphic to $\boldsymbol{\alpha}_p$. $\square$

Lemma 5.10. *Let E and E' be maximal elliptic curves over $\mathbb{F}_{p^2}$. Identify $\boldsymbol{\alpha}_p$ with a subgroup scheme of each. Then each homomorphism $E \to E'$ restricts to a homomorphism $\boldsymbol{\alpha}_p \to \boldsymbol{\alpha}_p$ and the resulting map*

$$\operatorname{Hom}(E, E') \longrightarrow \operatorname{End} \boldsymbol{\alpha}_p \simeq \mathbb{F}_{p^2} \tag{13}$$

is surjective.

Proof. Since each $\boldsymbol{\alpha}_p$ is the kernel of the p-power Frobenius morphism, any homomorphism $E \to E'$ must map $\boldsymbol{\alpha}_p$ to $\boldsymbol{\alpha}_p$. If $E' = E$, then the resulting ring homomorphism

$$\operatorname{End} E \longrightarrow \operatorname{End} \boldsymbol{\alpha}_p \simeq \mathbb{F}_{p^2}$$

is surjective because every ring homomorphism from $\mathcal{O}$ to $\mathbb{F}_{p^2}$ is surjective. In the general case, Lemma 5.5 provides a separable isogeny $\lambda\colon E \to E'$; then $\lambda|_{\boldsymbol{\alpha}_p} \neq 0$, so $\{\lambda \circ e : e \in \operatorname{End} E\}$ surjects onto $\operatorname{End} \boldsymbol{\alpha}_p$. $\square$

Lemma 5.11. *Let E and E' be maximal elliptic curves over $\mathbb{F}_{p^2}$. Let G be a subgroup scheme of E such that $\#G$ is prime. Then every homomorphism $h\colon G \to E'$ extends to a homomorphism $E \to E'$.*

Proof. Case 1: $\#G$ is a prime $\ell \neq p$. Then extend $G(\overline{\mathbb{F}}_p) \to E'(\overline{\mathbb{F}}_p)$ to a homomorphism $E[\ell](\overline{\mathbb{F}}_p) \to E'[\ell](\overline{\mathbb{F}}_p)$ and lift it arbitrarily to a $\mathbb{Z}_\ell$-module homomorphism $t\colon T_\ell E \to T_\ell E'$. Since the p^2-power Frobenius automorphism acts as $-p$ on both sides, t respects the action of $\mathcal{G}_{\mathbb{F}_{p^2}}$. By Tate's theorem on homomorphisms [Tat66], t comes from some $\tau \in \operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell$. Any $\tau' \in \operatorname{Hom}(E, E')$ congruent to τ modulo ℓ extends h.

Case 2: $\#G = p$. By Lemma 5.9, G is the copy of $\boldsymbol{\alpha}_p$ of E (the kernel of the p-power Frobenius morphism). By Lemma 5.10, h extends to a homomorphism $E \to E'$. □

Lemma 5.12. *Let $f\colon X \to Y$ be a homomorphism of commutative group schemes. Let Γ be the graph of f. Then there exists an automorphism of $X \times Y$ sending Γ to $X \times \{0\}$.*

Proof. Use $(x, y) \mapsto (x, y - f(x))$, which has inverse $(x, y) \mapsto (x, y + f(x))$. □

Lemma 5.13. *Let B be a product $E_1 \times \cdots \times E_g$ of maximal elliptic curves over $\mathbb{F}_{p^2}$. Let G be a finite subgroup scheme of B. Then B/G is isomorphic to a product of maximal elliptic curves over $\mathbb{F}_{p^2}$.*

Proof. First suppose that $\#G$ is prime. Let $\mathrm{pr}_j\colon B \to E_j$ denote the jth projection. Then $\mathrm{pr}_j(G) \neq 0$ for some j, say $j = 1$. Since $\#G$ is prime, pr_1 maps G isomorphically to its image $G_1 \subset E_1$. Thus G is the graph of a homomorphism $h\colon G_1 \to E_2 \times \cdots \times E_g$. Applying Lemma 5.11 to each factor $G_1 \longrightarrow E_j$ shows that h extends to a homomorphism $f\colon E_1 \to \prod_{j \geqslant 2} E_j$. Then G is contained in the graph of f. By Lemma 5.12, after applying an automorphism of B we may assume that $G \subseteq E_1$. Then B/G is the product of the maximal elliptic curves E_1/G, $E_2, \ldots, E_g$.

By Corollary 5.8 and Lemma 5.9, every Jordan–Hölder factor of G has prime order, so the general case follows by induction. □

Proof of Theorem 5.3.

(a) By Proposition 5.1(a)⇒(e), $A \simeq B/G$, where B is a product of maximal elliptic curves (in fact, a power) and G is a finite subgroup scheme of B. Apply Lemma 5.13.

(b) First let us justify the rewriting of the categories. F.p. torsion-free left $\mathcal{O}$-modules are projective by Theorem 3.3(a). By Proposition 5.1(a)⇔(e), the abelian varieties isogenous to a power of E are exactly the maximal abelian varieties over $\mathbb{F}_{p^2}$.
By (a), every maximal abelian variety is a product of maximal elliptic curves, each of which is $\mathscr{H}om_{\mathcal{O}}(I, E)$ for some left $\mathcal{O}$-ideal I, by the bottom of page 541 in [Wat69]. The result now follows from 4.8.

(c) Combine Theorem 3.3(c) and part (b).

The same proofs apply in the minimal case. □

Remark 5.14. Because of Lemma 5.2, Theorem 5.3(c) could be deduced also from its analogue over $\overline{\mathbb{F}}_p$, that for $g \geqslant 2$, any product of g supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is isomorphic to any other. The latter is a well-known theorem of Deligne, proved in a similar way: see [Ogu79, Theorem 6.2] and [Shi79, Theorem 3.5].

Remark 5.15. A related result can be found in [Oor75]: Theorem 2 there states that if A is an abelian variety over an algebraically closed field of characteristic p, and the a-number of A equals $\dim A$, then A is isomorphic to a product of supersingular elliptic curves.

6. Kernel subgroups

6.1 General properties of kernel subgroups

Definition 6.1. Let A be an abelian variety over a field. Call a subgroup scheme $G \subseteq A$ a *kernel subgroup* if $G = A[I]$ for some $I \subseteq \operatorname{End} A$. (These are called *ideal subgroups* in [Kan11, p. 302].)

In the definition, we may replace I by the left $(\operatorname{End} A)$-ideal it generates without changing $A[I]$. Thus we may always assume that I is a left $(\operatorname{End} A)$-ideal.

Proposition 6.2.

(a) *An intersection of kernel subgroups in A is a kernel subgroup.*

(b) *Let $A_1, \ldots, A_n$ be abelian varieties. Suppose that $G_i \subseteq A_i$ for $i = 1, \ldots, n$. Then $\prod_{i=1}^n G_i$ is a kernel subgroup of $\prod_{i=1}^n A_i$ if and only if each G_i is a kernel subgroup of A_i.*

(c) *Let $I_1, \ldots, I_n$ be pairwise coprime 2-sided ideals of $\operatorname{End} A$. Let $G_i \subseteq A[I_i]$ for $i = 1, \ldots, n$. Then $\sum_{i=1}^n G_i$ is a kernel subgroup if and only if each G_i is a kernel subgroup.*

Proof.

(a) We have $\bigcap A[I_i] = A[\sum I_i]$ for any left ideals I_i.

