Journal of Number Theory 133 (2013) 2843–2856

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The constant of the support problem for abelian varieties

Jeroen Demeyer[a,∗,1], Antonella Perucca[b,2]

[a] Ghent University, Department of Mathematics, Krijgslaan 281, 9000 Gent, Belgium
[b] Fakultät Mathematik Universität Regensburg, D-93040 Regensburg, Germany

ARTICLE INFO

Article history:
Received 29 March 2011
Revised 23 January 2013
Accepted 23 January 2013
Available online 22 April 2013
Communicated by David Goss

MSC:
primary 14K15
secondary 11G10, 16H10, 16S50, 14L10

Keywords:
Abelian varieties
Endomorphism
Maximal order
Support problem
Tori

ABSTRACT

Let A be an abelian variety defined over a number field K and let P and Q be points in $A(K)$ satisfying the following condition: for all but finitely many primes $\mathfrak{p}$ of K, the order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$. Larsen proved that there exists a positive integer c such that cQ is in the $\mathrm{End}_K(A)$-module generated by P. We study the minimal value of c and construct some refined counterexamples.

1. Introduction

Let A be an abelian variety defined over a number field K. Let P, Q be points in $A(K)$ satisfying the following condition: for all but finitely many primes $\mathfrak{p}$ of K, the order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$. The support problem asks whether there exists a K-endomorphism of A mapping P to Q.

If A is K-simple and the points P and Q have infinite order, Khare and Prasad proved in [6, Theorem 1] that indeed $\phi(P) = Q$ for some ϕ in $\mathrm{End}_K(A)$. This result does not hold for general abelian varieties. However, Larsen proved that there exist a K-endomorphism ϕ of A and a positive

[∗] Corresponding author.
E-mail addresses: jdemeyer@cage.ugent.be (J. Demeyer), antonella.perucca@mathematik.uni-regensburg.de (A. Perucca).

[1] Postdoctoral fellow of the Research Foundation — Flanders (FWO).

[2] Lecturer at the University of Regensburg, postdoctoral fellow of the Research Foundation — Flanders (FWO) during the preparation of this paper.

0022-314X/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2013.01.013

integer c such that $\phi(P) = cQ$ [7, Theorem 1]. So in general one cannot take $c = 1$ (not even if ϕ is taken in $\mathrm{End}_{\bar{K}}(A)$), as shown by Larsen in [7, Proposition 2].

We study the minimal positive integer c (depending only on A and K) for which the following holds: for every pair of points P, Q in $A(K)$ satisfying the condition of the support problem, there exists a K-endomorphism ϕ of A such that $\phi(P) = cQ$. It is known that such an integer exists ([13, Proposition 10] or [8, Proposition 4.3 and Theorem 5.2]): we call it the constant of the support problem. The following question arises:

Question 1.1. Does the constant of the support problem divide the exponent of the torsion part of $A(K)$?

The answer is affirmative for simple abelian varieties, as a consequence of [6, Theorem 1]. Larsen proved in [8, Proposition 4.3 and Theorem 5.2] that the answer is affirmative whenever all the Tate modules of A are integrally semi-simple [8, Definition 4.1].

In this paper, we use a new method to study the support problem: we view the Mordell–Weil group as a module over the endomorphism ring and apply the theory of maximal orders in division algebras.

We prove that the answer to Question 1.1 is affirmative whenever A is a power of a simple abelian variety A_1 such that $\mathrm{End}_K(A_1)$ is a maximal order in a division algebra. More generally, the answer is affirmative for products $\prod A_i^{e_i}$ of such powers, provided that $\mathrm{Hom}_K(A_i, A_j) = 0$ for $i \neq j$, see Theorem 5.1. In particular, the answer is affirmative for at least one variety in every K-isogeny class (this also follows from the results of Larsen in [8]).

We also construct two counterexamples to Question 1.1 in Section 6. They are respectively of the following kind: the power of a simple abelian variety whose endomorphism ring is not a maximal order; an abelian variety which is $\bar{K}$-isomorphic (but not K-isomorphic) to the power of an elliptic curve whose endomorphism ring is a maximal order.

With a similar construction, we answer in the negative to the question of the support problem for tori, see Section 6.3.

A motivation to study the support problem is given by the following theorem which is a consequence of results on the support problem by Larsen [7], Khare and Prasad [6] and the second author [13]:

Theorem 1.2. *Let A be an abelian variety defined over a number field K. Let R be a point in $A(K)$ such that $\mathbb{Z}R$ is Zariski-dense in A. Let S be a set of primes of K of Dirichlet density* 1.

1. *The sequence*

$$\left\{\mathrm{ord}(R \bmod \mathfrak{p})\right\}_{\mathfrak{p}\in S}$$

determines the K-isomorphism class of A and determines R up to K-isomorphism.

2. *Let ℓ be a prime number and write ord_ℓ for the ℓ-adic valuation of the order. The sequence*

$$\left\{\mathrm{ord}_\ell(R \bmod \mathfrak{p})\right\}_{\mathfrak{p}\in S}$$

determines the K-isogeny class of A.

We prove this result at the end of Section 4. An important special case is when A is K-simple because then $\mathbb{Z}R$ is Zariski-dense in A for any point R of infinite order. Notice that we had to assume that $\mathbb{Z}R$ is Zariski-dense in A: for example the point R in A and the point $(R, 0)$ in the square of A give rise to the same sequences.

2. A result on maximal orders

We begin by recalling some notions concerning algebras, modules and orders. We mainly refer to [14].

Let R be an associative ring with 1, not necessarily commutative and without zero divisors. By “R-module”, if not specified otherwise, we mean *left* R-module.

Let $\mathcal{M}$ be an R-module. We say that $\mathcal{M}$ is *torsion-free* if for all $\alpha \in R \setminus \{0\}$ and $P \in \mathcal{M} \setminus \{0\}$, we have $\alpha P \neq 0$. We say that $\mathcal{M}$ is *divisible* if, for every $P \in \mathcal{M}$ and every $\alpha \in R \setminus \{0\}$, there exists $Q \in \mathcal{M}$ such that $P = \alpha Q$.

