Noname manuscript No.
(will be inserted by the editor)

Grothendieck groups of categories of abelian varieties

Ari Shnidman

Received: date / Accepted: date

Abstract We compute the Grothendieck group of the category of abelian varieties over an algebraically closed field k. We also compute the Grothendieck group of the category of A-isotypic abelian varieties, for any simple abelian variety A, assuming k has characteristic 0, and for any elliptic curve A in any characteristic.

Keywords Abelian varieties · Grothendieck grops · elliptic curves

Mathematics Subject Classification (2000) 11G10 · 14K99 · 19A99

1 Introduction

The purpose of this note is to determine the Grothendieck groups of various categories of abelian varieties. If $\mathscr{C}$ is an exact category, then the Grothendieck group $K_0(\mathscr{C})$ is the quotient of the free abelian group generated by isomorphism classes in $\mathscr{C}$ modulo the relations $[X]-[Y]+[Z]$, for any exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathscr{C}$.

Let $\mathscr{A}$ be the category of abelian varieties over an algebraically closed field k. The morphisms in $\mathscr{A}$ are homomorphisms of abelian varieties. Kernels do not necessarily exist in $\mathscr{A}$, but cokernels do exist, and $\mathscr{A}$ is an exact category.

To compute the Grothendieck group $K_0(\mathscr{A})$, it is helpful to consider the simpler category $\tilde{\mathscr{A}}$ of abelian varieties up to isogeny. This category has the same objects as $\mathscr{A}$, and

$$\mathrm{Hom}_{\tilde{\mathscr{A}}}(A,B) = \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q},$$

for $A, B \in \mathrm{Ob}(\tilde{\mathscr{A}})$. The category $\tilde{\mathscr{A}}$ is semisimple by Poincaré's complete reducibility theorem, so that

$$K_0(\tilde{\mathscr{A}}) \cong \bigoplus_A \mathbb{Z}[A],$$

A. Shnidman
Boston College
Tel.: +1-617-552-3741
E-mail: shnidman@bc.edu
ORCID: 0000-0003-4689-2908

where the direct sum is over representatives of simple isogeny classes of abelian varieties. We have a surjective map $\iota\colon K_0(\mathscr{A}) \to K_0(\tilde{\mathscr{A}})$ which sends an abelian variety to its isogeny class. In fact:

Theorem 1 *The map ι is an isomorphism. In particular, any additive function $\mathrm{Ob}(\mathscr{A}) \to G$ to an abelian group G is an isogeny invariant.*

The proof of Theorem 1, which was suggested to us by Julian Rosen, uses a trick involving non-isotypic abelian varieties to reduce to showing the following fact: for every finite group scheme G over k of prime order, there is an abelian variety A over k with an endomorphism whose kernel is isomorphic to G. This fact is easily proved using the arithmetic of elliptic curves. Thus, the proof of Theorem 1 exploits the fact that certain elliptic curves have extra endomorphisms, and does not shed much light on the structure of the category $\mathscr{A}$.

For example, one consequence of Theorem 1 is that an abelian variety A and its dual $\hat{A}$ determine the same class in $K_0(\mathscr{A})$. It is then natural to ask whether we can witness the relation $[A] = [\hat{A}]$ in $K_0(\mathscr{A})$, using only short exact sequences that are intrinsic to A. In other words, we ask for short exact sequences involving only abelian varieties that can be constructed from A or $\hat{A}$ in some natural way, and that don't involve auxiliary abelian varieties such as CM elliptic curves. One way to formalize this question is as follows.

Let A be a simple abelian variety of dimension g. Write $\mathscr{C}_A$ for the category of abelian varieties B isogenous to A^n for some $n \geq 0$, with morphisms as usual. We will write $K_0(A)$ for $K_0(\mathscr{C}_A)$, but notice that this group depends only on the isogeny class of A. One can then ask whether it is true that $[A] = [\hat{A}]$ in $K_0(A)$. It will follow from our main result below that the answer is typically no.

Write $G(A)$ for the kernel of the map $\dim\colon K_0(A) \to \mathbb{Z}$ sending $[A]$ to $\dim A$. The group $G(A)$ measures the difference between the category $\mathscr{C}_A$ and its isogeny category $\tilde{\mathscr{C}}_A$. We will describe $G(A)$ in terms of the endomorphism algebra $D = \mathrm{End}(A) \otimes \mathbb{Q}$, assuming k has characteristic 0. So let us assume $\mathrm{char}\, k = 0$ until further notice. Let F be the center of D, and write $e = [F:\mathbb{Q}]$ and $d^2 = [D:F]$. Also let F^+ be the set of non-zero elements of F which are positive at all the ramified real places of D. Then our main result is:

Theorem 2 *Let $\mathbb{Q}_+$ be the group of positive rational numbers under multiplication. Then there is a canonical isomorphism*

$$\deg\colon G(A) \simeq \mathbb{Q}_+ \big/ \mathrm{Nm}_{F/\mathbb{Q}}\left(F^+\right)^{2g/de},$$

which, for any two simple $A_1, A_2 \in \mathrm{Ob}(\mathscr{C}_A)$, sends the class of $[A_1] - [A_2]$ to the class of the degree of any isogeny $A_1 \to A_2$.