(b) Let $A = \prod A_i$ and $G = \prod G_i$. Suppose that $G = A[I]$. For each $f \in I$, the composition $A_i \hookrightarrow A \xrightarrow{f} A \twoheadrightarrow A_i$ defines $\bar{f} \in \operatorname{End} A_i$, and G_i is the intersection of the kernels of all such $\bar{f}$. Conversely, suppose that $G_i = A_i[I_i]$ for each i. Let $I := \prod I_i$ denote the set of "diagonal" endomorphisms $(f_1, \ldots, f_n)\colon A \to A$ with $f_i \in I_i$. Then $G = A[I]$.

(c) By induction, we may assume $n = 2$. Since I_1 and I_2 are coprime 2-sided ideals, we have $A[I_1 I_2] = A[I_1] \oplus A[I_2]$, and every subgroup scheme $H \subseteq A[I_1 I_2]$ decomposes as $H_1 \oplus H_2$, where $H_i \subseteq A[I_i]$; namely, $H_i = H \cap A[I_i]$.
If $G_1 + G_2$ is a kernel subgroup, then so is $G_i = (G_1 + G_2) \cap A[I_i]$, by (a).
Conversely, suppose that $G_i = A[J_i]$ for some left ideal J_i. Replace J_i by $J_i + I_i$ to assume that $J_i \supseteq I_i$. Let $K := I_2 J_1 + I_1 J_2$. We claim that $A[K] = G_1 + G_2$. First, $I_2 J_1 \subseteq J_1$, which kills G_1; also, $I_1 J_2 \subseteq I_1$, which kills G_1. Thus K kills G_1. Similarly, K kills G_2. Thus $G_1 + G_2 \subseteq A[K]$. On the other hand, if we write $A[K] = H_1 \oplus H_2$ with $H_i \subseteq A[I_i]$, we will show that $H_i \subseteq G_i$, so that $A[K] \subseteq G_1 + G_2$. Write $1 = e_1 + e_2$ with $e_i \in I_i$. Then the subsets $e_1 J_1 \subseteq I_2 J_1 \subseteq K$ and $e_2 J_1 \subseteq I_2$ kill H_1, so J_1 kills H_1; i.e., $H_1 \subseteq A[J_1] = G_1$. Similarly $H_2 \subseteq G_2$. So $A[K] \subseteq G_1 + G_2$. Hence $G_1 + G_2 = A[K]$, a kernel subgroup. □

6.2 Kernel subgroups of a power of an elliptic curve

Proposition 6.3. *Let E be an elliptic curve over a field, and let $r \in \mathbb{Z}_{\geqslant 0}$. Let $R := \operatorname{End} E$. For a subgroup scheme $G \subseteq E^r$, the following are equivalent:*

(i) *G is a kernel subgroup.*

(ii) *G is the kernel of a homomorphism $E^r \to E^s$ for some $s \in \mathbb{Z}_{\geqslant 0}$.*

(iii) *There exists a f.p. torsion-free R-module M such that $E^r/G \simeq \mathscr{H}om_R(M, E)$.*

(iv) *There exists a submodule $M \subseteq R^r$ such that applying $\mathscr{H}om_R(-, E)$ to*

$$0 \to M \to R^r \to R^r/M \to 0$$

yields

$$0 \to G \to E^r \to E^r/G \to 0.$$

Proof.

(i)⇒(ii): Suppose that G is a kernel subgroup, say $A[I]$. Let $f_1, \dots, f_n$ be generators for I. Then G is the kernel of $E^r \xrightarrow{(f_1,\dots,f_n)} (E^r)^n$.

(ii)⇒(iii): This is a special case of Theorem 4.4(c).

(iii)⇒(iv): If $E^r/G \simeq \mathscr{H}om_R(M, E)$ for some f.p. torsion-free M, then by Theorem 4.8(a), the natural surjection $E^r \twoheadrightarrow E^r/G$ comes from some injection $M \hookrightarrow R^r$. Applying $\mathscr{H}om_R(-, E)$ to

$$0 \to M \to R^r \to R^r/M \to 0$$

yields

$$0 \to H \to E^r \twoheadrightarrow E^r/G$$

for some H, which must be isomorphic to G.

(iv)⇒(ii): Choose a surjection $h\colon R^s \twoheadrightarrow M$. Applying $\mathscr{H}om_R(-, E)$ to the composition $R^s \overset{h}{\twoheadrightarrow} M \hookrightarrow R^r$ produces a homomorphism $E^r \twoheadrightarrow E^r/G \hookrightarrow E^s$ with kernel G.

(ii)⇒(i): We may increase s to assume that $r|s$. Then G is an intersection of s/r endomorphisms of E^r, so it is a kernel subgroup by Proposition 6.2(a). □

PROPOSITION 6.4. *Let E be an elliptic curve. Let $R := \operatorname{End} E$. Then the following are equivalent:*

(i) *For each $r \in \mathbb{Z}_{\geqslant 0}$, every subgroup scheme of E^r is a kernel subgroup.*
(ii) *For each $r \in \mathbb{Z}_{\geqslant 0}$, every finite subgroup scheme of E^r is a kernel subgroup.*
(iii) *The functors $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are inverse equivalences of categories.*

Proof.

(i)⇒(ii): Trivial.

(ii)⇒(iii): Suppose that A is an abelian variety isogenous to E^r. Then $A \simeq E^r/G$ for some finite subgroup scheme G. By assumption, G is a kernel subgroup. Proposition 6.3(i)⇒(iii) implies that A is in the image of $\mathscr{H}om_R(-, E)$. The result now follows from Theorem 4.8.

(iii)⇒(i): Let G be a subgroup scheme of E^r. Then E^r/G is isogenous to E^s for some $s \leqslant r$. By assumption, $\mathscr{H}om_R(-, E)$ is an equivalence of categories, so E^r/G is of the form $\mathscr{H}om_R(M, E)$. By Proposition 6.3(iii)⇒(i), G is a kernel subgroup. □

In the next few sections, we investigate when it holds that all finite subgroup schemes of powers of E are kernel subgroups, in order to determine when $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are inverse equivalences of categories.

6.3 Prime-to-p subgroups

We continue to assume that E is an elliptic curve and $R = \operatorname{End} E$. Let ℓ be a prime not equal to $\operatorname{char} k$. Let $R_\ell := R \otimes \mathbb{Z}_\ell$. The natural map $R_\ell \to \operatorname{End}_{\mathbb{Z}_\ell} T_\ell E$ is injective since an endomorphism that kills $E[\ell^n]$ for all n is 0, and has saturated image since an endomorphism that kills $E[\ell]$ is equal to ℓ times an endomorphism. Let $C := \operatorname{End}_{R_\ell} T_\ell E$, which is the commutant of R_ℓ in $\operatorname{End}_{\mathbb{Z}_\ell} T_\ell E \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$. For any elliptic curve, we have $\operatorname{rk} R \in \{1, 2, 4\}$, so one of the following holds:

(i) $R_\ell = \mathbb{Z}_\ell$ and $C = \mathrm{M}_2(\mathbb{Z}_\ell)$;
(ii) $R_\ell = C = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \alpha$, a $\mathbb{Z}_\ell$-algebra that is a saturated rank 2 $\mathbb{Z}_\ell$-submodule of $\mathrm{M}_2(\mathbb{Z}_\ell)$ for some $\alpha \in \mathrm{M}_2(\mathbb{Z}_\ell)$; or

(iii) $R_\ell = \mathrm{M}_2(\mathbb{Z}_\ell)$ and $C = \mathbb{Z}_\ell$.

