Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Isabel VOGT

Abelian varieties isogenous to a power of an elliptic curve over a Galois extension

Tome 31, n° 1 (2019), p. 205-213.

<http://jtnb.cedram.org/item?id=JTNB_2019__31_1_205_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 205–213

Abelian varieties isogenous to a power of an elliptic curve over a Galois extension

par Isabel VOGT

Résumé. Soient E/k une courbe elliptique et k'/k une extension de Galois. On construit un foncteur exact de la catégorie des modules sans torsion sur l'anneau des endomorphismes $\operatorname{End} E_{k'}$ munis d'une action semi-linéaire de $\operatorname{Gal}(k'/k)$ vers la catégorie des variétés algébriques sur k qui sont k'-isogènes à une puissance de E. Comme application, on donne une preuve simple du fait que toute courbe elliptique sur k qui est géométriquement à multiplication complexe, est isogène sur k à une courbe elliptique à multiplication complexe par un ordre maximal.

Abstract. Given an elliptic curve E/k and a Galois extension k'/k, we construct an exact functor from torsion-free modules over the endomorphism ring $\operatorname{End} E_{k'}$ with a semilinear $\operatorname{Gal}(k'/k)$ action to abelian varieties over k that are k'-isogenous to a power of E. As an application, we give a simple proof that every elliptic curve with complex multiplication geometrically is isogenous over the ground field to one with complex multiplication by a maximal order.

1. Introduction

Let E be an elliptic curve over a field k. As in [4], the theory of abelian varieties isogenous over k to a power of E is related to the theory of finitely presented torsion-free modules over the endomorphism ring $R_k := \operatorname{End}_k E$. To recall briefly, there is a functor

$$\mathscr{H}om_{R_k}(\,\cdot\,, E)\colon \begin{Bmatrix}\text{finitely presented}\\ \text{left } R_k\text{-modules}\end{Bmatrix}^{\text{opp}} \to \begin{Bmatrix}\text{commutative proper}\\ k\text{-group schemes}\end{Bmatrix},$$

such that for M a finitely presented R_k-module and C a k-scheme, we have

$$\operatorname{Hom}_k(C, \mathscr{H}om_{R_k}(M, E)) = \operatorname{Hom}_{R_k}(M, \operatorname{Hom}_k(C, E)).$$

Restricting to torsion-free modules, we obtain a functor

$$\mathscr{H}om_{R_k}(\,\cdot\,, E)\colon \begin{Bmatrix}\text{fin. pres. tors. free}\\ \text{left } R_k\text{-modules}\end{Bmatrix}^{\text{opp}} \to \begin{Bmatrix}\text{abelian } k\text{-varieties}\\ \text{isogenous to } E^r,\ r \in \mathbb{Z}\end{Bmatrix}.$$

Manuscrit reçu le 29 avril 2018, accepté le 19 octobre 2018.
2010 *Mathematics Subject Classification.* 14K02, 11G10.
Mots-clefs. abelian varieties, complex multiplication, isogenies.
This research was partially supported by the National Science Foundation Graduate Research Fellowship Program under Grant DMS-1122374 as well as Grant DMS-1601946.

This functor is fully faithful, but not in general an equivalence of categories. For example, if $\operatorname{chat} k = 0$ and E does not have complex multiplication, then the image of this functor consists entirely of the powers of E; yet it is possible for E to be k-isogenous to a non-isomorphic curve.

In fact, this functor is never surjective if E/k acquires complex multiplication (CM) over a separable quadratic extension k'/k: E is always k-isogenous to its k'/k quadratic twist E'/k, as we now show. Suppose that $E_{k'}$ has CM by the order $\mathcal{O}$. Let $\alpha \in \mathcal{O}$ be a purely imaginary element of $\mathcal{O}$, so that the nontrivial element $\sigma \in \operatorname{Gal}(k'/k)$ acts as ${}^{\sigma}\alpha = -\alpha$. Multiplication by α composed with the isomorphism $E_{k'} \xrightarrow{\simeq} E'_{k'}$ is Galois stable, and so descends to an isogeny $E \to E'$ over k.