This shows that even though $\iota\colon K_0(\mathscr{A}) \to K_0(\tilde{\mathscr{A}})$ is an isomorphism, the Grothendieck group of the A-isotypic part of $\mathscr{A}$ is very far from isomorphic to the Grothendieck group of the A-isotypic part of $\tilde{\mathscr{A}}$. Indeed:

Corollary 1 *The group $G(A)$ is an infinite torsion group.*

Proof The group $\mathbb{Q}_+/\mathrm{Nm}_{F/\mathbb{Q}}\left(F^+\right)^{2g/de}$ is torsion since every integer has a power which is a norm from F. If $\mathbb{Q}_+/\mathrm{Nm}_{F/\mathbb{Q}}\left(F^+\right)^{2g/de}$ is finite, then we must have $2g = de$. By the classification of endomorphism algebras of abelian varieties in characteristic 0, this implies that F is a CM field of degree $e > 1$. But then $\mathrm{Nm}_{F/\mathbb{Q}}(F^\times)$ has infinite index in $\mathbb{Q}^\times$, which contradicts the assumption that $\mathbb{Q}_+/\mathrm{Nm}_{F/\mathbb{Q}}\left(F^+\right)$ is finite. □

Duality fits nicely into this picture as well:

Theorem 3 *The automorphism* $[B] \mapsto [\hat{B}]$ *of* $K_0(A)$ *is inversion on* $G(A)$.

Remark 1 Note that duality does not induce inversion on all of $K_0(A)$, as the map $[A] \mapsto -[A]$ does not preserve dimension.

This lets us exhibit many cases where $[A] \neq [\hat{A}]$ in $K_0(A)$.

Example 1 If A is an abelian surface with $\mathrm{End}(A) = \mathbb{Z}$, then Theorem 2 gives

$$G(A) \simeq \mathbb{Q}_+/\mathbb{Q}_+^4 \simeq \bigoplus_\ell \mathbb{Z}/4\mathbb{Z},$$

with the direct sum over all primes ℓ. Suppose A admits an isogeny $A_0 \to A$ of degree ℓ from a principally polarized surface A_0; in particular $A_0 \simeq \hat{A}_0$. Then $[A] = [\hat{A}]$ in $K_0(A)$ if and only if $[A_0] - [A] = [A_0] - [\hat{A}]$ in $G(A)$. By Theorem 3, this would mean that the class of $[A_0] - [A]$ in $G(A)$ is its own inverse. But the inverse of $\deg([A_0] - [A]) = \ell$ in $\mathbb{Q}_+/\mathbb{Q}_+^4$ is ℓ^3 and not ℓ, so we must have $[A] \neq [\hat{A}]$ in $K_0(A)$.

On the other hand, Theorem 3 immediately yields the following positive result, giving a canonical class in degree two in $K_0(A)$:

Theorem 4 *If* $A_1, A_2 \in \mathrm{Ob}(\mathscr{C}_A)$ *are simple, then* $[A_1] + [\hat{A}_1] = [A_2] + [\hat{A}_2]$ *in* $K_0(A)$. *In other words, the class* $[A] + [\hat{A}]$ *is independent of the choice of* A *in its isogeny class.*

Theorem 2 and Corollary 1 can fail quite dramatically in characteristic p. The next two results show that $G(A)$ need not be infinite nor torsion in positive characteristic.

Theorem 5 *Suppose* $\mathrm{char}\ k = p > 0$ *and let* A *be a supersingular elliptic curve. Then* $G(A) = 0$. *In particular,* $K_0(A) \simeq \mathbb{Z}$.

Theorem 6 *Suppose* $\mathrm{char}\ k = p > 0$ *and let* A *be an elliptic curve with* $\mathrm{End}(A) = \mathbb{Z}$. *Then* $G(A)$ *contains an element of infinite order.*

For general A in characteristic p, determining the structure of $G(A)$ is somewhat subtle, and we hope to return to this question in future work. It would also be interesting to compute the groups $G(A)$ when k is a finite field. The answer should be related to Milne's computation [8] of the size of the Ext group of two abelian varieties over a finite field. When A is an elliptic curve over a finite field, one can presumably deduce the answer from the results of the recent paper [5].

The plan for the rest of the note is as follows. In Section 2, we produce certain relations in Grothendieck groups of abelian varieties. In Section 3, we prove Theorem 1. In Section 4, we define the map deg in Theorem 2. In Section 5, we prove that deg is an isomorphism in characteristic 0. In Section 6, we determine $G(E)$ for any elliptic curve E, in any characteristic.

2 Relations in the Grothendieck group

Recall k is an algebraically closed field and $\mathscr{A}$ is the category of abelian varieties over k. We will assume basic facts about commutative group schemes over algebraically closed fields, such as can be found in [10].

The first result is elementary:

Lemma 1 *Suppose A and B are abelian varieties, each containing an embedding of a finite group scheme G. Let C be the quotient of $A \times B$ by a diagonal copy of $G \subset A \times B$. Then there are exact sequences*

$$0 \to A \to C \to B/G \to 0,$$

$$0 \to B \to C \to A/G \to 0.$$

In particular, there is the relation

$$[A] - [A/G] = [B] - [B/G]$$

in $K_0(\mathscr{A})$.