(To see that $C = R_\ell$ in case (ii), one may argue as follows. By [Mum70, Corollary 3 in III.§19], the $\mathbb{Q}$-algebra $R \otimes \mathbb{Q}$ is semisimple, so $R \otimes \mathbb{Q}_\ell$ is either a degree 2 field extension of $\mathbb{Q}_\ell$, or is conjugate to $\mathbb{Q}_\ell \times \mathbb{Q}_\ell$. In either case, the commutant $C \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of $R \otimes \mathbb{Q}_\ell$ in $\mathrm{M}_2(\mathbb{Q}_\ell)$ is 2-dimensional. On the other hand, an algebra generated by one element is commutative, so C contains R_ℓ. Also, R_ℓ is saturated in $\mathrm{M}_2(\mathbb{Z}_\ell)$. The previous three sentences imply that $C = R_\ell$.)

Let $e \in \mathbb{Z}_{>0}$.

Lemma 6.5. *Every finitely generated left $C/\ell^e C$-module injects into a free $C/\ell^e C$-module.*

Proof. If $C = \mathbb{Z}_\ell$, this is trivial. For any ring A and positive integer n, the category of A-modules is equivalent to the category of $\mathrm{M}_n(A)$-modules [Lam99, Theorem 17.20], and the equivalence preserves injections, finite generation, and projectivity [Lam99, Remark 17.23(A)]; applying this to $A = \mathbb{Z}_\ell/\ell^e\mathbb{Z}_\ell$ and $n = 2$ shows that the case $C = \mathbb{Z}_\ell$ implies the case $C = \mathrm{M}_2(\mathbb{Z}_\ell)$.

Finally, suppose that C is of rank 2. Then $C/\ell^e C$ is free of rank 2 over $\mathbb{Z}/\ell^e\mathbb{Z}$; say with basis $1, \alpha$. For $c \in C/\ell^e C$, let $\lambda(c)$ be the coefficient of α in c. Multiplying any nonzero element of $\ker \lambda$ by α gives an element outside $\ker \lambda$. Therefore the pairing

$$\begin{aligned} C/\ell^e C \times C/\ell^e C &\longrightarrow \mathbb{Z}/\ell^e\mathbb{Z} \\ x, y &\longmapsto \lambda(xy) \end{aligned}$$

is a perfect pairing. In other words, the Pontryagin dual $(C/\ell^e C)^D$ is isomorphic to $C/\ell^e C$ as a $C/\ell^e C$-module. If M is a finitely generated $C/\ell^e C$-module, there exists a surjection $(C/\ell^e C)^r \twoheadrightarrow M^D$ for some $r \in \mathbb{Z}_{\geqslant 0}$; taking Pontryagin duals yields an injection

$$M \hookrightarrow ((C/\ell^e C)^r)^D \simeq (C/\ell^e C)^r. \qquad \square$$

Lemma 6.6. *The group $(T_\ell E)^2$ is free as an R_ℓ-module and as a C-module. The group $E[\ell^e](k_s)^2$ is free as an $R/\ell^e R$-module and as a $C/\ell^e C$-module.*

Proof. Since $E[\ell^e](k_s) = T_\ell E/\ell^e T_\ell E$, by Nakayama's lemma it is enough to check that $E[\ell](k_s)^2$ is free as an A-module, for $A = R/\ell R$ and for $A = C/\ell C$. Identify $E[\ell](k_s)^2$ with $\mathbb{F}_\ell^2$, so that $A \subseteq \mathrm{M}_2(\mathbb{F}_\ell)$. The case $A = \mathbb{F}_\ell$ is trivial. If A is $\mathbb{F}_\ell \oplus \mathbb{F}_\ell\alpha$ for some $\alpha \in \mathrm{M}_2(\mathbb{F}_\ell)$, then every faithful A-module of dimension 2 over $\mathbb{F}_\ell$ is free. If $A = \mathrm{M}_2(\mathbb{F}_\ell)$, then the free A-module A is a direct sum of two copies of $\mathbb{F}_\ell^2$ (the two column spaces). $\square$

Lemma 6.7. *The natural maps*

$$\begin{aligned} C/\ell^e C &\longrightarrow \mathrm{End}_{R/\ell^e R} E[\ell^e](k_s) \\ R/\ell^e R &\longrightarrow \mathrm{End}_{C/\ell^e C} E[\ell^e](k_s) \end{aligned}$$

are isomorphisms.

Proof. The first map is an isomorphism since $C = \mathrm{End}_{R_\ell} T_\ell E$ and C and R_ℓ are saturated in $\mathrm{End}\, T_\ell E \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$. Lemma 6.6 and [Lam99, Theorem 18.8(3)⇒(1)] imply that $E[\ell^e](k_s)$ is a generator of the category of finitely generated $R/\ell^e R$-modules, so [Lam99, Proposition 18.17(2)(d)] yields the second isomorphism. $\square$

Recall that $\mathcal{G}_k = \mathrm{Gal}(k_s/k)$. There is a group homomorphism $\mathcal{G}_k \to C^\times$ since each $\sigma \in \mathcal{G}_k$ respects the R-action on the groups $E[\ell^e](k_s)$ and $T_\ell E$.

Proposition 6.8. *Let E be an elliptic curve over a field k. Let ℓ, e, C be as above. Let G be a subgroup scheme of $E[\ell^e]^r$ for some r. Then G is a kernel subgroup if and only if $G(k_s)$ is a $C/\ell^e C$-submodule of $E[\ell^e]^r(k_s)$.*

Proof. Suppose that $G(k_s)$ is a $C/\ell^e C$-submodule of $E[\ell^e]^r(k_s)$. Let $H := E[\ell^e]^r/G$. Then $H(k_s)$ is a finitely generated $C/\ell^e C$-module. By Lemma 6.5, $H(k_s)$ injects into a free $C/\ell^e C$-module, which in turn injects into $E[\ell^e]^s(k_s)$ for some s. Because of the homomorphisms $\mathcal{G}_k \to C^\times \to (C/\ell^e C)^\times$, the $C/\ell^e C$-module homomorphism $H(k_s) \to E[\ell^e]^s(k_s)$ is a $\mathcal{G}_k$-module homomorphism, so it comes from a homomorphism $H \to E[\ell^e]^s$ of étale group schemes. The composition $E[\ell^e]^r \twoheadrightarrow H \hookrightarrow E[\ell^e]^s$ is given by an $s \times r$ matrix N_e with entries in $\operatorname{End}_{C/\ell^e C} E[\ell^e](k_s) = R/\ell^e R$ (the equality is Lemma 6.7). Lift N_e to $N \in \mathrm{M}_{s\times r}(R)$. Then G is the intersection of the kernel subgroups $E[\ell^e]^r$ and $\ker(N\colon E^r \to E^s)$. By Propositions 6.2(a) and 6.3 G is a kernel subgroup.

Conversely, if G is a kernel subgroup, say the kernel of $E^r \to E^s$, then it is also the kernel of $E[\ell^e]^r \to E[\ell^e]^s$, which is a homomorphism of $C/\ell^e C$-modules, so G is a $C/\ell^e C$-module. □

The group homomorphism $\mathcal{G}_k \to C^\times$ induces algebra homomorphisms $\mathbb{Z}_\ell[\mathcal{G}_k] \to C$ and $\mathbb{F}_\ell[\mathcal{G}_k] \to C/\ell C$.