In this note we describe a generalization of the functor $\mathscr{H}om_{R_k}(\,\cdot\,, E)$, which in particular addresses the case when $\operatorname{End}_k E \neq \operatorname{End}_{\bar{k}} E$. We will show that the essential image of this functor always contains all of the quadratic twists of E.

More generally, one may also consider abelian varieties, as in the case of nontrivial twists, that are isogenous to a power of an elliptic curve only after passing to a Galois extension of the ground field. When restricted to torsion-free modules, the image of the functor we construct will lie in the category of abelian varieties that become isogenous to a power of E over a Galois extension. This functor may therefore shed light upon abelian varieties that are not isogenous to a power of E over the ground field, and therefore missed by the previous functor, but become isogenous to a power of E after making a suitable extension.

Let k'/k be a finite Galois extension and let $G := \operatorname{Gal}(k'/k)$. As every proper commutative group scheme over a field is projective, the category of commutative proper k-group schemes is equivalent to the category of commutative proper k'-group schemes equipped with descent data for k'/k. For this reason we may identify commutative proper k-group schemes with commutative proper k'-group schemes with an action of G, such that all maps, including the structure maps, are G-equivariant.

Let $R = R_{k'} := \operatorname{End} E_{k'}$ be the endomorphism ring of the base change $E_{k'}$ of E to k'. In particular, R is noetherian. This inherits an action of G. We denote this action by $r \mapsto {}^{\sigma}r$ for $\sigma \in G$ and $r \in R$. We may then form the twisted group ring $R\langle G\rangle$ as the free R-module

$$R\langle G\rangle = \bigoplus_{\sigma \in G} R \cdot \sigma$$

with the commutation relation $\sigma r = {}^{\sigma}r\sigma$. In this way, a module over $R\langle G\rangle$ is an R-module with a semilinear G-action.

We give a construction of the following in Section 2.

Theorem 1.1. *There exists an exact functor*

$$\mathscr{H}\!om_{R\langle G\rangle}(\,\cdot\,, E_{k'})\colon \left\{\begin{matrix}\textit{fin. pres. left}\\ R\langle G\rangle\textit{-modules}\end{matrix}\right\}^{\mathrm{opp}} \to \left\{\begin{matrix}\textit{commutative proper}\\ k\textit{-group schemes}\end{matrix}\right\},$$

such that

1. *For a finitely presented $R\langle G\rangle$-module M and any k-scheme C, we have*

$$\operatorname{Hom}_k(C, \mathscr{H}\!om_{R\langle G\rangle}(M, E_{k'})) = \operatorname{Hom}_{R\langle G\rangle}(M, \operatorname{Hom}_{k'}(C_{k'}, E_{k'})).$$

2. *The functor agrees with $\mathscr{H}\!om_R(\,\cdot\,, E_{k'})$ under the forgetful functors mapping $R\langle G\rangle$-modules to R-modules and base-changing k-schemes to k'-schemes.*

In particular, this shows that if M is an $R\langle G\rangle$-module that is torsion-free as an R-module, then $\mathscr{H}\!om_{R\langle G\rangle}(M, E_{k'})$ is an abelian variety A over k, such that $A_{k'}$ is isogenous to a power of E. However, we may say something about the k-isogeny class of A as well. Recall that the category of abelian varieties over k up to isogeny has the same objects as the category of abelian varieties over k, but all isogenies are inverted.

Let $F = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Since F is semisimple, the category of finitely presented modules over the twisted group algebra $F\langle G\rangle$ is semisimple (as in the case when the action of G on F is trivial, see Lemma 2.3 below). Let $S_1, \dots, S_\ell$ denote the simple objects.