Now fix an abelian variety A, not necessarily simple. Recall from the introduction the category $\mathscr{C}_A$ of abelian varieties isogenous to A^n for some n, and let $K_0(A)$ be the Grothendieck group $K_0(\mathscr{C}_A)$.

Lemma 2 *Suppose $\pi_1 : A \to A_1$ and $\pi_2 : A \to A_2$ are isogenies and suppose that* $\ker \pi_1 \cap \ker \pi_2 = 0$. *Then*

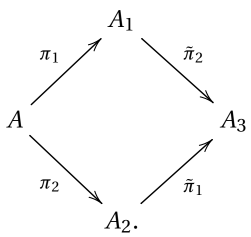
$$[A] = [A_1] + [A_2] - [A_3],$$

in $K_0(A)$, where A_3 is the quotient $A/(\ker \pi_1 + \ker \pi_2)$.

Proof Let $\tilde{\pi}_1 \colon A_2 \to A_3$ and $\tilde{\pi}_2 \colon A_1 \to A_3$ be the natural quotient maps, satisfying

$$\ker \tilde{\pi}_1 = \pi_1(\ker \pi_2) \qquad \text{and} \qquad \ker \tilde{\pi}_2 = \pi_2(\ker \pi_1).$$

We have the commutative diagram:



(1)

Since $\ker \pi_1 \cap \ker \pi_2 = 0$, we have $\ker \pi_2 \simeq \ker \tilde{\pi}_2$. Now apply Lemma 1 to A, $B = A_1$, and $G = \ker \pi_2$. This gives short exact sequences

$$0 \to A \to C \to A_3 \to 0$$

$$0 \to A_1 \to C \to A_2 \to 0,$$

with C in $\mathscr{C}_A$, so we conclude that $[A] + [A_3] = [A_1] + [A_2]$ in $K_0(A)$. $\square$

Theorem 7 *Let $\pi_1\colon A \to A'$ and $\pi_2\colon B \to B'$ be isogenies in $\mathscr{C}_A$. If $\ker \pi_1$ and $\ker \pi_2$ have the same Jordan-Hölder factors (with multiplicity), then $[A] - [A'] = [B] - [B']$ in $K_0(A)$.*

Proof We factor π_1 and π_2 into isogenies whose kernels are the Jordan-Hölder factors and then apply Lemma 1. □

Corollary 2 *If $\pi_1\colon A \to A_1$ and $\pi_2\colon A \to A_2$ are isogenies of degree n, and n is invertible in k, then $[A_1] = [A_2]$ in $K_0(A)$.*

Proof Since n is invertible in k, the Jordan-Hölder factors of $\ker \pi_1$ and $\ker \pi_2$ are of the form $\mathbb{Z}/\ell\mathbb{Z}$, for primes ℓ not equal to the characteristic of k. As $\ker \pi_1$ and $\ker \pi_2$ have the same rank, they must have the same Jordan-Hölder factors as well, and so $[A_1] = [A_2]$ by Theorem 7. □

3 The Grothendieck group $K_0(\mathscr{A})$

We compute the group $K_0(\mathscr{A})$, where $\mathscr{A}$ the category of abelian varieties over k.

Theorem 8 *There is an isomorphism $K_0(\mathscr{A}) \cong \bigoplus_A \mathbb{Z}[A]$, where the sum is over representatives A of simple isogeny classes of abelian varieties.*

Proof By Poincaré's complete reducibility theorem, it is enough to show that if $\phi\colon A \to A'$ is an isogeny of abelian varieties, then $[A] = [A']$ in $K_0(\mathscr{A})$. Set $p = \operatorname{char} k$. As k is algebraically closed, each Jordan-Hölder factor of $\ker \phi$ is of the form $\mathbb{Z}/\ell\mathbb{Z}$ for some prime ℓ, μ_p, or α_p (if $p \neq 0$) [10, §I.2]. We therefore reduce to the case where ϕ is an ℓ-isogeny for some prime ℓ (possibly equal to p).

By Lemma 1, it suffices to find, for every prime ℓ and for every group scheme G of order ℓ, an abelian variety A and an endomorphism $f \in \operatorname{End}(A)$ such that $\ker f \simeq G$. In fact, we will take A to be an elliptic curve E. If $\ell \neq p$, then $G \simeq \mathbb{Z}/\ell\mathbb{Z}$, and we may take E such that $\operatorname{End}(E)$ contains the quadratic ring $\mathbb{Z}[\sqrt{-\ell}]$. Such an E exists over any algebraically closed field k, by the theory of complex multiplication.

If $\ell = p$, then there are three group schemes G to consider, but for all three we will take E with j-invariant lying in $\mathbb{F}_p$. In this case, the Frobenius morphism

$$F\colon E \to E^{(p)} \simeq E$$

is an endomorphism. If E is supersingular, then $\ker F \simeq \alpha_p$, while if E is ordinary, then $\ker F \simeq \mu_p$ and $\ker \hat{F} \simeq \mathbb{Z}/p\mathbb{Z}$. So it is enough to show that there are both supersingular and ordinary j-invariants in $\mathbb{F}_p$, for all primes p.