Proposition 6.9. *Let E, k, ℓ, R, R_ℓ, C be as above. The following are equivalent:*

(i) *The homomorphism $\mathbb{F}_\ell[\mathcal{G}_k] \to C/\ell C$ is surjective.*

(ii) *The homomorphism $\mathbb{Z}_\ell[\mathcal{G}_k] \to C$ is surjective.*

(iii) *Every ℓ-power order subgroup scheme of E^r for every r is a kernel subgroup.*

Proof.

(i)⇒(ii): Nakayama's lemma.

(ii)⇒(iii): Let G be an ℓ-power subgroup scheme of E^r, say $G \subseteq E[\ell^e]^r$. Then $G(k_s)$ is a $\mathbb{Z}_\ell[\mathcal{G}_k]$-module. Since $\mathbb{Z}_\ell[\mathcal{G}_k] \to C$ is surjective, $G(k_s)$ is also a C-module, and hence a $C/\ell^e C$-module. By Proposition 6.8, G is a kernel subgroup.

(iii)⇒(i): Suppose that $\mathbb{F}_\ell[\mathcal{G}_k] \to C/\ell C$ is not surjective; let D be the image. The algebra $C/\ell C$ is one of $\mathbb{F}_\ell$, $\left\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)\right\} \simeq \mathbb{F}_\ell[\epsilon]/(\epsilon^2)$, $\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\right\} \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$, $\mathbb{F}_{\ell^2}$, or $\mathrm{M}_2(\mathbb{F}_\ell)$. The first is excluded since it has no nontrivial subalgebras. In the second, third, and fourth cases, D can only be $\mathbb{F}_\ell$, and it is easy to find a subspace of $\mathbb{F}_\ell^2 \simeq E[\ell](k_s)$ that is not a $C/\ell C$-module. In the fifth case, D is contained in a copy of either $\left\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\right\}$ or $\mathbb{F}_{\ell^2}$. Now $\left\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\right\}$ fixes a line in $\mathbb{F}_\ell^2$ not fixed by $\mathrm{M}_2(\mathbb{F}_\ell)$. And $\mathbb{F}_{\ell^2}$ fixes an $\mathbb{F}_{\ell^2}$-line in $\mathbb{F}_{\ell^2}^2 \simeq E^2[\ell](k_s)$ that is not fixed by $\mathrm{M}_2(\mathbb{F}_\ell)$. Thus in each case, there is a subgroup scheme of $E[\ell]$ or $E^2[\ell]$ that is not a $C/\ell C$-module, and hence by Proposition 6.8 not a kernel subgroup. □

6.4 *p*-power subgroups

Proposition 6.10. *Let E be an ordinary elliptic curve over a field k of characteristic p. Assume that $\operatorname{End} E \neq \mathbb{Z}$ (automatic if k is finite). Then every p-power order subgroup scheme $G \subseteq E^r$ is a kernel subgroup.*

Proof. The ring $R := \operatorname{End} E \simeq \operatorname{End} E_{\overline{k}}$ is a quadratic order. Although R is not necessarily a Dedekind domain, its conductor is prime to p, so it makes sense to speak of the splitting behavior of (p) in R. In fact, since E is ordinary, (p) splits, say as $\mathfrak{p}\mathfrak{q}$. So $E[p]$ is the direct sum of group schemes $E[\mathfrak{p}]$ and $E[\mathfrak{q}]$, each of order p by Theorem 4.4(e). Since E is ordinary, one of them, say $E[\mathfrak{p}]$, is étale, and the other is connected. For any $e \in \mathbb{Z}_{\geqslant 0}$, we have $(p^e) = \mathfrak{p}^e\mathfrak{q}^e$ so

$E[p^e] \simeq E[\mathfrak{p}^e] \oplus E[\mathfrak{q}^e]$. The Jordan–Hölder factors of $E[\mathfrak{p}^e]$ are isomorphic to $E[\mathfrak{p}]$, so $E[\mathfrak{p}^e]$ is étale; similarly $E[\mathfrak{q}^e]$ is connected. We have $G \subseteq E[p^e]^r$ for some e. By Proposition 6.2(c), we may assume that $G \subseteq E[\mathfrak{p}^e]^r$ or $G \subseteq E[\mathfrak{q}^e]^r$.

In the first case, $E[\mathfrak{p}^e](k^s) \simeq \mathbb{Z}/p^e\mathbb{Z}$, so G is the kernel of a homomorphism $E[\mathfrak{p}^e]^r \to E[\mathfrak{p}^e]^s$ given by a matrix in $\mathrm{M}_{s\times r}(\mathbb{Z})$. Since $E[\mathfrak{p}^e]$ is a kernel subgroup, so is $E[\mathfrak{p}^e]^r$, and so is G, by Propositions 6.2(a) and 6.3.

In the second case, we take Cartier duals: $E[\mathfrak{p}^e]^r \twoheadrightarrow G^\vee$. Then $G^\vee$ is the cokernel of some homomorphism $E[\mathfrak{p}^e]^s \to E[\mathfrak{p}^e]^r$ given by a matrix $N \in \mathrm{M}_{r\times s}(\mathbb{Z})$. So G is the kernel of the homomorphism $E[\mathfrak{q}^e]^r \to E[\mathfrak{q}^e]^s$ given by the transpose $N^T \in \mathrm{M}_{s\times r}(\mathbb{Z})$. Since $E[\mathfrak{q}^e]$ is a kernel subgroup, so is $E[\mathfrak{q}^e]^r$, and so is G, by Propositions 6.2(a) and 6.3. □

Proposition 6.11. *Let E be a supersingular elliptic curve over a field k of characteristic p.*

(a) *If $k = \mathbb{F}_p$, then every p-power order subgroup scheme $G \subseteq E^r$ is a kernel subgroup, and in fact is a kernel of an endomorphism of E^r.*

(b) *If $k = \mathbb{F}_{p^2}$ and $\operatorname{rk} R = 4$ (i.e., $\#E(\mathbb{F}_{p^2}) = (p \pm 1)^2$), then every subgroup scheme $G \subseteq E^r$ is a kernel subgroup.*

(c) *If $k = \mathbb{F}_{p^2}$ and $\operatorname{rk} R \neq 4$, then there exists a copy of $\boldsymbol{\alpha}_p$ in $E \times E$ that is not a kernel subgroup.*

(d) *If k is $\mathbb{F}_{p^a}$ for some $a \geqslant 3$, or if k is infinite, then there exists a copy of $\boldsymbol{\alpha}_p$ in $E \times E$ that is not a kernel subgroup.*

Proof. The kernel of $\pi_{E,p}\colon E \to E^{(p)}$ is $\boldsymbol{\alpha}_p$. Suppose that $\boldsymbol{\alpha}_p \subseteq E$ is a kernel subgroup. By Proposition 6.3(i)⇒(iv), $\boldsymbol{\alpha}_p \simeq \mathscr{H}\!om_R(R/I, E)$ for some left R-ideal I. By Theorem 4.4(e), $p = \#(R/I)^{2/\operatorname{rk} R}$. We have three cases:

- If $R = \mathbb{Z}$, this is a contradiction.
- If $\operatorname{rk} R = 2$, then $\#(R/I) = p$, so $R/I \simeq \mathbb{F}_p$. Since E is supersingular, p is ramified or inert in R, and the above implies that p is ramified.
- If $\operatorname{rk} R = 4$, then $\#(R/I) = p^2$, so I is the unique ideal of index p^2 in R, and $R/I \simeq \mathbb{F}_{p^2}$.