Theorem 1.2. *There is a functor*

$$\mathscr{H}\!om_{F\langle G\rangle}(\,\cdot\,, E_{k'})\colon \left\{\begin{matrix}\textit{fin. pres.}\\ F\langle G\rangle\textit{-modules}\end{matrix}\right\}^{\mathrm{opp}} \to \left\{\begin{matrix}\textit{abelian varieties over } k\\ \textit{up to isogeny}\end{matrix}\right\},$$

compatible with the functor $\mathscr{H}\!om_{R\langle G\rangle}(\,\cdot\,, E_{k'})$. For any torsion-free finitely presented $R\langle G\rangle$-module M, $\mathscr{H}\!om_{R\langle G\rangle}(M, E_{k'})$ is isogenous over k to a product of powers of the abelian varieties $\mathscr{H}\!om_{F\langle G\rangle}(S_i, E_{k'})$.

As an application of this Galois-equivariant functor, we give a simple and new proof of the following old result (see [3, Prop. 25], [2, Prop. 2.2], [6, Prop. 5.3], [5, Prop. 2.3b] for other proofs of the same or similar results), which is useful in reducing questions about arbitrary CM elliptic curves to those with complex multiplication by a maximal order; this will be used in [7] for this very reason.

Corollary 1.3. *Let k be a number field and let E/k be an elliptic curve. Suppose that $E_{\bar{k}}$ has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field F. Then there exists an elliptic curve E'/k and an isogeny*

$$\varphi\colon E' \to E$$

defined over k, such that $E'_{\bar{k}}$ has complex multiplication by the full ring of integers of F.

Acknowledgments. I would like to thank Bjorn Poonen for suggesting that the initial functor could be useful in addressing the problem in Corollary 1.3 and for helpful discussions. I also thank Pavel Etingof for answering some questions, and Pete Clark for explaining the history of the result in Corollary 1.3 and providing references.

2. Categorical Constructions

For any $R\langle G\rangle$-module M, let $\mathscr{H}om_{R\langle G\rangle}(M, E_{k'})$ be the functor from the category of k-schemes to the category of sets sending a k-scheme C to

$$\mathrm{Hom}_{R\langle G\rangle}(M, \mathrm{Hom}_{k'}(C_{k'}, E_{k'})).$$

Let

$\mathrm{Res}_{k'/k}\colon \{\text{comm. proper } k'\text{-group schemes}\} \to \{\text{comm. proper } k\text{-group sch}\}$

denote Weil restriction of scalars.

Proposition 2.1. *The functor $\mathscr{H}om_{R\langle G\rangle}(M, E_{k'})$ is representable by a commutative proper k-group scheme. When $M = R\langle G\rangle$, the representing scheme is $\mathrm{Res}_{k'/k} E_{k'}$.*

Proof. We first show that $\mathscr{H}om_{R\langle G\rangle}(R\langle G\rangle, E_{k'}) = \mathrm{Res}_{k'/k} E_{k'}$. Indeed, by the universal property of the restriction of scalars we have

$$\begin{aligned}
&\mathrm{Hom}_k(C, \mathrm{Res}_{k'/k} E_{k'})\\
&\qquad = \mathrm{Hom}_{k'}(C_{k'}, E_{k'}) = \mathrm{Hom}_{R\langle G\rangle}(R\langle G\rangle, \mathrm{Hom}_{k'}(C_{k'}, E_{k'}))\\
&\qquad = \mathrm{Hom}_k(C, \mathscr{H}om_{R\langle G\rangle}(R\langle G\rangle, E_{k'}))
\end{aligned}$$

as desired. Note that the k-scheme $\mathrm{Res}_{k'/k} E_{k'}$ has endomorphisms by $R\langle G\rangle$.