The number of supersingular elliptic curves over $\mathbb{F}_p$ is related to a certain class number by a result of Deuring [2], and is always non-zero [1, Thm. 14.18]. On the other hand, the number of supersingular j-invariants over $\bar{\mathbb{F}}_p$ is less than $p/12+2$, and is equal to 1 for $p = 2$ [12, Thm. 4.1]. Since there are p total j-invariants in $\mathbb{F}_p$, it follows that there is at least one ordinary j-invariant in $\mathbb{F}_p$, for every p. □

Corollary 3 *Any additive function $\operatorname{Ob}(\mathscr{A}) \to G$ to an abelian group G is an isogeny invariant.*

Corollary 3 can be used to show that certain functions are *not* additive:

Example 2 If $k = \bar{\mathbb{Q}}$, then the stable Faltings height is additive under taking products of abelian varieties. If it were additive under short exact sequences, then it would be an isogeny invariant, by Corollary 3. But it is easy to see from Faltings' isogeny formula [3, Lem. 5] that the height sometimes changes under isogeny.

4 Simple isogeny classes

Now let $\tilde{A}$ be an isogeny class of simple abelian varieties of dimension g. Since k is algebraically closed, we may choose $A \in \tilde{A}$ admitting a principal polarization [9, Cor. p. 234], so that $A \simeq \hat{A}$. Our ultimate goal is to compute the Grothendieck group $K_0(A)$ of the category $\mathscr{C}_A$, in terms of the division algebra $D := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and the map $\deg : D^\times \to \mathbb{Q}_+$ extending the degree map $\mathrm{End}(A) \to \mathbb{Z}$.

Note that the group $K_0(A)$ depends only on $\tilde{A}$ and not A itself. The same is true for the division algebra D. For if $f\colon A' \to A$ is an isogeny, then there exists $g\colon A \to A'$ such that $g \circ f = [n]$ for some $n \in \mathbb{Z}$. The map $h \mapsto \frac{1}{n} f \circ h \circ g$ then gives a degree-preserving isomorphism $\mathrm{End}(A') \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D$ of $\mathbb{Q}$-algebras. Via this isomorphism, we may consider $\mathrm{End}(A')$ as a subring of D.

Lemma 3 *If $f : A_1 \to A_2$ is an isogeny in $\tilde{A}$ of degree n, such that n is invertible in k and $n = \deg(\beta)$ for some $\beta \in D^\times$, then $[A_1] = [A_2]$ in $K_0(A)$.*

Proof Write $\beta = ab^{-1}$ with $a, b \in \mathrm{End}(A_1) \cap \mathrm{End}(A_2)$, and with $\deg(a)$ invertible in k. Here we are thinking of $\mathrm{End}(A_1)$ and $\mathrm{End}(A_2)$ as embedded in D, as above. Then the composition

$$A_1 \xrightarrow{f} A_2 \xrightarrow{b} A_2$$

has the same degree as $a : A_1 \to A_1$. By Corollary 2, $[A_1] = [A_2]$. □

We write $\deg(D)$ for the submonoid $\deg(D^\times) \cap \mathbb{Z}$ of the monoid $\mathbb{Z}_+$ of positive integers under multiplication. Note that $\mathbb{Z}_+ \big/ \deg(D)$ is a group.

Remark 2 There may be elements of $\deg(D)$ which are not of the form $\deg(\alpha)$ for some $\alpha \in \mathrm{End}(A)$.

Lemma 4 *Suppose $f : A^n \to A^n$ is an isogeny. Then $\deg(f) \in \deg(D)$.*

Proof The isogeny f can be thought of as an element $M \in \mathrm{GL}_n(D)$. If D is commutative then one has the formula

$$\deg(f) = \deg(\det M).$$

In the general case, there is no well behaved determinant map $\mathrm{GL}_n(D) \to D^\times$. Instead, we have

$$\deg(f) = (\mathrm{Nm}_{F/\mathbb{Q}} \circ \mathrm{Nrd}_n(M))^{2g/de},$$

where F is the center of D, $d = [F:\mathbb{Q}]$, $e^2 = [D:F]$, and $\mathrm{Nrd}_n : \mathrm{GL}_n(D) \to F^\times$ is the reduced norm; see [9, §19]. On the other hand, for $g \in D$, we have

$$\deg(g) = (\mathrm{Nm}_{F/\mathbb{Q}} \circ \mathrm{Nrd}(g))^{2g/de},$$

where $\mathrm{Nrd} : D^\times \to F^\times$ is the reduced norm. The lemma then follows from Dieudonné's result [4, Cor. 2.8.10] that $\mathrm{Nrd}_n(\mathrm{GL}_n(D)) = \mathrm{Nrd}(D^\times)$. □

Lemma 5 *Let $B \in \mathscr{C}_A$ and let $f : A^n \to B$ be an isogeny. Then the class of* $\deg(f)$ *in* $\mathbb{Z}_+ / \deg(D)$ *is independent of the choice of f.*