Definition 2.1. Let G be an R-module. Let $\mathcal{M}$ be a torsion-free submodule of G and let $P \in G$. We say that P is *independent* of $\mathcal{M}$ if $\alpha P \notin \mathcal{M}$ for all $\alpha \in R \setminus \{0\}$.

Lemma 2.2. *Let G be an R-module. The following are equivalent:*

1. *G contains a free R-module of infinite rank.*
2. *For all finitely generated R-modules $\mathcal{M} \subseteq G$, there exists some $P \in G$ which is independent of $\mathcal{M}$.*

Proof. **1 ⇒ 2**: Let $n \in \mathbb{N}$ be such that $\mathcal{M}$ can be generated by n elements. By assumption, G contains a free submodule $\mathcal{B} = RB_1 \oplus \cdots \oplus RB_{n+1}$. Suppose that none of the points B_i is independent of $\mathcal{M}$. Then there would exist $\alpha_i \in R \setminus \{0\}$ such that $\alpha_i B_i \in \mathcal{M}$ for all $i = 1, \ldots, n+1$. Since $\mathcal{M}$ is generated by n elements, there must be some non-trivial linear combination $\sum \beta_i(\alpha_i B_i)$ which is zero. This is a contradiction.

2 ⇒ 1: We reason by induction. Clearly, $\{0\} \subseteq G$ is free of rank 0. Let $\mathcal{M} \subseteq G$ be a free R-module of rank n. Since $\mathcal{M}$ is finitely generated, there exists a $P \in G$ which is independent of $\mathcal{M}$. Then $\mathcal{M} + RP \simeq R^{n+1}$. Indeed, suppose that $Q + \alpha P = 0$ for some $Q \in \mathcal{M}$ and $\alpha \in R$. Then $\alpha P \in \mathcal{M}$, therefore $\alpha = 0$ and also $Q = 0$. □

We recall the definition of tensor products for modules over a ring which is not necessarily commutative:

Definition. Let $\mathcal{M}$ be a right R-module and $\mathcal{N}$ a left R-module. Then the *tensor product* $\mathcal{M} \otimes_R \mathcal{N}$ is the free abelian group on the symbols $m \otimes n$, where $m \in \mathcal{M}$ and $n \in \mathcal{N}$, modulo the relations $(m + m') \otimes n = m \otimes n + m' \otimes n$, $m \otimes (n + n') = m \otimes n + m \otimes n'$, $(mr) \otimes n = m \otimes (rn)$ for all $m, m' \in \mathcal{M}$, $n, n' \in \mathcal{N}$, $r \in R$.

This tensor product is always an abelian group, but in general not an R-module. If $\mathcal{M}$ is a two-sided R-module, then $\mathcal{M} \otimes_R \mathcal{N}$ becomes a left R-module by defining $r(m \otimes n) := (rm) \otimes n$.

In this paper, a $\mathbb{Q}$-algebra means a ring $D \supseteq \mathbb{Q}$ which is a finite dimensional $\mathbb{Q}$-vector space. We do not assume that the centre is exactly $\mathbb{Q}$.

Let D be a $\mathbb{Q}$-algebra. An *order* in D is a subring $R \subseteq D$ whose additive group is finitely generated and such that $\mathbb{Q}R = D$. A *maximal order* is an order which is not contained in any larger order. If D is a number field, the ring of integers is the unique maximal order.

Proposition 2.3. *Let R be a maximal order in a $\mathbb{Q}$-division algebra D. The centre of R is the ring of integers of the number field K, where K denotes the centre of D.*

Proof. Let $\mathcal{O}_K$ denote the ring of integers of K. We have $\mathbb{Q}R = D$, therefore the centre of R is $R \cap K$. Since $R \cap K$ is an order in K, we must have $R \cap K \subseteq \mathcal{O}_K$. Conversely, $\mathcal{O}_K R$ is an order in D. Since R is a maximal order, this implies that $\mathcal{O}_K \subseteq R$. We conclude that $\mathcal{O}_K = R \cap K$. □

Lemma 2.4. *Let D be a $\mathbb{Q}$-division algebra and let R be a maximal order in D. Let $\mathcal{M}$ be a finitely generated and torsion-free R-module. Then $\mathcal{M}$ is projective.*

Proof. Since R is a maximal $\mathbb{Z}$-order in the $\mathbb{Q}$-algebra D, it follows from [14, (21.4)] that R is a left (and right) hereditary ring. Such rings have the property that all submodules of free modules are projective, see [14, (2.44)]. So it suffices to show that $\mathcal{M}$ can be embedded in a free R-module.

Define $V := D \otimes_R \mathcal{M}$. Since $\mathcal{M}$ is torsion-free, the map

$$\theta : \mathcal{M} \to D \otimes_R \mathcal{M}; \quad m \mapsto 1 \otimes m$$

is an embedding of R-modules. Let $\{v_1, \dots, v_r\}$ be a basis of V as D-vector space. Since $\mathbb{Q}R = D$, there exists $b \in \mathbb{Z} \setminus \{0\}$ such that $b\theta(\mathcal{M})$ is contained in $Rv_1 \oplus \cdots \oplus Rv_r$. Then the map $\mathcal{M} \to V : m \mapsto b\theta(m)$ embeds $\mathcal{M}$ into R^r. □

Theorem 2.5. *Let D be a $\mathbb{Q}$-division algebra and let R be a maximal order in D. Let G be an R-module containing a submodule isomorphic to $R^{\mathbb{N}}$. Let $\mathcal{M} \subseteq \mathcal{N}$ be finitely generated and torsion-free submodules of G. Then there exists a finitely generated free module $\mathcal{F} \subseteq G$ such that $\mathcal{F} \cap \mathcal{N} = \mathcal{M}$.*

Proof. By Lemma 2.4, $\mathcal{M}$ is projective. This means that there exists an abstract R-module $\mathcal{A}$ such that $\mathcal{M} \oplus \mathcal{A} \simeq R^r$ for some $r \geqslant 0$.