Now let

$$R\langle G\rangle^m \to R\langle G\rangle^n \to M \to 0 \tag{2.1}$$

be a finite presentation of M as $R\langle G\rangle$-modules. The map $R\langle G\rangle^m \to R\langle G\rangle^n$ is given by multiplication on the right by a $m \times n$ matrix X. Multiplication by X on the left also defines a map

$$(\mathrm{Res}_{k'/k} E_{k'})^n \to (\mathrm{Res}_{k'/k} E_{k'})^m.$$

As commutative proper group schemes over k form an abelian category, the above morphism has a kernel in this category,

$$0 \to A \to (\mathrm{Res}_{k'/k} E_{k'})^n \to (\mathrm{Res}_{k'/k} E_{k'})^m. \tag{2.2}$$

We claim that A represents the functor $\mathscr{H}om_{R\langle G\rangle}(M, E_{k'})$ defined above. Indeed, we may apply the left-exact functor $\mathrm{Hom}_k(C, -)$ to (2.2) to obtain

$$0 \to \mathrm{Hom}_k(C, A) \to \mathrm{Hom}_{k'}(C_{k'}, E_{k'})^n \to \mathrm{Hom}_{k'}(C_{k'}, E_{k'})^m. \tag{2.3}$$

Similarly apply the left-exact functor $\mathrm{Hom}_{R\langle G\rangle}(\,\cdot\,,\mathrm{Hom}_{k'}(C_{k'},E_{k'}))$ to (2.1) to obtain

$$(2.4)\quad 0\to \mathrm{Hom}_{R\langle G\rangle}(M,\mathrm{Hom}_{k'}(C_{k'},E_{k'}))\to \mathrm{Hom}_{k'}(C_{k'},E_{k'})^n \\ \to \mathrm{Hom}_{k'}(C_{k'},E_{k'})^m.$$

As the right maps in both (2.3) and (2.4) are induced by multiplication by X, the kernels are functorially isomorphic, as desired. □

Recall that we let $F := R\otimes\mathbb{Q}$. We now show that we have a compatible functor taking values in the category of abelian varieties over k up to isogeny, as in Theorem 1.2. For objects B_1 and B_2 in the isogeny category, denote by $\mathrm{Hom}_{\mathrm{isog}}(B_1,B_2)$ the morphisms in the isogeny category.

For a finitely presented $F\langle G\rangle$-module N, define the functor

$$\mathscr{H}om_{F\langle G\rangle}(N,E_{k'})$$

from the isogeny category of abelian varieties over k to sets by

$$B\mapsto \mathrm{Hom}_{F\langle G\rangle}(N,\mathrm{Hom}_{\mathrm{isog}}(B_{k'},E_{k'})).$$

Proposition 2.2. *The functor $\mathscr{H}om_{F\langle G\rangle}(N,E_{k'})$ defined above is represented by an abelian variety in the isogeny category over k.*

Proof. As above, let B be an object of the isogeny category of abelian varieties over k. If $N = M\otimes_{R\langle G\rangle}F\langle G\rangle$, we have

$$\begin{aligned}\mathrm{Hom}_{F\langle G\rangle}&(N,\mathrm{Hom}_{\mathrm{isog}}(B_{k'},E_{k'}))\\ &= \mathrm{Hom}_{F\langle G\rangle}(M\otimes F\langle G\rangle,\mathrm{Hom}_{k'}(B_{k'},E_{k'})\otimes\mathbb{Q}),\\ &= \mathrm{Hom}_{R\langle G\rangle}(M,{}_{R\langle G\rangle}\,\mathrm{Hom}_{k'}(B_{k'},E_{k'})\otimes\mathbb{Q}),\\ &= \mathrm{Hom}_{R\langle G\rangle}(M,\mathrm{Hom}_{k'}(B_{k'},E_{k'}))\otimes\mathbb{Q}.\end{aligned}$$

And so this functor agrees with the original $\mathscr{H}om_{R\langle G\rangle}(\,\cdot\,,E_{k'})$ after composing with the localization map to the isogeny category.