If J is an R-module with $I^2 \subsetneq J \subsetneq R^2$ (here I^2 means $I \times I$), then $R^2/J \simeq R/I$ (since R/I is a field), and the surjection $R^2 \twoheadrightarrow R^2/J$ gives rise to an injection $\boldsymbol{\alpha}_p \hookrightarrow E \times E$. Conversely, any *kernel* subgroup $\boldsymbol{\alpha}_p \subseteq E \times E$ arises from such a J. So such kernel subgroups are in bijection with $\mathbb{P}^1(R/I)$. On the other hand, $\operatorname{End} \boldsymbol{\alpha}_p \simeq k$, so $\operatorname{Hom}(\boldsymbol{\alpha}_p, E \times E) = k^2$, and the copies of $\boldsymbol{\alpha}_p$ in $E \times E$ are in bijection with $\mathbb{P}^1(k)$. Thus if every $\boldsymbol{\alpha}_p$ in $E \times E$ is a kernel subgroup, then $\mathbb{P}^1(R/I)$ is in bijection with $\mathbb{P}^1(k)$, so $\#(R/I) = \#k$; i.e., $k \simeq R/I$, which is $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ as above. This proves (c) and (d).

(a) By Lemma 5.9, $E^r \to E^r/G$ factors as a chain of p-isogenies, each with kernel $\boldsymbol{\alpha}_p$. If we show that any quotient $E^r/\boldsymbol{\alpha}_p$ is isomorphic to E^r, then each abelian variety in the chain must be isomorphic to E^r, so G is a kernel of an endomorphism of E^r, as desired.
The group $\mathrm{GL}_r(\mathbb{Z}) \subseteq \mathrm{GL}_r(\operatorname{End} E)$ acts on E^r, and acts transitively on the nonzero elements of $\operatorname{Hom}(\boldsymbol{\alpha}_p, E^r) = \mathbb{F}_p^r$. Therefore it suffices to consider the quotient $E^r/\boldsymbol{\alpha}_p$ in which the $\boldsymbol{\alpha}_p$ is contained in $E \times 0 \times \cdots \times 0$. Now $E/\boldsymbol{\alpha}_p = E/E[\pi_E] \simeq E$, so $E^r/\boldsymbol{\alpha}_p \simeq E^r$.

(b) The abelian variety E^r/G is isogenous to a power of E, so by Theorem 5.3(b), it is of the form $\mathscr{H}\!om_R(M, E)$. By Proposition 6.3(iii)⇒(i), G is a kernel subgroup. □

7. Abelian varieties isogenous to a power of an elliptic curve

Let E be an elliptic curve over k. We break into cases, first according to whether E is ordinary or supersingular, and next according to $\operatorname{rk} \operatorname{End} E$ and $\#k$. By convention, elliptic curves over a field of characteristic 0 are included among the ordinary curves.

7.1 E is ordinary and $\operatorname{rk} \operatorname{End} E = 1$

THEOREM 7.1. *Fix an elliptic curve E over a field k such that* $\operatorname{End} E \simeq \mathbb{Z}$.

(a) *The image of $\mathscr{H}om_R(-, E)$ consists of abelian varieties* isomorphic *to a power of E.*

(b) *The functors $\mathscr{H}om_R(-, E)$ and* $\operatorname{Hom}(-, E)$ *are inverse equivalences of categories (i.e., every abelian variety isogenous to a power of E is isomorphic to a power of E) if and only if* $\operatorname{char} k = 0$ *and for every prime ℓ the homomorphism* $\mathbb{F}_\ell[\mathcal{G}_k] \to \operatorname{End} E[\ell](k_s) \simeq \mathrm{M}_2(\mathbb{F}_\ell)$ *is surjective.*

Proof of Theorem 7.1.

(a) Every f.p. torsion-free $\mathbb{Z}$-module is free.

(b) By Proposition 6.4, $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are equivalences if and only if every finite subgroup scheme G is a kernel subgroup. By Proposition 6.2(c), we need only consider G of prime power order.
If $\operatorname{char} k = p > 0$, then $\# \ker \pi_{E,p} = p$, but $\#E[I]$ is a square for every nonzero ideal $I \subseteq \mathbb{Z}$, so $\ker \pi_{E,p}$ is not a kernel subgroup. If $\operatorname{char} k = 0$, then apply Proposition 6.9(i)$\Leftrightarrow$(iii) for every ℓ. □

Remark 7.2. Surjectivity of $\mathbb{F}_\ell[\mathcal{G}_k] \to \mathrm{M}_2(\mathbb{F}_\ell)$ *fails* if and only if the image G of $\mathcal{G}_k \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is contained in a Borel subgroup or a nonsplit Cartan subgroup, as we now explain. Let A be the image of $\mathbb{F}_\ell[\mathcal{G}_k] \to \mathrm{M}_2(\mathbb{F}_\ell)$. View $V := \mathbb{F}_\ell^2$ as an A-module. If V is reducible, then surjectivity fails and G is contained in a Borel subgroup. So suppose that V is irreducible. By Schur's lemma [Lan02, XVII.1.1], $\operatorname{End}_A V$ is a division algebra D. But $D \subseteq \mathrm{M}_2(\mathbb{F}_\ell)$, so D is $\mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$. By Wedderburn's theorem [Lan02, XVII.3.5], $A \simeq \operatorname{End}_D V$. If $D = \mathbb{F}_\ell$, then $A = \mathrm{M}_2(\mathbb{F}_\ell)$, and G is not contained in a Borel subgroup or a nonsplit Cartan subgroup. If $D \simeq \mathbb{F}_{\ell^2}$, then $\dim_D V = 1$, so $A \simeq \operatorname{End}_D V \simeq \mathbb{F}_{\ell^2}$, and G is contained in the nonsplit Cartan subgroup $A \cap \mathrm{GL}_2(\mathbb{F}_\ell)$.

Example 7.3. Let E be the elliptic curve $X_0(11)$ over $\mathbb{Q}$, with equation $y^2 + y = x^3 - x^2 - 10x - 20$. As in [Ser72, 5.5.2], the image of $\mathcal{G}_\mathbb{Q} \to \operatorname{Aut} E[5] \simeq \mathrm{GL}_2(\mathbb{F}_5)$ is contained in a Borel subgroup, so by Theorem 7.1(b) and Remark 7.2, the functors $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are *not* inverse equivalences of categories.

Example 7.4. Let E be the elliptic curve over $\mathbb{Q}$ of conductor 37 with equation $y^2 + y = x^3 - x$. By [Ser72, 5.5.6], the homomorphism $\mathcal{G}_\mathbb{Q} \to \operatorname{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective for every prime ℓ, so by Theorem 7.1(b), the functors $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ *are* inverse equivalences of categories.

7.2 E is ordinary and $\operatorname{rk} \operatorname{End} E = 2$

Fix an ordinary elliptic curve E over a field k such that $\operatorname{rk} \operatorname{End} E = 2$. (These are called *CM elliptic curves* in [Kan11, Section 3].) Then $\operatorname{End} E \simeq \operatorname{End} E_{\overline{k}}$, because if an endomorphism becomes divisible by a positive integer n over an extension field, it kills $E[n]$, so it is divisible by n already over k. Let $R := \operatorname{End} E$ and $K := \operatorname{Frac} R$.

If E' is an elliptic curve isogenous to E, then $\operatorname{End} E'$ is another order R' in K. Let $f_{E'}$ be the conductor of R', i.e., the index of R' in its integral closure. More generally, if A is an abelian variety isogenous to E^r, then $\operatorname{End} A$ is an order in $M_r(K)$, and its center $Z(\operatorname{End} A)$ is an order in $Z(M_r(K)) = K$, and we let f_A be the conductor of $Z(\operatorname{End} A)$.