By Lemma 2.2, there exists $B_1 \in G$ which is independent of $\mathcal{N}$. Since $\mathcal{N}$ and RB_1 are torsion-free, also $\mathcal{N} \oplus RB_1$ is torsion-free. Analogously, we can find $B_2, \dots, B_r$ in G such that, for all $k = 2, \dots, r$, the point B_k is independent of $\mathcal{N} \oplus \langle B_1, \dots, B_{k-1} \rangle$. Eventually, we get a finitely generated and torsion-free module $\mathcal{N} \oplus \langle B_1, \dots, B_r \rangle$.

Since $\mathcal{M} \oplus \mathcal{A} \simeq R^r \simeq \langle B_1, \dots, B_r \rangle$, we can see $\mathcal{A}$ as a submodule of $\langle B_1, \dots, B_r \rangle$. Now $\mathcal{M}$ and $\mathcal{A}$ are submodules of G satisfying $\mathcal{M} \cap \mathcal{A} \subseteq \mathcal{N} \cap \langle B_1, \dots, B_r \rangle = \{0\}$. Let $\mathcal{F} := \mathcal{M} \oplus \mathcal{A}$. We clearly have $\mathcal{M} \subseteq \mathcal{F} \cap \mathcal{N}$.

Let $P \in \mathcal{F} \cap \mathcal{N}$. We need to show that $P \in \mathcal{M}$. We can write $P = P_{\mathcal{M}} + P_{\mathcal{A}}$ with $P_{\mathcal{M}} \in \mathcal{M}$ and $P_{\mathcal{A}} \in \mathcal{A}$. Since $P \in \mathcal{N}$ and $P_{\mathcal{M}} \in \mathcal{N}$, we also have $P_{\mathcal{A}} \in \mathcal{N}$. But $\mathcal{N} \cap \mathcal{A} = \{0\}$, therefore $P_{\mathcal{A}} = 0$ and $P = P_{\mathcal{M}}$. □

3. Preliminaries on abelian varieties

Let A be an abelian variety defined over a number field K and let L be an extension of K. We write $\mathrm{End}_L(A)$ for the ring of endomorphisms of A which are defined over L. Let $D := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then D is a finite dimensional $\mathbb{Q}$-algebra and $\mathrm{End}_K(A)$ is an order in D. If A is K-simple, then $\mathrm{End}_K(A)$ does not contain any zero divisors and D is a division algebra.

The group $A(\bar{K})$ is a divisible $\mathbb{Z}$-module [11, Theorem 7.2]. If A is K-simple, then $A(\bar{K})$ is also a divisible $\mathrm{End}_K(A)$-module: this is because every non-zero element of $\mathrm{End}_K(A)$ is an isogeny and thus it divides the multiplication by some non-zero integer.

Definition 3.1. We say that a point in $A(K)$ of infinite order is *independent* if it generates a free $\mathrm{End}_K(A)$-module or, equivalently, a free $\mathrm{End}_{\bar{K}}(A)$-module. This is also equivalent to the fact that $\mathbb{Z}R$ is Zariski-dense in A. See [12, Section 2]. We say that finitely many points $\{P_1, \dots, P_n\}$ on n abelian varieties $A_1, \dots, A_n$ are independent if the point $(P_1, \dots, P_n)$ in $\prod_{i=1}^n A_i(K)$ is independent.

Proposition 3.2. *Let K be a number field and fix an algebraic closure $\bar{K}$ of K. Let $F \subseteq \bar{K}$ be a finite extension of K. Then there exists an extension $E \subseteq \bar{K}$ of K such that $E \cap F = K$ and such that, for every abelian variety A/K of positive dimension, $A(E)$ has infinite rank.*

Proof. Without loss of generality, we may assume that F/K is Galois. Let $\{\sigma_1, \dots, \sigma_e\}$ be generators of $\mathrm{Gal}(F/K)$. We can equip $\mathrm{Gal}(\bar{K}/K)$ with the normalized Haar measure and consider the product measure on $\mathrm{Gal}(\bar{K}/K)^e$. By translation invariance, the set of all lifts of $(\sigma_1, \dots, \sigma_e)$ in $\mathrm{Gal}(\bar{K}/K)^e$ has the same measure as the set of lifts of $(\mathrm{id}, \dots, \mathrm{id})$. Therefore, the set of lifts of $(\sigma_1, \dots, \sigma_e)$ has positive measure $[F : K]^{-e}$ [3, Lemma 1.1]. So by [3, Theorem 9.1] there exists a lift $(\tau_1, \dots, \tau_e)$ of $(\sigma_1, \dots, \sigma_e)$ in $\mathrm{Gal}(\bar{K}/K)^e$ such that the following holds: for all abelian varieties A/K of positive dimension, the rank of $A(E)$ is infinite, where E is the subfield of $\bar{K}$ fixed by $\{\tau_1, \ldots, \tau_e\}$. Every element of $F \cap E$ must be fixed by $\{\sigma_1, \ldots, \sigma_e\}$, therefore $E \cap F = K$. □

Every simple abelian variety is isogenous to a simple abelian variety whose endomorphism ring is a maximal order in a division algebra:

Proposition 3.3. *Let A be an abelian variety defined over a number field K and assume that A is K-simple. Let $R := \mathrm{End}_K(A)$ and $D := R \otimes_{\mathbb{Z}} \mathbb{Q}$. Let Λ be a maximal order in D. There exists an abelian variety B defined over K which is K-isogenous to A and such that $\mathrm{End}_K(B) \simeq \Lambda$.*

Proof. Since R and Λ are full-rank lattices in the same $\mathbb{Q}$-vector space, we can take an $n \in \mathbb{Z} \setminus \{0\}$ such that $n\Lambda \subseteq R$. Define

$$\Delta := n\Lambda \quad \text{and} \quad H := \bigl\{T \in A(\bar{K}) \bigm| \Delta \cdot T = 0\bigr\}.$$

Since H is contained in $A[n]$, it is a finite group. Consider the quotient abelian variety $B := A/H$. Since the endomorphisms in $\Delta \subseteq R$ are defined over K, it follows that H is stable under $\mathrm{Gal}(\bar{K}/K)$. Therefore, B and the projection isogeny $\pi : A \to B$ are defined over K.