Proof Let $\phi_L : B \to \hat{B}$ be a polarization on B. Then

$$\deg(\phi_{f^*L}) = \deg(\hat{f}\phi_L f) = \deg(f)^2 \deg(\phi_L).$$

The isogeny $\phi_{f^*L} : A^n \to \hat{A}^n \cong A^n$ has degree in $\deg(D)$ by Lemma 4. Hence

$$\deg(f)^2 \deg(\phi_L) = 1 \in \mathbb{Z}_+ / \deg(D). \qquad (2)$$

If $g : A^n \to B$ is another isogeny, then the composite map

$$h : A^n \xrightarrow{f} B \xrightarrow{\phi_L} \hat{B} \xrightarrow{\hat{g}} \hat{A}^n \xrightarrow{\psi} A^n$$

also has degree in $\deg(D)$. Here, ψ is any principal polarization. So modulo $\deg(D)$, we have

$$1 = \deg(f)\deg(\hat{g})\deg(\phi_L) = \deg(f)\deg(g)\deg(g)^{-2} = \deg(f)/\deg(g),$$

and therefore $\deg(f) = \deg(g)$ in $\mathbb{Z}_+ / \deg(D)$. □

Definition 1 If $B \in \mathscr{C}_A$, then the class of $\deg(f)$ in $\mathbb{Z}_+ / \deg(D)$, for any isogeny $f : A^n \to B$, is denoted $\mathrm{dist}_A(B)$ and is called the *distance* of B from A.

Lemma 6 *If $B \in \mathscr{C}_A$, then* $\mathrm{dist}_A(\hat{B}) = \mathrm{dist}_A(B)^{-1}$.

Proof From the sequence

$$A^n \longrightarrow B \xrightarrow{\phi_L} \hat{B},$$

we obtain $\mathrm{dist}_A(\hat{B}) = \mathrm{dist}_A(B)\deg(\phi_L)$, which is equal to $\mathrm{dist}_A(B)^{-1}$, by (2). □

Lemma 7 *Let $B \in \mathscr{C}_A$ and let $g : B \to A^n$ be an isogeny. Then the class of* $\deg(g)$ *in* $\mathbb{Z}_+ / \deg(D)$ *is independent of the choice of g and is equal to* $\mathrm{dist}_A(B)^{-1}$.

Proof We have $\deg(g) = \deg(\hat{g})$, with $\hat{g} : \hat{A}^n \to \hat{B}$ the dual isogeny. Since $\hat{A}^n \cong A^n$, the class of $\deg(g)$ in $\mathbb{Z}_+ / \deg(D)$ is independent of g and equal to $\mathrm{dist}_A(\hat{B})$. Now use the previous lemma. □

Definition 2 If $B \in \mathscr{C}_A$, then the class of $\deg(f)$ in $\mathbb{Z}_+ / \deg(D)$, for any isogeny $f : B \to A^n$, is denoted $\deg_A(B)$.

Remark 3 We have $\deg_A(B) = \mathrm{dist}_A(B)^{-1}$ in $\mathbb{Z}_+ / \deg(D)$. Context dictates which invariant is most convenient to use.

Remark 4 The map $\deg_A : \mathrm{Ob}(\mathscr{C}_A) \to \mathbb{Z}_+/\deg(D)$ depends on the choice of A. But note that if $f: B_1 \to B_2$ is an isogeny in $\mathscr{C}_A$, then

$$\frac{\deg_A(B_1)}{\deg_A(B_2)}$$

is equal to the class of $\deg(f) \in \mathbb{Z}_+/\deg(D)$ and hence is independent of the choice of A. In particular, we deduce:

Corollary 4 *If* $B \in \mathscr{C}_A$ *and* $\alpha \in \mathrm{End}(B)$ *is any isogeny, then* $\deg(\alpha) \in \deg(D)$.

5 Determination of $G(A)$ in characteristic 0

Now we connect the notion of degree with the Grothendieck group.

Proposition 1 *The function* $\deg_A : \mathrm{Ob}(\mathscr{C}_A) \to \mathbb{Z}_+/\deg(D)$ *is additive.*

Proof Let

$$0 \to B_1 \xrightarrow{j} B \xrightarrow{\pi} B_2 \to 0$$

be an exact sequence in $\mathscr{C}_A$. Let $\phi_M : \hat{B}_1 \to B_1$ and $\phi_L : B \to \hat{B}$ be polarizations and define $h : B \to B_1 \times B_2$ to be the map $\phi_M \hat{j} \phi_L \times \pi$. From the sequence of isogenies

$$B \xrightarrow{h} B_1 \times B_2 \longrightarrow A^{n_1} \times A^{n_2} \cong A^n,$$

we conclude

$$\deg_A(B) = \deg_A(B_1)\deg_A(B_2)\deg(h) \in \mathbb{Z}_+/\deg(D).$$

So it suffices to show that $\deg(h)$ is in $\deg(D)$. For this, note that $\ker h$ is isomorphic to the kernel of the isogeny $\phi_M \hat{j} \phi_L j \in \mathrm{End}(B_1)$. Then by Corollary 4, $\deg(h) \in \deg(D)$. □

We therefore have a homomorphism $\deg_A : K_0(A) \to \mathbb{Z}_+/\deg(D)$. By Remark 4, the restriction of $\deg_A$ to the dimension 0 subgroup $G(A) \subset K_0(A)$ is independent of A, so we write

$$\deg : G(A) \to \mathbb{Z}_+/\deg(D).$$

This homomorphism is surjective, since for every positive integer n, we can find an isogeny $A_1 \to A_2$ in $\tilde{A}$ of degree n, so that the class $[A_1] - [A_2] \in G(A)$ has degree n. In fact, in characteristic 0, the degree homomorphism is injective as well:

Theorem 9 *Suppose* $\mathrm{char}\, k = 0$. *Then the degree map* $\deg : G(A) \to \mathbb{Z}_+/\deg(D)$ *is an isomorphism.*

Proof We write A_n for any $A_n \in \tilde{A}$ such that $\mathrm{dist}_A(A_n) = n$. The class $[A_n] \in K_0(A)$ is independent of the choice of A_n by Corollary 2. For any $m, n \in \mathbb{Z}_+$, we have

$$[A_{nm}] - [A_n] = [A_m] - [A]. \tag{3}$$

This follows from Theorem 7, since in characteristic 0 the Jordan-Hölder factors of a finite group scheme are determined by its rank.

Note that $K_0(A)$ is generated by classes $[A']$ of *simple* $A' \in \mathrm{Ob}(\mathscr{C}_A)$. Thus, any $\beta \in G(A)$, can be written as

$$\beta = \sum_{i=1}^{r} \left([A_{n_i}] - [A_{m_i}]\right) = [A_{\prod_i^r n_i}] + (r-1)[A] - [A_{\prod_i^r m_i}] - (r-1)[A] = [A'] - [A''],$$

for certain $A', A'' \in \tilde{A}$. If β is also in the kernel of the degree map $G(A) \to \mathbb{Z}_+ \big/ \deg(D)$, then

$$\deg_A(A') / \deg_A(A'') \in \deg(D).$$

Equivalently, there is an isogeny $f : A' \to A''$ of degree $\deg(\alpha)$ for some $\alpha \in D$. By Lemma 3, $[A'] = [A'']$ and hence $\beta = 0$. This shows that $G(A) \to \mathbb{Z}_+ \big/ \deg(D)$ is injective, and hence an isomorphism. □

As a corollary, we obtain Theorem 3:

Corollary 5 *The additive function $B \mapsto \hat{B}$ induces the inversion homomorphism on $G(A)$.*

Proof Since $\deg_A(\hat{B}) = \deg_A(B)^{-1}$, by Lemma 6 and Remark 3. □

The following proposition gives a concrete description of $\mathbb{Z}_+ \big/ \deg(D)$.

Proposition 2 *Let A be a simple abelian variety of dimension g and $D = \mathrm{End}(A) \otimes \mathbb{Q}$ its endomorphism algebra, with center $Z(D) = F$. Write $e = [F : \mathbb{Q}]$ and $d^2 = [D : F]$. Then*

$$\mathbb{Z}_+ \big/ \deg(D) \simeq \mathbb{Q}_+ \big/ \mathrm{Nm}_{F/\mathbb{Q}}(F^+)^{2g/de},$$

where F^+ is the set of non-zero elements of F which are positive at all the ramified real places of D.

Proof We have seen already that $\deg : D^\times \to \mathbb{Q}_+$ is given by the map $(\mathrm{Nm}_{F/\mathbb{Q}} \circ \mathrm{Nrd})^{2g/de}$. But the Hasse-Schilling-Maass theorem [11, Thm 33.15] states that the reduced norm on D surjects onto F^+. □

Theorem 2 now follows from Theorem 9 and Proposition 2.

6 The case dim $A = 1$

In this section we determine $G(E)$, for any elliptic curve E over any algebraically closed field k, of any characteristic. The characteristic 0 cases can be read off from Theorem 2:

Theorem 10 *Suppose k has characteristic 0 and E/k is an elliptic curve with endomorphism algebra D. Then the degree map induces an isomorphism*

$$G(E) \simeq \begin{cases} \mathbb{Q}_+/\mathbb{Q}_+^2 & \text{if } D = \mathbb{Q}, \\ \mathbb{Q}_+/\mathrm{Nm}_{K/\mathbb{Q}}(K^\times) & \text{if } D = K \text{ is imaginary quadratic.} \end{cases}$$

In the case $D = \mathbb{Q}$, we have the concrete description $\mathbb{Q}_+/\mathbb{Q}_+^2 \cong \bigoplus_\ell \mathbb{Z}/2\mathbb{Z}$, where the sum is over all primes ℓ. We can make the group structure of $G(E)$ more explicit in the CM case $D = K$ as well:

Proposition 3 *If K is imaginary quadratic over $\mathbb{Q}$, then*

$$\mathbb{Q}_+/\mathrm{Nm}_{K/\mathbb{Q}}(K^\times) \simeq C/C^2 \oplus \bigoplus_{\ell \text{ inert}} \mathbb{Z}/2\mathbb{Z},$$

where $C = \mathrm{Pic}(\mathscr{O}_K)$ is the class group of K and the sum is over primes ℓ which are inert in K.