Theorem 7.5. *Fix an ordinary elliptic curve E over a field k such that $\operatorname{rk}\operatorname{End} E = 2$. Let $R := \operatorname{End} E$. The image of $\mathscr{H}om_R(-, E)$ consists of the abelian varieties A isogenous to a power of E such that $f_A | f_E$, i.e., such that $R \subseteq Z(\operatorname{End} A)$. These are exactly the products of elliptic curves E' each isogenous to E and satisfying $f_{E'} | f_E$.*

Proof. Suppose that $\phi\colon E^r \to A$ is an isogeny and $f_A | f_E$. Since $f_A | f_E$, there is an R-action on A such that ϕ respects the R-actions. Let $G := \ker \phi$, so $G(k_s)$ is an R-module. Write $G = \bigoplus_\ell G_\ell$, where G_ℓ is a group scheme of ℓ-power order. For $\ell \neq \operatorname{char} k$, we are in the case $R_\ell = C$ of Section 6.3, so $G_\ell(k_s)$ is also a $C/\ell^e C$-module for some e, and Proposition 6.8 shows that G_ℓ is a kernel subgroup. If $\operatorname{char} k = p > 0$, then G_p is a kernel subgroup by Proposition 6.10. By Proposition 6.2(c), G is a kernel subgroup. By Proposition 6.3(i)⇒(iii), the abelian variety $A \simeq E^r/G$ is in the image of $\mathscr{H}om_R(-, E)$.

Conversely, if A is in the image of $\mathscr{H}om_R(-, E)$ then by Theorem 4.8(c), A is a product of elliptic curves of the form $\mathscr{H}om_R(I, E)$. Because the functor $\mathscr{H}om_R(-, E)$ is fully faithful, if $E' = \mathscr{H}om_R(I, E)$ then E' is isogenous to E and $\operatorname{End} E' \simeq \operatorname{End}_R I$, which contains R since R is commutative. In particular, $f_{E'} | f_E$. Finally, f_A is the least common multiple of the $f_{E'}$, so $f_A | f_E$ too. □

Theorem 7.6. *Fix an ordinary elliptic curve E over a finite field $\mathbb{F}_q$. Let $R := \operatorname{End} E$. Then $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are equivalences of categories if and only if $\mathbb{Z}[\pi_E] = R$.*

Proof. Suppose that $\mathbb{Z}[\pi_E] = R$. If A is isogenous to a power of E, then π_A has the same minimal polynomial as π_E, so $Z(\operatorname{End} A)$ contains $\mathbb{Z}[\pi_A] \simeq \mathbb{Z}[\pi_E]$; i.e., $f_A | f_E$ is automatic.

On the other hand, if $\mathbb{Z}[\pi_E] \neq R$, then E is isogenous to an elliptic curve E' satisfying $\operatorname{End} E' = \mathbb{Z}[\pi_{E'}]$ [Wat69, Theorem 4.2(2)]. Theorem 7.5 shows that E' is not in the image of $\mathscr{H}om_R(-, E)$, so $\mathscr{H}om_R(-, E)$ is not an equivalence of categories. □

We can also give a more general criterion that applies even if k is not finite.

Theorem 7.7. *Fix an ordinary elliptic curve E over a field k such that $\operatorname{rk}\operatorname{End} E = 2$. Then $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are equivalences of categories if and only if for every prime $\ell \neq \operatorname{char} k$, there exists $\sigma \in \mathcal{G}_k$ whose action on $E[\ell](k_s)$ is not multiplication by a scalar.*

Proof. By Propositions 6.4(i)⇔(iii), 6.2(c), and 6.10, the functors $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are equivalences if and only if for each $\ell \neq \operatorname{char} k$, the homomorphism $\mathbb{F}_\ell[\mathcal{G}_k] \to C/\ell C$ is surjective. Since $\dim_{\mathbb{F}_\ell} C/\ell C = 2$, surjectivity is equivalent to the image of

$$\mathbb{F}_\ell[\mathcal{G}_k] \longrightarrow C/\ell C \subseteq \operatorname{End} E[\ell](k_s) \simeq \mathrm{M}_2(\mathbb{F}_\ell)$$

not being $\mathbb{F}_\ell$. □

Example 7.8. Let E be the elliptic curve $y^2 = x^3 - x$ over $k := \mathbb{Q}(\sqrt{-1})$; then $j(E) = 1728$ and $\operatorname{End} E = \mathbb{Z}[\sqrt{-1}]$. The group $\mathcal{G}_k$ acts trivially on $E[2](k_s)$, so by Theorem 7.7, the functors $\mathscr{H}om_R(-, E)$ and $\operatorname{Hom}(-, E)$ are *not* inverse equivalences of categories.

Example 7.9. Let E be the elliptic curve $y^2 = x^3 + x^2 - 3x + 1$ over $k := \mathbb{Q}(\sqrt{-2})$; then $j(E) = 8000$ and $\operatorname{End} E = \mathbb{Z}[\sqrt{-2}]$. The field $k(E[2])$ equals $k(\sqrt{-1})$, so the image of $\mathcal{G}_k$ in $\mathrm{GL}_2(\mathbb{F}_2)$ has order

2 and hence does not consist of scalars. Now consider a prime $\ell > 2$. Choose a prime $p \neq \ell$ such that p splits in $k/\mathbb{Q}$ and $\left(\frac{p}{\ell}\right) = -1$. Let σ be a Frobenius element of $\mathcal{G}_k$ at a prime above p. The image of σ in $\operatorname{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ has nonsquare determinant ($p \bmod \ell$), so it is not a scalar. Thus, by Theorem 7.7, the functors $\mathscr{H}om_R(-,E)$ and $\operatorname{Hom}(-,E)$ *are* inverse equivalences of categories.

Remark 7.10. If E and E' are ordinary elliptic curves over an algebraically closed field k and their endomorphism rings are orders in the same quadratic field, then E and E' are isogenous. But over non-algebraically closed fields, this can fail. For example, if E is an ordinary elliptic curve over a finite field, then its quadratic twist E' has the same endomorphism ring, but opposite trace of Frobenius, so E and E' are not isogenous.

7.3 E is supersingular and $k = \mathbb{F}_p$

Fix a supersingular elliptic curve E over $\mathbb{F}_p$. Let $R := \operatorname{End} E$. Let $P(x)$ be the characteristic polynomial of $\pi := \pi_E$. Define f_A as in Section 7.2. In particular, f_E is the conductor of R. We have the following cases:

prime	$P(x)$	$\mathbb{Z}[\pi]$	$R = \operatorname{End} E$	f_E	equivalence?
$p \not\equiv 3 \pmod 4$	x^2+p	$\mathbb{Z}\left[\sqrt{-p}\right]$	$\mathbb{Z}\left[\sqrt{-p}\right]$	1	YES
$p \equiv 3 \pmod 4$	x^2+p	$\mathbb{Z}\left[\sqrt{-p}\right]$	$\mathbb{Z}\left[\sqrt{-p}\right]$	2	YES
$p \equiv 3 \pmod 4$	x^2+p	$\mathbb{Z}\left[\sqrt{-p}\right]$	$\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$	1	NO
$p = 2$	$x^2 \pm 2x + 2$	$\mathbb{Z}[i]$	$\mathbb{Z}[i]$	1	YES
$p = 3$	$x^2 \pm 3x + 3$	$\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$	$\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$	1	YES

The last column, which indicates when $\mathscr{H}om_R(-,E)$ and $\operatorname{Hom}(-,E)$ are equivalences of categories, is explained by the following analogues of Theorems 7.5 and 7.6, proved in the same way except that we use Proposition 6.11(a) in place of Proposition 6.10.