Now we prove that the endomorphism ring of B is Λ. Since A and B are K-isogenous, they have the same K-endomorphism algebra; hence, $\mathrm{End}_K(B)$ is an order in D. Since $A(\bar{K})$ is divisible, we can write every point P in $B(\bar{K})$ as $P = \pi(n\hat{P})$ for some $\hat{P} \in A(\bar{K})$. Let α be in Λ and remark that $\alpha n = n\alpha$ belongs to R. Thus we can define

$$\alpha P = \pi\bigl((\alpha n)\hat{P}\bigr).$$

This definition does not depend on the choice of $\hat{P}$. Indeed, let $P = \pi(n\hat{P}')$. Then the difference $n(\hat{P} - \hat{P}')$ is in H because π maps it to 0. This implies $\Delta n(\hat{P} - \hat{P}') = 0$. Since Δ is a right Λ-module, we have $\Delta\alpha n \subseteq \Delta n$ and so $\Delta\alpha n(\hat{P} - \hat{P}') = 0$. This means that $\pi((\alpha n)\hat{P}) = \pi((\alpha n)\hat{P}')$.

It is clear that α is an endomorphism and that the above map $\Lambda \to \mathrm{End}_K(B)$ is an injection of rings. Since Λ is a maximal order, this must be an isomorphism. □

4. The condition of the support problem

Let A be an abelian variety defined over a number field K and let P and Q be points in $A(K)$. The support problem asks whether there exists a K-endomorphism of A which maps P to Q, provided that the following condition is satisfied:

Condition (SP). For all but finitely many primes $\mathfrak{p}$ of K, the order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$.

We reformulate the condition of the support problem by using $\mathrm{End}_K(A)$-modules instead of points on $A(K)$. Let Q be a point in $A(K)$ and let $\mathcal{M}$ be an $\mathrm{End}_K(A)$-submodule of $A(K)$. The condition of the support problem for modules is the following:

Condition (SPM). For all but finitely many primes $\mathfrak{p}$ of K, the order of $(Q \bmod \mathfrak{p})$ divides the exponent of $(\mathcal{M} \bmod \mathfrak{p})$.

The question now is whether Q belongs to $\mathcal{M}$. For free modules, we have the analogue of [13, Proposition 9]:

Theorem 4.1. *Let A be an abelian variety defined over a number field K. Let $\mathcal{F}$ be a free $\mathrm{End}_K(A)$-submodule of $A(K)$ and let $Q \in A(K)$. If Q and $\mathcal{F}$ satisfy Condition (SPM), then $Q \in \mathcal{F}$.*

Proof. Let $\{P_1, \ldots, P_n\}$ be a basis of $\mathcal{F}$ and consider $P' = (P_1, \ldots, P_n) \in A^n(K)$. Since $\mathcal{F}$ is a free module, the point P' is independent in A^n. Then we can apply [13, Proposition 9] to the points $P' = (P_1, \ldots, P_n)$ and $Q' = (Q, 0, \ldots, 0)$ in $A^n(K)$. We find $Q' = \phi(P')$ for some $\phi \in \mathrm{End}_K(A^n)$, which implies $Q \in \mathcal{F}$. □

It is important to note that Conditions (SP) and (SPM) do not depend on the field: if the condition is satisfied over a field K, it is also satisfied over any finite extension.

In this paper, coherently to the other references on the support problem, we consider Conditions (SP) and (SPM) for all but finitely many primes $\mathfrak{p}$ of K. However, it is possible to require the conditions only for a set of primes $\mathfrak{p}$ of K of Dirichlet density 1. The same results hold as soon as the proofs are based on the Cebotarev Density Theorem. For example, one has:

Theorem 4.2. *(See [13, Corollary 8 and Proposition 9].) Let A and A' be products of an abelian variety and a torus defined over a number field K. Let R be a point in $A(K)$ and let R' be a point in $A'(K)$. Let ℓ be a rational prime and let S be a set of primes of K of Dirichlet density 1. Suppose that for every $\mathfrak{p} \in S$ we have*

$$\mathrm{ord}_\ell(R \bmod \mathfrak{p}) \geqslant \mathrm{ord}_\ell\big(R' \bmod \mathfrak{p}\big).$$

Then there exist $\phi \in \mathrm{Hom}_K(A, A')$ and a non-zero integer c such that $\phi(R) = cR'$. If $\mathbb{Z}R$ is Zariski-dense in A, one can take c coprime to ℓ.

Corollary 4.3. *Let A be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $A(K)$ such that $\mathbb{Z}R$ is Zariski-dense in A. Let S be a set of primes of K of Dirichlet density 1.*

1. *The sequence*

$$\big\{\mathrm{ord}(R \bmod \mathfrak{p})\big\}_{\mathfrak{p}\in S}$$

determines the K-isomorphism class of A and determines R up to K-isomorphism.

2. *Let ℓ be a prime number and write ord_ℓ for the ℓ-adic valuation of the order. The sequence*

$$\big\{\mathrm{ord}_\ell(R \bmod \mathfrak{p})\big\}_{\mathfrak{p}\in S}$$

determines the K-isogeny class of A.

Proof. Let A' be the product of an abelian variety and a torus defined over K and let R' be a point in $A'(K)$ such that $\mathbb{Z}R'$ is Zariski-dense in A'. Suppose that $\mathrm{ord}_\ell(R \bmod \mathfrak{p}) = \mathrm{ord}_\ell(R' \bmod \mathfrak{p})$ for every $\mathfrak{p} \in S$. Then by Theorem 4.2 there exist an integer c coprime to ℓ and a K-homomorphism ϕ from A to A' mapping R to cR' and analogously there exist an integer c' coprime to ℓ and a K-homomorphism ϕ' from A' to A mapping R' to $c'R$. Then $\phi' \circ \phi$ maps R to $c'cR$. Since $\mathbb{Z}R$ is Zariski-dense in A, we deduce $\phi' \circ \phi = [c'c]$. In particular, ϕ is an isogeny of degree coprime to ℓ. Now suppose that $\mathrm{ord}(R \bmod \mathfrak{p}) = \mathrm{ord}(R' \bmod \mathfrak{p})$ for every $\mathfrak{p} \in S$. Then we can take $c = c' = 1$ (consider a suitable finite linear combination of the isogenies obtained for each prime ℓ). Thus ϕ is a K-isomorphism mapping R to R'. □

5. Positive results for the constant of the support problem

In this section, we prove that Question 1.1 has an affirmative answer provided that the abelian variety is of the following type: it is the product of powers of simple abelian varieties, which are in pairs non-isogenous and whose endomorphism rings are maximal orders in division algebras.