Proof If $\ell = \mathrm{Nm}(\alpha)$ for some $\alpha \in K^\times$, then ℓ is not inert in K and $(\alpha) = \mathfrak{l}\mathfrak{a}\bar{\mathfrak{a}}^{-1}$ for some ideal $\mathfrak{a}$ of $\mathscr{O}_K$ and some prime $\mathfrak{l}$ above ℓ. It follows that $[\mathfrak{l}]$ is a square in C. We therefore get a well defined map

$$\mathbb{Q}_+/\mathrm{Nm}_{K/\mathbb{Q}}(K^\times) \longrightarrow C/C^2 \oplus \bigoplus_{\ell \text{ inert}} \mathbb{Z}/2$$

by sending an inert prime ℓ to the generator of $\mathbb{Z}/2\mathbb{Z}$ in the ℓth slot, and sending a non-inert prime ℓ to the class of $[\mathfrak{l}]$ in C/C^2, where $\mathfrak{l}$ is any prime above ℓ. This map is clearly surjective, and to prove injectivity, we need to show that if $[\mathfrak{l}]$ is a square in C, then ℓ is a norm. If $[\mathfrak{l}]$ is a square, then $\mathfrak{l} = (\alpha)\mathfrak{a}^2 = (\beta)\mathfrak{a}\bar{\mathfrak{a}}^{-1}$ for some ideal $\mathfrak{a}$, so we see that $\mathrm{Nm}(\beta) = \ell$. □

Now suppose k has characteristic $p > 0$. There are three cases to consider, depending on the dimension of $D = \mathrm{End}(E) \otimes \mathbb{Q}$ over $\mathbb{Q}$.

Theorem 11 *If E is supersingular, then $G(E) = 0$.*

Proof The isogeny class of E is the set of supersingular elliptic curves over k. It is therefore enough to show that $[E'] = [E]$ in $K_0(E)$ for all, supersingular elliptic curves E'. By [7, Cor. 77], we may choose a prime number $\ell \neq p$ such that there exist ℓ-isogenies $E \to E$ and $E \to E'$. Then $[E'] = [E]$ in $K_0(E)$ by Corollary 2. □

Theorem 12 *If D is isomorphic to an imaginary quadratic field K, then the degree map induces an isomorphism $G(E) \simeq \mathbb{Q}_+/\mathrm{Nm}_{K/\mathbb{Q}}(K^\times)$.*

Proof Let E' be an elliptic curve isogenous to E. By a result of Deuring [2, p. 263], the rings $\mathrm{End}(E)$ and $\mathrm{End}(E')$ have index prime to p in $\mathscr{O}_K$ and p is split in $\mathscr{O}_K$. Thus, by [6, Prop. 40], the rank two quadratic form $\deg\colon \mathrm{Hom}(E,E') \to \mathbb{Z}$, has discriminant prime to p. It follows that there is an isogeny $E \to E'$ of degree prime to p. We may then write $[E'] = [E_n]$ for some $n \in \mathbb{Z}$ prime to p, and where E_n is the class of any elliptic curve isogenous to E with $\mathrm{dist}_E(E') = n$ (this is well-defined by Corollary 2).

As in the proof of Theorem 9, we conclude that any $\beta \in G(E)$ has the form $[E_n] - [E_m]$ with n and m prime to p. If β is also in the kernel of the degree map, then $\deg(\beta)$ is the class of n/m and lies in $\deg(D)$. By Lemma 3, we have $[E_n] = [E_m]$ and $\beta = 0$. Thus, the degree map is injective and hence an isomorphism onto $\mathbb{Q}_+/\mathrm{Nm}_{K/\mathbb{Q}}(K^\times)$. □

Theorem 13 *If $D = \mathbb{Q}$, then $G(E)$ is isomorphic to a subgroup of index 2 in $\mathbb{Z} \bigoplus \mathbb{Q}_+/\mathbb{Q}_+^2$. In particular, $G(E)$ is not a torsion group.*

Proof We define an additive map $\deg_{p,E}\colon \mathrm{Ob}(\mathscr{C}_E) \to \mathbb{Z}$ as follows. For any isogeny $f\colon B \to B'$ in $\mathscr{C}_E$, let $e(f)$ denote the number of Jordan-Hölder factors of $\ker f$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$, let $c(f)$ denote the number of factors isomorphic to μ_p, and let $\deg_p(f) = e(f) - c(f)$. For $B \in \mathrm{Ob}(\mathscr{C}_E)$, we define $\deg_{p,E}(B) = \deg_p(f)$, where f is any isogeny $f\colon B \to E^n$. To check that this is well-defined we use:

Lemma 8 *If $f\colon E^n \to E^n$ is an isogeny, then* $\deg_p(f) = 0$.

Proof The case $n = 1$ is clear since then $f \in \mathbb{Z}$ and $E[p] \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. For $n > 1$, we may think of f as a matrix $M \in \mathrm{Mat}_n(\mathbb{Z})$. We may assume M is in Smith normal form, at the cost of choosing a new product decomposition for E^n. Then $\ker f$ is the direct sum of kernels of endomorphisms of E and the lemma follows from the case $n = 1$. □

Now suppose $f'\colon B \to E^n$ is another isogeny. If we let $g'\colon E^n \to B$ be such that $f'g' = [\deg f']_{E^n}$, then $\deg_p(f') + \deg_p(g') = 0$ and

$$\deg_p(f) - \deg_p(f') = \deg_p(f) + \deg_p(g') = \deg_p(fg') = 0,$$

by the lemma. So $\deg_{p,E}(B)$ is well-defined. We also conclude that $\deg_p(f) = 0$ for any $f \in \mathrm{End}(B)$, just as in Corollary 4.