Theorem 7.11. *Fix a supersingular elliptic curve E over $\mathbb{F}_p$. Let $R := \operatorname{End} E$. The image of $\mathscr{H}om_R(-,E)$ consists of the abelian varieties A isogenous to a power of E such that $f_A | f_E$, i.e., such that $R \subseteq Z(\operatorname{End} A)$. These are exactly the products of elliptic curves E' each isogenous to E and satisfying $f_{E'} | f_E$.*

Theorem 7.12. *Fix a supersingular elliptic curve E over $\mathbb{F}_p$. Let $R := \operatorname{End} E$. Then $\mathscr{H}om_R(-,E)$ and $\operatorname{Hom}(-,E)$ are equivalences of categories if and only if $\mathbb{Z}[\pi_E] = R$.*

7.4 E is supersingular, $k = \mathbb{F}_{p^2}$, and $\operatorname{rk} \operatorname{End} E = 4$

In this case, E is a maximal or minimal elliptic curve over $\mathbb{F}_{p^2}$. These cases were already handled: see Theorem 5.3.

7.5 E is supersingular, $k = \mathbb{F}_{p^2}$, and $\operatorname{rk} \operatorname{End} E = 2$

By Proposition 6.11(c), not every subgroup scheme is a kernel subgroup. By Proposition 6.4(iii)$\Leftrightarrow$(ii), the functors $\mathscr{H}om_R(-,E)$ and $\operatorname{Hom}(-,E)$ are not equivalences of categories.

Remark 7.13. These are the cases in which the characteristic polynomial of π_E is one of x^2+px+p^2, x^2+p^2, or x^2-px+p^2. Hence $\pi_E = p\zeta$ for a root of unity ζ of order 3, 4, or 6, respectively. But p does not divide the conductor of R, so $\zeta \in R$. Now $\zeta \in \operatorname{Aut} E$, so E has j-invariant 0 or 1728.

7.6 E is supersingular and $\#k > p^2$

By Proposition 6.11(d), not every subgroup scheme is a kernel subgroup. By Proposition 6.4(iii)$\Leftrightarrow$(ii), the functors $\mathscr{H}om_R(-,E)$ and $\operatorname{Hom}(-,E)$ are not equivalences of categories.

8. A partial generalization to higher-dimensional abelian varieties over $\mathbb{F}_p$

Let B be an abelian variety over a prime field $\mathbb{F}_p$. Let $R \subseteq \operatorname{End} B$ be the (central) subring $\mathbb{Z}[F,V]$ generated by the Frobenius and Verschiebung endomorphisms. Given a f.p. reflexive R-module M, let $M^* := \operatorname{Hom}_R(M,R)$; then M^* is reflexive too.

As in the case of elliptic curves, we can define functors

$$\mathscr{H}om_R(-,B)\colon \{\text{f.p. } R\text{-modules}\}^{\text{opp}} \longrightarrow \{\text{commutative proper group schemes over } \mathbb{F}_p\}$$

and

$$\operatorname{Hom}(-,B)\colon \{\text{commutative proper group schemes over } \mathbb{F}_p\} \longrightarrow \{\text{f.p. } R\text{-modules}\}^{\text{opp}}.$$

The work of Centeleghe and Stix [CS15], combined with some further arguments, allows us to analyze this higher-dimensional case. The main extra ingredient we supply is that, under appropriate hypotheses, the functor $M \mapsto M^* \otimes_R B$ implicit in [CS15] is isomorphic to $\mathscr{H}om_R(-,B)$.

Theorem 8.1. *Let B be an abelian variety over $\mathbb{F}_p$. Let $R = \mathbb{Z}[F,V] \subseteq \operatorname{End} B$. Then the functors $\mathscr{H}om_R(-,B)$ and $\operatorname{Hom}(-,B)$ restrict to inverse equivalences of categories*

$$\{\text{f.p. reflexive } R\text{-modules}\}^{\text{opp}} \rightleftarrows \{\text{abelian variety quotients of powers of } B\}$$

if and only if $R = \operatorname{End} B$. Moreover, in this case, the functor $\mathscr{H}om_R(-,B)$ so restricted is exact, and it is isomorphic to the functor $M \mapsto M^* \otimes B$.

Proof. If the functors give inverse equivalences as stated, then the argument in the paragraph before Theorem 4.8 proves that $R = \operatorname{End} B$.

Now let us prove the converse. Suppose that $R = \operatorname{End} B$. Then $(\operatorname{End} B) \otimes \mathbb{Q}$ is commutative. This implies that in the decomposition of B into simple factors up to isogeny, no factor is repeated, and also no factor is associated to the Weil number $\sqrt{p}$, since such a factor would give a direct factor of $(\operatorname{End} B) \otimes \mathbb{Q}$ isomorphic to a quaternion algebra over $\mathbb{Q}(\sqrt{p})$: see [Wat69, p. 528, Case 2]. Let w be the set of Weil number conjugacy classes associated to B. Then the category AV_w of [CS15, 5.1] is the category of abelian variety quotients of powers of B. The ring R_w in [CS15, Definition 2] is $R = \mathbb{Z}[F,V]$. It is Gorenstein by [CS15, Theorem 11(2)]. Reflexive finitely generated R-modules are the same as f.p. torsion-free R-modules, or equivalently f.p. R-modules that are free over $\mathbb{Z}$ [CS15, Lemma 13]. By [CS15, Proposition 24], for every prime ℓ the $(R \otimes \mathbb{Z}_\ell)$-module $T_\ell B$ (Tate module or contravariant Dieudonné module) is free of rank 1, so the abelian variety A_w in [CS15, Proposition 21] may be taken to be B by [CS15, Proposition 24].

We now check that if M is a f.p. torsion-free R-module, then the commutative proper group scheme $G := \mathscr{H}om_R(M,B)$ is an abelian variety. It suffices to prove that for every prime ℓ and $n \geqslant 0$, the homomorphism $G[\ell^{n+1}] \xrightarrow{\ell} G[\ell^n]$ is surjective. Choose a presentation $R^a \xrightarrow{N} R^b \to M \to 0$, so $G := \ker(B^b \to B^a)$. Both M and M^* are reflexive R-modules, so they are free over $\mathbb{Z}$.

Suppose that $\ell \neq p$. Then

$$\begin{aligned}
G[\ell^n] &= (\ker(B^b \to B^a))[\ell^n] \\
&= \ker(B^b[\ell^n] \to B^a[\ell^n]) \\
&\simeq \ker(T_\ell(B^b)/\ell^n \to T_\ell(B^a)/\ell^n) \\
&= \ker((R/\ell^n)^b \xrightarrow{N^T} (R/\ell^n)^a) \\
&= \ker(\operatorname{Hom}_R(R^b, R/\ell^n) \xrightarrow{N^T} \operatorname{Hom}_R(R^a, R/\ell^n)) \\
&\simeq \operatorname{Hom}_R(M, R/\ell^n) \\
&\simeq M^*/\ell^n \quad (\text{since } \operatorname{Ext}^1_R(M,R) = 0 \text{ by [CS15, Lemma 17]}) \\
&= M^* \underset{\mathbb{Z}}{\otimes} \frac{\ell^{-n}\mathbb{Z}}{\mathbb{Z}}.
\end{aligned}$$

Since M^* is free over $\mathbb{Z}$, the homomorphism

$$M^* \underset{\mathbb{Z}}{\otimes} \frac{\ell^{-(n+1)}\mathbb{Z}}{\mathbb{Z}} \xrightarrow{\ \ell\ } M^* \underset{\mathbb{Z}}{\otimes} \frac{\ell^{-n}\mathbb{Z}}{\mathbb{Z}}$$

is surjective, so $G[\ell^{n+1}] \xrightarrow{\ell} G[\ell^n]$ is surjective.