Therefore the functor $\mathscr{H}om_{F\langle G\rangle}(F\langle G\rangle,E_{k'})$ is represented by $\mathrm{Res}_{k'/k}(E_{k'})$ in the isogeny category. Furthermore, as the isogeny category is an abelian category, the same proof as in Lemma 2.1 shows that for all finitely presented $F\langle G\rangle$-modules N, the functor $\mathscr{H}om_{F\langle G\rangle}(N,E_{k'})$ is represented by an object in the isogeny category. □

Lemma 2.3. *Let F be a semisimple $\mathbb{Q}$-algebra. Then $F\langle G\rangle$ is semisimple.*

Proof. Let $V\to W$ be a surjection of finite-dimensional left $F\langle G\rangle$-modules. As F is semisimple, we may choose a splitting $\varphi\colon W\to V$ as F-modules. The map $\pi\colon W\to V$ given by

$$\pi(w)=\sum_{g\in G} g\varphi(g^{-1}w),$$

defines a splitting as $F\langle G\rangle$-modules. □

Since the endomorphism algebra of an elliptic curve is always semisimple, Lemma 2.3 combined with the above construction proves Theorem 1.2.

We now show compatibility with base change and restriction of scalars.

Lemma 2.4. *Let M be a finitely presented left R-module and set $A := \mathscr{H}om_R(M, E_{k'})$. Then we have that*

$$\operatorname{Res}_{k'/k} A \simeq \mathscr{H}om_{R\langle G\rangle}(R\langle G\rangle \otimes_R M, E_{k'}).$$

Proof. By Yoneda's Lemma, it suffices to show that $\operatorname{Res}_{k'/k} A$ and

$$\mathscr{H}om_{R\langle G\rangle}(R\langle G\rangle \otimes_R M, E_{k'}$$

have the same functors of points. Let C be a k-scheme. By the universal property of restriction of scalars, we have

$$\operatorname{Res}_{k'/k} A(C) = A(C_{k'}) = \operatorname{Hom}_R(M, \operatorname{Hom}(C_{k'}, E_{k'})).$$

By the adjunction between restriction and induction [1, Prop. 2.8.3 (i)], we have

$$\operatorname{Hom}_R(M, \operatorname{Hom}(C_{k'}, E_{k'})) \simeq \operatorname{Hom}_{R\langle G\rangle}(R\langle G\rangle \otimes M, \operatorname{Hom}(C_{k'}, E_{k'})),$$

which completes the proof. □

For any ring R and any left R-algebra S, let $\underline{S}$ denote the (R, S)-bimodule S under multiplication by R on the left and S on the right.

Lemma 2.5. *Let M be a finitely presented left $R\langle G\rangle$-module and let $A := \mathscr{H}om_{R\langle G\rangle}(M, E_{k'})$. Then the base change $A_{k'}$ is isomorphic to*

$$\mathscr{H}om_R({}_RM, E_{k'}),$$

where ${}_RM$ denotes the underlying R-module of M.

Proof. By Yoneda's Lemma, it suffices to show that $A_{k'}$ and $\mathscr{H}om_R({}_RM, E_{k'})$ have the same functor of points. Let D be a k'-scheme. Let ${}_kD$ denote the k-scheme whose structure morphism is the composition $D \to \operatorname{Spec} k' \to \operatorname{Spec} k$. By the universal property of fiber products,

$$A_{k'}(D) = A({}_kD) = \operatorname{Hom}_{R\langle G\rangle}\left(M, E_{k'}(({}_kD)_{k'})\right).$$

We are thus reduced to showing that

$$\operatorname{Hom}_{R\langle G\rangle}\left(M, E_{k'}(({}_kD)_{k'})\right) = \operatorname{Hom}_R({}_RM, E_{k'}(D)).$$

Furthermore, by the adjunction between restriction and coinduction [1, Prop. 2.8.3 (ii)],

$$\operatorname{Hom}_R({}_RM, E_{k'}(D)) = \operatorname{Hom}_{R\langle G\rangle}(M, \operatorname{Hom}_R(\underline{R\langle G\rangle}, E_{k'}(D))).$$