One now checks that $\deg_{p,E}$ is additive, exactly as in Proposition 1. We therefore get an induced map $K_0(E) \to \mathbb{Z}$ which depends on E. But the restriction to $G(E)$ gives a canonical map $\deg_p\colon G(E) \to \mathbb{Z}$ sending $[E'] - [E'']$ to $\deg_p(f)$, where $f\colon E' \to E''$ is any isogeny.

For any isogeny f, we write $\deg_\ell(f)$ for the prime-to-p part of $\deg(f)$. Now consider the composite map

$$\mathrm{tot}\colon G(E) \overset{(\deg_p,\deg)}{\longrightarrow} \mathbb{Z} \oplus \mathbb{Q}_+/\mathbb{Q}_+^2 \longrightarrow \mathbb{Z} \oplus H_p$$

where $H_p \simeq \bigoplus_{\ell \neq p} \mathbb{Z}/2\mathbb{Z}$ is the prime-to-p part of $\mathbb{Q}_+/\mathbb{Q}_+^2$, and the map $\mathbb{Q}_+/\mathbb{Q}_+^2 \to H_p$ is the canonical surjection. Then

$$\mathrm{tot}([E_1] - [E_2]) = (\deg_p(f), \deg_\ell(f))$$

for any isogeny $f\colon E_1 \to E_2$. It follows that tot is surjective, and we will show that it is injective as well.

For every $(a,n) \in \mathbb{Z} \oplus \mathbb{Z}_+$ with n prime to p, we let $E_{a,n}$ be any elliptic curve admitting an isogeny $f\colon E \to E_{a,n}$ such that $\deg_p(f) = a$ and $\deg_\ell(f) = n$. Then the class of $[E_{a,n}]$ in $K_0(E)$ is independent of the choice of $E_{a,n}$. Indeed, the isogeny $f\colon E \to E_{a,n}$ can be factored as

$$E \longrightarrow E_a \xrightarrow{g} E_{a,n},$$

where g is an n-isogeny, and E_a is the unique étale (resp. connected) quotient of E of degree p^a if $a \geq 0$ (resp. $a \leq 0$). Thus the class of $[E_{a,n}]$ is uniquely determined by Corollary 2.

Using Lemma 2, we obtain the following relations in $K_0(E)$, for any integers a and b, and any positive integers n and m coprime to p:

$$\begin{aligned}[E_{a,n}] &= [E_{a,1}] + [E_{0,n}] - [E] \\ [E_{a+b,1}] &= [E_{a,1}] + [E_{b,1}] - [E] \\ [E_{0,nm}] &= [E_{0,n}] + [E_{0,m}] - [E].\end{aligned}$$

It follows that any $\beta \in G(E)$ can be written as

$$\beta = [E_{a,1}] - [E_{b,1}] + [E_{0,n}] - [E_{0,m}]$$

for integers a and b, and positive integers n and m. If $\mathrm{tot}(\beta) = 0$, then we must have $a = b$ and $n = md^2$ for some rational number d. By Lemma 3, we must have $[E_{0,n}] = [E_{0,m}]$, and so $\beta = 0$. Thus, tot is an injection, and hence an isomorphism. Since $\mathbb{Z} \oplus H_p$ embeds in $\mathbb{Z} \oplus \mathbb{Q}_+/\mathbb{Q}_+^2$ with index 2, Theorem 13 is proved. □

Remark 5 An example of a non-torsion class in $G(E)$ is $[E] - [E^{(p)}]$, where $E^{(p)}$ is the Frobenius-transform of E, i.e. the elliptic curve with j-invariant $j(E)^p$.

Acknowledgements The author thanks Julian Rosen for suggesting the proof of Theorem 1 and for other conversations on this topic. He also thanks Taylor Dupuy, Yuri Zarhin, and the anonymous referee for their helpful feedback.

References

1. D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley, 1989.
2. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14** (1941), 197-272.
3. G. Faltings, Endlichkeitssäatze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349-366.
4. P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, **101**, Cambridge University Press, Cambridge, 2006.
5. B. Jordan, A. Keeton, B. Poonen, E. Rains, N. Shepherd-Barron, and J. Tate, Abelian varieties isogenous to a power of an elliptic curve, preprint, arXiv:1602.06237 (2016).
6. E. Kani, Products of CM Elliptic Curves, *Collectanea Math.* **62** (2011) 297-339.
7. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California at Berkeley, 1996.
8. J. S. Milne, Extensions of abelian varieties defined over a finite field. *Invent. Math.* **5** (1968), 63-84.

9. D. Mumford, *Abelian Varieties*, Oxford Univ. Press, 1970.
10. F. Oort, *Commutative group schemes*, Lecture Notes in Mathematics **15**, Springer-Verlag, Berlin-New York, 1966.
11. I. Reiner, *Maximal Orders*, London Math. Soc. Monographs **5**, Academic Press, London, 1975.
12. J. Silverman, *The Arithmetic of Elliptic Curves*, Second edition. Graduate Texts in Math. **106**. Springer, Dordrecht, 2009.