Now suppose that $\ell = p$. For each commutative group scheme H over $\mathbb{F}_p$, let H^D denote its contravariant Dieudonné module. Since the $R \otimes \mathbb{Z}_p$-module $T_p B$ is free of rank 1, we have $B[p^n]^D \simeq R/p^n$ as an R-module. Next,

$$\begin{aligned}
G[p^n]^D &= \operatorname{coker}\left(B^a[p^n]^D \to B^b[p^n]^D\right) \\
&\simeq \operatorname{coker}\left((R/p^n)^a \xrightarrow{N} (R/p^n)^b\right) \\
&= M/p^n.
\end{aligned}$$

Since M is free over $\mathbb{Z}$, the homomorphism $M/p^n \xrightarrow{p} M/p^{n+1}$ is injective, so $G[p^n]^D \xrightarrow{p} G[p^{n+1}]^D$ is injective, so $G[p^{n+1}] \xrightarrow{p} G[p^n]$ is surjective.

Thus G is an abelian variety. The proof of Theorem 4.4(b) now shows that $\mathscr{H}om_R(-,B)$ is exact. In particular, if $0 \to M \to R^n \to R^m$ is an exact sequence of R-modules, then $B^m \to B^n \to \mathscr{H}om_R(M,B) \to 0$ is exact. But $M^* \otimes B$ too is defined as $\operatorname{coker}(B^m \to B^n)$, so $\mathscr{H}om_R(M,B) \simeq M^* \otimes_R B$, and this holds functorially in M.

Finally, by [CS15, Theorem 25 and p. 247],

$$\operatorname{Hom}(-,B)\colon \mathsf{AV}_w \longrightarrow \{\text{f.p. reflexive } R\text{-modules}\}^{\text{opp}}$$

is an equivalence of categories with inverse functor $M \mapsto M^* \otimes_R B$. We may replace the latter with the isomorphic functor $\mathscr{H}om_R(-,B)$. $\square$

Remark 8.2. Over $\mathbb{F}_{p^n}$ with $n > 1$, the functors $\mathscr{H}om_R(-,B)$ and $\operatorname{Hom}(-,B)$ are sometimes inverse equivalences of categories, and sometimes not, as we saw already in the case of elliptic curves: see Theorem 1.1.

ACKNOWLEDGEMENTS

It is a pleasure to thank Everett Howe, Tony Scholl, and Christopher Skinner for helpful discussions. We thank also the referees for valuable suggestions on the exposition.

References

BGGP05 M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, Finiteness results for modular curves of genus at least 2, *Amer. J. Math.* **127** (2005), 1325–1387.

Bas63 H. Bass, On the ubiquity of Gorenstein rings, *Math. Z.* **82** (1963), 8–28.

BF60 Z. I. Borevič and D. K. Faddeev, Integral representations of quadratic rings, *Vestik Leningrad Univ.* **15** (1960), no. 19, 52–64.

BF65 Z. I. Borevič and D. K. Faddeev, Representations of orders with a cyclic index, *Proc. Steklov Inst. Math.* **80** (1965), 51–65; translated in *Algebraic number theory and representations* (ed. D. K. Faddeev), Amer. Math. Society, 56–72, 1968.

Bou70 N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 1 á 3*, Hermann, Paris, 1970.

CS15 T. G. Centeleghe and J. Stix, Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$, *Algebra Number Theory* **9** (2015), no. 1, 225–265.

Del69 P. Deligne, Variétés abéliennes ordinaires sur un corp fini, *Invent. Math.* **8** (1969), 238–243.

Eic38 M. Eichler, Über die Idealklassenzahl hyperkomplexer Systeme, *Math. Z.* **43** (1938), 481–494.

Gir68 J. Giraud, Remarque sur une formule de Shimura-Taniyama, *Invent. Math.* **5** (1968), 231–236.

Gro61 A. Grothendieck, Techniques de construction et théorèmes d'existence en géomtrie algébrique III: préschemas quotients, Séminaire Bourbaki 13e année, 1960/61, no. 212.

Kan11 E. Kani, Products of CM elliptic curves, *Collect. Math.* **62** (2011), 297–339.

Lam99 T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics **189**, Springer-Verlag, New York, 1999.

Lan02 S. Lang, *Algebra*, revised 3rd edition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

Lan75 H. Lange, Produkte elliptischer Kurven, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* (1975), 95–108.

Lau02 K. Lauter, The maximum or minimum number of rational points on genus three curves over finite fields, with an appendix by J.-P. Serre, *Compositio Math.* **134** (2002), 87–111.

Lev85 L. Levy, Modules over Dedekind-like rings, *J. Algebra* **93** (1985), 1–116.

LO98 K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Springer-Verlag, 1998.

Mes86 J.-F. Mestre, La méthode des graphes. Exemples et applications, pp. 217–242 in: *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, Nagoya Univ., Nagoya, 1986.

Mum70 D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research and Oxford University Press, 1970.

Ogu79 A. Ogus, Supersingular K3 crystals, Journées Géom. Algébr. Rennes 1978, Vol. II, *Astérisque* **64**, Soc. Math. France (1979), 3–86.

Oor75 F. Oort, Which abelian surfaces are products of elliptic curves?, *Math. Ann.* **214** (1975), 35–47.

Rei03 I. Reiner, *Maximal Orders*, Oxford University Press, 2003.

Sal02 L. Salce, Warfield domains: module theory from linear algebra to commutative algebra through abelian groups, *Milan J. Math.* **70** (2002), 163–185.

Sch92 C. Schoen, Produkte abelscher Varietäten und Moduln über Ordnungen, *J. Reine Angew. Math.* **429** (1992), 115–123.

Ser72 J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

Ser85 J.-P. Serre, Rational points on curves over finite fields, Part I: "q large", lectures given at Harvard University, September to December 1985, notes taken by Fernando Gouvêa.

Shi79 T. Shioda, Supersingular $K3$ surfaces, pp. 564–591 in: *Algebraic geometry*, Copenhagen 1978 (ed. K. Lønsted), Lecture Notes in Math. **732**, Springer-Verlag, 1979.

SM74 T. Shioda and N. Mitani, Singular abelian surfaces and binary quadratic forms, pp. 259–287 in: *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Math. **412**, Springer-Verlag, 1974.

Tat66 J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.

Wat69 W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.

Yu12 C.-F. Yu, Superspecial abelian varieties over finite prime fields, *J. Pure Appl. Algebra* **216** (2012), 1418-1427.

Bruce W. Jordan bruce.jordan@baruch.cuny.edu
Department of Mathematics, Baruch College, The City University of New York, One Bernard Baruch Way, New York, NY 10010-5526, USA

Allan G. Keeton agk@idaccr.org
Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540-1966, USA

Bjorn Poonen poonen@math.mit.edu
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Eric M. Rains rains@caltech.edu
Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA

Nicholas Shepherd-Barron nicholas.shepherd-barron@kcl.ac.uk
Mathematics Department, King's College London, Strand, London WC2R 2LS, United Kingdom

John T. Tate Tate@math.utexas.edu
Mathematics Department, Harvard University, 1 Oxford Street, Cambridge MA 02138-2901, USA