We start with the torsion-free case.

Theorem 5.1. *Let $A_1, \ldots, A_n$ be abelian varieties defined over a number field K and let $A := A_1 \times \cdots \times A_n$. Suppose that all A_i are K-simple and that $\mathrm{Hom}_K(A_i, A_j) = \{0\}$ whenever $i \neq j$. Assume that every $\mathrm{End}_K(A_i)$ is a maximal order. Let $\mathcal{M}$ be an $\mathrm{End}_K(A)$-submodule of $A(K)$ and let $Q \in A(K)$. If Q and $\mathcal{M}$ satisfy Condition (SPM) and $\mathcal{M}$ is torsion-free, then $Q \in \mathcal{M}$.*

Proof. Let $R := \mathrm{End}_K(A)$. The assumptions on A imply that $R \simeq \mathrm{End}_K(A_1) \times \cdots \times \mathrm{End}_K(A_n)$. Define $\mathcal{M}_i$ as the projection of $\mathcal{M}$ onto the factor $A_i(K)$. So $\mathcal{M}_i$ is an $\mathrm{End}_K(A_i)$-module and we have

$$\mathcal{M} = \mathcal{M}_1 \times \cdots \times \mathcal{M}_n.$$

Let $\mathcal{N} := \mathcal{M} + RQ$. Analogously, we can write $\mathcal{N} = \mathcal{N}_1 \times \cdots \times \mathcal{N}_n$.

Since every $\mathrm{End}_{\bar{K}}(A_i)$ is a finitely generated group, there exists a finite extension F of K such that $\mathrm{End}_{\bar{K}}(A_i) = \mathrm{End}_F(A_i)$ for all i. We apply Proposition 3.2 to find a field $E \subseteq \bar{K}$ such that $E \cap F = K$ and such that every $A_i(E)$ has infinite rank as a $\mathbb{Z}$-module. Clearly, $\mathrm{End}_E(A_i) = \mathrm{End}_K(A_i)$ for all i. Recall that every non-zero element of $\mathrm{End}_K(A_i)$ divides a non-zero integer. Then, by applying Lemma 2.2, it easily follows that $A_i(E)$ contains a free $\mathrm{End}_K(A_i)$-module of infinite rank.

The modules $\mathcal{M}$ and $\mathcal{N}$ are finitely generated since $A(K)$ is finitely generated. By assumption $\mathcal{M}$ is torsion-free; we now prove that $\mathcal{N}$ is torsion-free. Let e be the exponent of $\mathcal{N}_{\mathrm{tor}}$ and suppose $e > 1$. For all $i = 1, \ldots, n$, Theorem 2.5 (with $G := A_i(E)$ and $R := \mathrm{End}_K(A_i)$) shows that $\mathcal{M}_i$ is contained in a finitely generated free $\mathrm{End}_K(A_i)$-module $\mathcal{F}_i \subseteq A_i(E)$. For every i, let $\{F_{i1}, \ldots, F_{ir_i}\}$ be a basis for $\mathcal{F}_i$. Let $L \subseteq E$ be a finite extension of K where all points F_{ij} are defined. Since the points $\{F_{ij}\}$ are independent, by [12, Proposition 12] there exists a positive density of primes $\mathfrak{p}$ of L such that for every i and j the order of $(F_{ij} \bmod \mathfrak{p})$ is coprime to e. Hence, the exponent of $(\mathcal{M} \bmod \mathfrak{p})$ is coprime to e. After removing finitely many primes $\mathfrak{p}$ we may assume that $\mathrm{ord}(Q \bmod \mathfrak{p}) \mid \exp(\mathcal{M} \bmod \mathfrak{p})$ and also that $\exp(\mathcal{N}_{\mathrm{tor}} \bmod \mathfrak{p}) = e$. It follows that the exponent of $(\mathcal{N} \bmod \mathfrak{p})$ is coprime to e. We have a contradiction: the exponent of $(\mathcal{N} \bmod \mathfrak{p})$ is a multiple of e, but it is also coprime to e.

We can apply Theorem 2.5 on $\mathcal{M}_i \subseteq \mathcal{N}_i$, for every $i = 1, \ldots, n$. We find that $\mathcal{M}_i$ is contained in a finitely generated free $\mathrm{End}_K(A_i)$-module $\mathcal{F}_i \subseteq A_i(E)$ such that $\mathcal{F}_i \cap \mathcal{N}_i = \mathcal{M}_i$. These free modules $\mathcal{F}_i$ can be chosen of arbitrarily large rank, so choose them such that their ranks are all equal to some $r > 0$. Then $\mathcal{F} := \mathcal{F}_1 \times \cdots \times \mathcal{F}_n$ is a free R-module of rank r such that $\mathcal{F} \cap \mathcal{N} = \mathcal{M}$. Let $L \subseteq E$ be a finite extension of K such that all points of $\mathcal{F}$ are defined over L. Since Q and $\mathcal{F}$ satisfy Condition (SPM) and $\mathcal{F}$ is free over $\mathrm{End}_L(A) = R$, Theorem 4.1 implies that $Q \in \mathcal{F}$. Thus $Q \in \mathcal{F} \cap \mathcal{N} = \mathcal{M}$. □

Corollary 5.2. *Let A be an abelian variety defined over a number field K. Suppose that $A = \prod_{i=1}^{n} A_i^{e_i}$ is the product of powers of K-simple abelian varieties, which are in pairs non-K-isogenous. Suppose that $\mathrm{End}_K(A_i)$ is a maximal order for every $i = 1, \ldots, n$. Let P and Q be points in $A(K)$ satisfying Condition (SP). Suppose that the $\mathrm{End}_K(A)$-module generated by P is torsion-free. Then there exists ϕ in $\mathrm{End}_K(A)$ such that $\phi(P) = Q$.*

Proof. Let $\bar{A} = A_1 \times \cdots \times A_n$ and $\bar{\mathcal{M}} = \mathrm{Hom}_K(A, \bar{A}) \cdot P$. The assumption on P implies that $\bar{\mathcal{M}}$ is a torsion-free $\mathrm{End}_K(\bar{A})$-module. Notice that the identity of $\mathrm{End}_K(A)$ can be written as $\beta_1\alpha_1 + \cdots + \beta_m\alpha_m$ for some $m \in \mathbb{N}$, where $\alpha_i \in \mathrm{Hom}_K(A, \bar{A})$ and $\beta_i \in \mathrm{Hom}_K(\bar{A}, A)$.