It suffices then to show that, as left $R\langle G\rangle$-modules,

$$E_{k'}(({}_kD)_{k'}) \simeq \operatorname{Hom}_R(R\langle G\rangle, E_{k'}(D)).$$

As $k' \otimes_k k' \simeq \prod_{\sigma \in G} k'$, we have that

$$({}_kD)_{k'} \simeq \amalg_{\sigma \in G} D,$$

where $\tau \in G$ maps the σth copy of D to the $\tau\sigma$th copy. Elements of $E_{k'}(\amalg_{\sigma \in G} D)$ can be represented as tuples $f = (f_\sigma)_\sigma$ where $f_\sigma \in E_{k'}(D)$ and

$$({}^\tau f)_\sigma = \tau f_{\tau^{-1}\sigma}.$$

Similarly elements of $\operatorname{Hom}_R(R\langle G \rangle, E_{k'}(D))$ are tuples $g = (g_\sigma)_\sigma$ where $g \in E_{k'}(D)$ and $({}^\tau g)_\sigma = g_{\sigma\tau}$. The correspondence

$$g_\sigma = \sigma f_{\sigma^{-1}},$$

shows that these $R\langle G \rangle$-modules are isomorphic. □

Note that any finitely presented R-module with a semilinear G-action is also a finitely presented $R\langle G \rangle$-module, as we now explain. As R is noetherian, it suffices to show that any $R\langle G \rangle$-module M, which is finitely generated as an R-module, admits a G-equivariant surjection from $R\langle G \rangle^n$ for some n. If $m_1, \ldots, m_r$ are R-module generators of M, then the map $R\langle G \rangle^r \to M$ sending $e_i \mapsto m_i$ has the desired properties.

We have the following nice properties of the functor $\mathscr{H}om_{R\langle G \rangle}(\,\cdot\,, E_{k'})$.

Proposition 2.6. *Let E/k be an elliptic curve and k'/k a finite Galois extension with Galois group G. Let $R := \operatorname{End}_{k'} E$ and let M be a finitely presented $R\langle G \rangle$-module and let $A := \mathscr{H}om_{R\langle G \rangle}(M, E_{k'})$.*

1. *$\mathscr{H}om_{R\langle G \rangle}(\,\cdot\,, E_{k'})$ is exact.*
2. *A is a commutative proper group scheme over k of dimension $\operatorname{rk}_R(M)$.*
3. *If M is torsion-free as an R-module, then A is an abelian variety over k such that $A_{k'}$ is isogenous to a power of $E_{k'}$.*
4. *$\mathscr{H}om_{R\langle G \rangle}(R, E_{k'}) = E$.*

Proof. Parts (1)–(3) follow from the corresponding properties after base-extension to k' [4, ThM. 4.4]. For part (4), we have

$$\begin{aligned}\operatorname{Hom}_k(C, \mathscr{H}om_{R\langle G \rangle}(R, E_{k'})) &= \operatorname{Hom}_{R\langle G \rangle}(R, \operatorname{Hom}_{k'}(C_{k'}, E_{k'})) \\ &= \operatorname{Hom}_{k'}(C_{k'}, E_{k'})^G \\ &= \operatorname{Hom}_k(C, E).\end{aligned}$$

□

3. Examples and Applications

As an example of Theorem 1.2, we have the following in the special case k'/k is a separable quadratic extension.

Proposition 3.1. *Let k'/k be a separable quadratic extension and set $G := \operatorname{Gal}(k'/k)$ with nontrivial element σ. Let E' denote the corresponding k'/k quadratic twist of E. If M is a torsion-free $R\langle G \rangle$-module, then the abelian variety $\mathscr{H}om_{R\langle G \rangle}(M, E_{k'})$ is isogenous to $E^r \times (E')^{r'}$ for some $r, r' \geq 0$.*