Let σ be any element of $\mathrm{Hom}_K(A, \bar{A})$ and let $\bar{Q} := \sigma Q$. If $\mathfrak{p}$ is a prime of K, we have $\mathrm{ord}(\bar{Q} \bmod \mathfrak{p}) \mid \mathrm{ord}(Q \bmod \mathfrak{p})$ and $\mathrm{ord}(\beta_i\alpha_i P \bmod \mathfrak{p}) \mid \mathrm{ord}(\alpha_i P \bmod \mathfrak{p})$ for every $i = 1, \ldots, m$. We deduce that $\mathrm{ord}(P \bmod \mathfrak{p}) \mid \exp(\bar{\mathcal{M}} \bmod \mathfrak{p})$ and then that $\bar{Q}$ and $\bar{\mathcal{M}}$ satisfy Condition (SPM). By applying Theorem 5.1, we get that $\bar{Q} \in \bar{\mathcal{M}}$.

Since σ was chosen freely, for every $i = 1, \ldots, m$ there exists $\psi_i \in \mathrm{Hom}(A, \bar{A})$ such that $\alpha_i Q = \psi_i P$. Thus $Q = \sum_i \beta_i\alpha_i Q = (\sum_i \beta_i\psi_i)(P)$. □

We now turn our attention from torsion-free $\mathrm{End}_K(A)$-modules to the general case. Consider the following property:

Definition 5.3. Let R be a ring and let $\mathcal{M}$ be an R-module with a finite number of elements. We call $\mathcal{M}$ *semi-cyclic* if the following property is satisfied: for any two elements T_1 and T_2 in $\mathcal{M}$ with $\mathrm{ord}(T_1) \mid \mathrm{ord}(T_2)$, we must have that $T_1 = \phi T_2$ for some $\phi \in R$.

This notion of semi-cyclic is "in between" the notions of cyclic group and cyclic module. Indeed, an R-module whose additive group is cyclic, is obviously semi-cyclic. On the other hand, a finite semi-cyclic R-module is generated (as R-module) by any element of largest order.

Let A be an abelian variety defined over a number field K. Whenever the torsion part of $A(K)$ is not a semi-cyclic $\mathrm{End}_K(A)$-module, the constant of the support problem is greater than 1 (take P and Q independent torsion points of the same order).

Corollary 5.4. *Let A be as in Corollary 5.2. Let $c \in \mathbb{N}$ be such that $c \cdot A(K)_{\mathrm{tor}}$ is a semi-cyclic $\mathrm{End}_K(A)$-module. Let P and Q be points in $A(K)$ satisfying Condition (SP). Then there exists ϕ in $\mathrm{End}_K(A)$ such that $Q = \phi(P) + T$ for some $T \in A(K)[c]$.*

Proof. Let $\mathcal{M}$ be the $\mathrm{End}_K(A)$-module generated by P and let e be the exponent of the torsion part of $\mathcal{M}$. By applying Corollary 5.2 to eP and eQ, we find $\phi(eP) = eQ$ for some ϕ in $\mathrm{End}_K(A)$.

Let $T := Q - \phi P$, then $\mathrm{ord}(T) \mid e$. Let T_e be a torsion point in $\mathcal{M}$ of order e and write $T_e = \tau P$. The fact that $cA(K)_{\mathrm{tor}}$ is semi-cyclic implies that $cT = \psi c T_e$ for some $\psi \in \mathrm{End}_K(A)$. Now we can write $Q = (\phi + \psi\tau)P + (T - \psi T_e)$ with $c(T - \psi T_e) = 0$. □

This corollary has two important special cases. Firstly, if $A(K)_{\mathrm{tor}}$ is semi-cyclic then we can take $c = 1$ and we find that $Q = \phi(P)$ for some $\phi \in \mathrm{End}_K(A)$. Secondly, since the zero module is semi-cyclic, we can always take c to be the exponent of $A(K)_{\mathrm{tor}}$. Then we have $Q = \phi(P) + T$ for some $T \in A(K)_{\mathrm{tor}}$ and $\phi \in \mathrm{End}_K(A)$.

The question whether or not (SP) implies $Q = \phi(P) + T$ for some torsion point T in $A(K)$ has been investigated by Larsen and Schoof in [8] and [9]. They showed in [9] that this is not true in general. However in [8, Proposition 4.3 and Theorem 5.2] Larsen proved that the above property holds for at least one variety in every K-isogeny class (whenever all Tate modules of A are integrally semi-simple [8, Definition 4.1]). This also follows from our results: by the Poincaré Reducibility Theorem and by Proposition 3.3, in every K-isogeny class there is at least one variety satisfying the hypothesis of Corollary 5.2.

6. Refined counterexamples to the support problem

6.1. First counterexample

We construct a counterexample to Question 1.1. The abelian variety in this counterexample is the square of an absolutely simple abelian variety whose endomorphism ring is not a maximal order.

Let ζ_7 be a primitive seventh root of unity and consider $\tau := \zeta_7 + \zeta_7^{-1}$. The ring $R := \mathbb{Z}[2\tau, 2\tau^2]$ is a non-maximal order in $\mathbb{Q}(\tau)$. Let $\mathfrak{m} := (2, 2\tau, 2\tau^2)$, a maximal ideal in R with residue field $\mathbb{F}_2$.

In Appendix A, we constructed an abelian variety A defined over a number field K satisfying the following properties: it is absolutely simple, it has dimension 6, $\mathrm{End}_{\bar{K}}(A) = R$ and $A[2] \simeq (R/2R)^2 \times (R/\mathfrak{m})^6$ as R-modules.