Proof. As above, we denote the G-action on F by $\sigma(x) = {}^{\sigma}x$. By Theorem 1.2, it suffices to decompose $F\langle G\rangle$ into simple modules. Let ${}^{\sigma}F$ denote F endowed with the G-action $\sigma(x) = -{}^{\sigma}x$ for $x \in F$. Then we have an isomorphism

$$F \oplus {}^{\sigma}F \xrightarrow{\varphi} F\langle G\rangle,$$

defined by $\varphi(a, b) = a(\sigma + 1) + b(\sigma - 1)$. By comparing functors of points, we have $\mathscr{H}om_{F\langle G\rangle}(F, E_{k'}) \simeq E$ and $\mathscr{H}om_{F\langle G\rangle}({}^{\sigma}F, E_{k'}) \simeq E'$ in the isogeny category. □

Example 3.2. Consider the special case that k is a number field, and E has complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field $F = \operatorname{Frac}\mathcal{O}$, which is defined over the quadratic extension $k' = kF/k$ with Galois group $G = \{1, \sigma\}$. Let M be a finitely presented $\mathcal{O}\langle G\rangle$-module that is torsion-free as an $\mathcal{O}$-module. Then as multiplication by a totally imaginary element of $\mathcal{O}$ defines an isomorphism ${}^{\sigma}F \simeq F$ of $F\langle G\rangle$-modules, we have that $\mathscr{H}om_{\mathcal{O}\langle G\rangle}(M, E_{k'})$ is an abelian variety defined over k, which is isogenous over k to a power of E.

Continuing in the setup of the previous example, we conclude by proving Corollary 1.3.

Proof of Corollary 1.3. This follows from Example 3.2 as the full ring of integers $\mathcal{O}_F$ of F is a finitely presented $\mathcal{O}\langle G\rangle$-module, which is torsion-free of rank 1 over $\mathcal{O}$. The full endomorphism ring of E is defined over (the at most quadratic extension) k', so we have that $\mathcal{O} = \operatorname{End} E_{k'}$. This inherits a (possibly trivial) action of G. We therefore have the following exact sequence of $\mathcal{O}\langle G\rangle$-modules:

$$0 \to \mathcal{O} \to \mathcal{O}_F \to \mathcal{O}_F/\mathcal{O} \to 0,$$

where the action of G is induced from the action on F. Applying the functor $\mathscr{H}om_{\mathcal{O}\langle G\rangle}(\,\cdot\,, E_{k'})$ we obtain an exact sequence

$$0 \to \mathscr{H}om_{\mathcal{O}\langle G\rangle}(\mathcal{O}_F/\mathcal{O}, E_{k'}) \to E' \to E \to 0,$$

where E' is again an elliptic curve over k and the right map is an isogeny to E. By functoriality, $E'_{k'}$ has an action of $\mathcal{O}_F$, as desired. □

References

[1] D. J. Benson, *Representations and cohomology. I. Basic representation theory of finite groups and associative algebras*, Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, 1998.

[2] A. Bourdon & P. Pollack, "Torsion subgroups of CM elliptic curves over odd degree number fields", *Int. Math. Res. Not.* **2017** (2017), no. 16, p. 4923-4961.

[3] P. L. Clark, B. Cook & J. Stankewicz, "Torsion points on elliptic curves with complex multiplication", *Int. J. Number Theory* **9** (2013), no. 2, p. 447-479.

[4] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron & J. T. Tate, “Abelian varieties isogenous to a power of an elliptic curve”, *Compos. Math.* **154** (2018), no. 5, p. 934-959.

[5] S. Kwon, “Degree of isogenies of elliptic curves with complex multiplication”, *J. Korean Math. Soc.* **36** (1999), no. 5, p. 945-958.

[6] K. Rubin, “Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton–Dyer”, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, Lecture Notes in Mathematics, vol. 1716, Springer, 1997, p. 167-234.

[7] I. Vogt, “A local-global principle for isogenies of composite degree”, `https://arxiv.org/abs/1801.05355`, 2018.

Isabel Vogt
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139, USA
E-mail: `ivogt@mit.edu`
URL: `http://web.mit.edu/~ivogt/`