Enlarge K if necessary such that the 2-torsion points on A are K-rational, such that all endomorphisms of A are defined over K and such that $A(K)$ contains a point of infinite order. Let $L_1, \dots, L_8 \in A[2]$ be such that

$$A[2] = (R/2R)L_1 \oplus (R/2R)L_2 \oplus (R/\mathfrak{m})L_3 \oplus \cdots \oplus (R/\mathfrak{m})L_8.$$

In the ring $R/2R$, all elements apart from 0 and 1 have $\mathfrak{m}$ as annihilator. This implies the following crucial fact:

Observation 6.1. Every point of $A[2]$ has as annihilator inside $\mathrm{End}_K(A)$ either (1), (2) or $\mathfrak{m} = (2, 2\tau, 2\tau^2)$.

A result by Bogomolov [1, Corollaire 1] tells us that the image of the 2-adic representation of A contains an open subset of the homotheties of the Tate module $\mathrm{T}_2 A$. In particular, there exist an integer $t \geqslant 2$ and an element of the Galois group which fixes every point in $A[2^t]$ and does not fix any point of A order 2^{t+1}. Then, after extending K, we may assume that all the 2^t-torsion points of A are K-rational but no point of order 2^{t+1} is K-rational. For $i \in \{1, \dots, 8\}$, choose T_i in $A(K)$ such that $2^{t-1} T_i = L_i$. In particular, T_i has order 2^t.

Let S be a point of infinite order on $A(K)$. Let $G := A \times A$ and consider the following points in $G(K)$:

$$P = (2S + T_1, 2\tau S + T_2) \quad \text{and} \quad Q = \bigl(2\tau^2 S + T_3, 0\bigr).$$

We claim that the points P and Q satisfy Condition (SP) for every prime $\mathfrak{p}$ of good reduction for A, not over 2. By [4, Theorem C.1.4], the reduction modulo $\mathfrak{p}$ gives an isomorphism from $A[2^t]$ to $(A \bmod \mathfrak{p})[2^t]$. If n is the order of $(P \bmod \mathfrak{p})$, we have

$$2nS + nT_1 \equiv 0 \pmod{\mathfrak{p}} \quad \text{and} \quad 2\tau nS + nT_2 \equiv 0 \pmod{\mathfrak{p}}. \tag{1}$$

It follows that $(2\tau n T_1 \bmod \mathfrak{p}) = (2nT_2 \bmod \mathfrak{p})$. Then we have $2\tau n T_1 = 2nT_2$. This is only possible if $2\tau n T_1 = 2nT_2 = 0$. Since $\mathrm{Ann}(L_1) = (2)$, we have $\mathrm{Ann}(T_1) = (2^t)$; hence n is a multiple of 2^t.

From (1) we deduce that $(nS \bmod \mathfrak{p})$ equals $(U \bmod \mathfrak{p})$ for a point U in $A[2]$. Since $nT_3 = 0$, to prove that $(nQ \bmod \mathfrak{p}) = 0$, it suffices to show that $2\tau^2 U = 0$. By (1), we know that $(2\tau nS \bmod \mathfrak{p}) = 0$. Therefore $2\tau U = 0$. Because of Observation 6.1, this implies $2\tau^2 U = 0$.

Suppose that c is an integer such that $\phi(P) = cQ$ for some ϕ in $\mathrm{End}_K(A)$. We now prove that c must be a multiple of 2^{t+1}. Because $A(K)$ has no torsion point of order 2^{t+1}, this will give a counterexample to Question 1.1.

Since $\phi(P) = cQ$, there exist $\phi_1, \phi_2 \in \mathrm{End}_K(A)$ such that

$$\phi_1(2S + T_1) + \phi_2(2\tau S + T_2) = 2\tau^2 cS + cT_3. \tag{2}$$

After rearranging the terms:

$$\bigl(2\tau^2 c - 2\phi_1 - 2\tau\phi_2\bigr)S = \phi_1 T_1 + \phi_2 T_2 - cT_3. \tag{3}$$

Since S has infinite order and the points T_1, T_2, T_3 are independent over $R/2^t R$, (3) implies

$$2\tau^2 c - 2\phi_1 - 2\tau\phi_2 = 0; \qquad \phi_1 T_1 = \phi_2 T_2 = cT_3 = 0. \tag{4}$$

Since $\mathrm{Ann}(T_1) = \mathrm{Ann}(T_2) = (2^t)$ and T_3 has order 2^t, we can divide ϕ_1, ϕ_2 and c by 2^t. So there exist ϕ_1' and ϕ_2' in $\mathrm{End}_K(A)$ and an integer c' such that $\phi_1 = 2^t\phi_1'$, $\phi_2 = 2^t\phi_2'$ and $c = 2^t c'$. Then (4) implies

$$2\tau^2 c' - 2\phi_1' - 2\tau\phi_2' = 0.$$

An odd multiple of $2\tau^2$ is not contained in the ideal $(2, 2\tau)$. Therefore, c' is even and c is divisible by 2^{t+1}.

6.2. Second counterexample

We construct a different counterexample for Question 1.1. Only after a finite extension of the base field, the abelian variety of this counterexample is isomorphic to the power of an elliptic curve whose endomorphism ring is a maximal order. The two given points lie on a proper abelian subvariety and one point is the image of the other by an isomorphism of the subvariety.

Consider the following elliptic curves over $\mathbb{Q}$:

$$A\colon\ y^2 = x^3 + 40,$$
$$B\colon\ y^2 = x^3 + 5.$$

Both A and B have complex multiplication over the field $\mathbb{Q}(\zeta_3)$, where ζ_3 corresponds to the map $x \mapsto \zeta_3 x;\ y \mapsto y$. This means that $\operatorname{End}_{\bar{\mathbb{Q}}}(A) \simeq \operatorname{End}_{\bar{\mathbb{Q}}}(B) \simeq \mathbb{Z}[\zeta_3]$, the maximal order in $\mathbb{Q}(\zeta_3)$. The two curves are isomorphic over $\mathbb{Q}(\sqrt{2})$ (from B to A, consider $\theta : x \mapsto 2x;\ y \mapsto 2\sqrt{2}y$). However, the two curves are not isogenous over $\mathbb{Q}$. Suppose there is an isogeny $\alpha \in \operatorname{Hom}_{\mathbb{Q}}(A, B)$. Then $\theta \circ \alpha$ is an endomorphism of A defined over $\mathbb{Q}(\sqrt{2})$. Since $\operatorname{End}_{\mathbb{Q}(\sqrt{2})}(A) = \operatorname{End}_{\mathbb{Q}}(A)$ and α is defined over $\mathbb{Q}$, it would follow that θ is also defined over $\mathbb{Q}$.

The map θ induces an isomorphism of Galois modules from $B[2]$ to $A[2]$. Thus the group

$$H := \bigl\{(\theta T, T) \in \bigl(A(\bar{K}), B(\bar{K})\bigr) \bigm| T \in B[2]\bigr\}$$

is $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable. It follows that the abelian variety

$$G = \bigl((A \times B)/H\bigr) \times B$$

is defined over $\mathbb{Q}$. We claim that $G[2](\mathbb{Q})$ is zero. Since B has no torsion over $\mathbb{Q}$, it suffices to show that $(A \times B)/H$ has no 2-torsion over $\mathbb{Q}$. Over $\mathbb{Q}(\sqrt{2})$, we have

$$\begin{aligned}(A \times B)/H = (A \times B)/\bigl\{(\theta T, T)\bigr\} &\simeq (B \times B)/\bigl\{(T, T)\bigr\}\\ &\simeq (B \times B)/\bigl\{(T, 0)\bigr\} \simeq B/B[2] \times B \simeq B \times B.\end{aligned}$$

Since $B[2](\mathbb{Q}(\sqrt{2})) = \{0\}$, it follows that $(A \times B)/H$ has no 2-torsion over $\mathbb{Q}$.

The point $R = (-1, 2)$ in $B(\mathbb{Q})$ has infinite order. Define the following points in $G(\mathbb{Q})$:

$$P = \bigl(\bigl[(0, R)\bigr], 0\bigr); \qquad Q = \bigl(\bigl[(0, 0)\bigr], R\bigr).$$

The two points belong to the abelian subvariety $(\{0\} \times B)/H \times B \simeq B \times B$. The isomorphism which switches the two factors maps P to Q. In particular, the points P and Q satisfy Condition (SP).

We now prove that the above points provide a counterexample to Question 1.1. Since $G[2](\mathbb{Q})$ is zero, it suffices to show that if $\phi(P) = cQ$ for some ϕ in $\operatorname{End}_{\mathbb{Q}}(G)$ and $c \in \mathbb{Z}$, then c must be even.

Let Φ be the composition

$$\begin{tikzcd} A \times B \arrow[r, "\pi"] & (A \times B)/H \arrow[r, hook, "\iota"] & G \arrow[r, "\phi"] & G \arrow[r, "\pi_B"] & B \end{tikzcd}$$

where π is the quotient map, ι is the inclusion and π_B is the projection of G onto its direct factor B.

Having $\Phi : A \times B \to B$ is equivalent to having Φ_A in $\operatorname{Hom}_{\mathbb{Q}}(A, B)$ and Φ_B in $\operatorname{End}_{\mathbb{Q}}(B)$. We know that Φ_A is zero since A and B are not $\mathbb{Q}$-isogenous. Since $\phi(P) = cQ$, we deduce that $\Phi_B(R) = cR$; hence Φ_B is the multiplication by c. Let $(\theta T, T)$ be a non-zero element of H. Notice that the order of θT equals the order of T. If c is odd, we have a contradiction:

$$0 = \Phi_A(\theta T) = \Phi(\theta T, 0) = \Phi(0, -T) = \Phi_B(-T) = -cT \neq 0.$$

6.3. The support problem for tori

Let G be a torus defined over a number field K and let P and Q be points in $G(K)$ satisfying Condition (SP). The support problem asks whether there exists a K-endomorphism of G mapping P to Q.

If G is one-dimensional then $\phi(P) = Q$ for some ϕ in $\mathrm{End}_K(G)$, as follows from a result by Khare [5, Propostion 3]. The second author proved in [13, Proposition 12] that if G is split then $\phi(P) = Q$ for some ϕ in $\mathrm{End}_K(G)$. Furthermore, she proved that in general $\phi(P) = dQ$ for some ϕ in $\mathrm{End}_K(G)$, where d is the degree of the smallest Galois extension of K splitting the torus [13, Lemma 2 and Proposition 12]. We now answer in the negative the question of the support problem for tori.

Let T be any torus satisfying the following property: the intersection $T_a \cap T_d$ of the maximal anisotropic subtorus with the maximal split subtorus is non-trivial (this intersection is always finite, see [2, Chapter III, Section 8.15, Proposition]). Let R be a point in $T_d(K)$ which is independent: this amounts to choosing some multiplicatively independent elements in K^*. Then a counterexample is given by:

$$G = T \times T_d; \qquad P = (R, 0); \qquad Q = (0, R).$$

It is clear that the points P and Q satisfy Condition (SP). By [13, Main Theorem], we have $\phi(P) = cQ$ for some minimal positive integer c and for some ϕ in $\mathrm{End}_K(G)$. Let Φ be the composition

$$\begin{tikzcd} T \arrow[r, hook, "\iota"] & G \arrow[r, "\phi"] & G \arrow[r, "\pi"] & T_d \end{tikzcd}$$

where ι is the inclusion and π is the projection of G onto T_d. Since $\Phi(R) = cR$ and R is independent in T_d, the restriction of Φ to T_d is the multiplication by c. Because $\mathrm{Hom}_K(T_a, T_d)$ is zero [2, Chapter III, Section 8.15, Proposition], the restriction of Φ to T_a is zero. We deduce that the points in $(T_a \cap T_d)(\bar{K})$ are killed by the multiplication by c. So c must be a multiple of the exponent of the group $(T_a \cap T_d)(\bar{K})$ and in particular it is not 1.

Since c divides the degree of the smallest Galois extension of K splitting the torus [13, Lemma 2 and Proposition 12], we also provided an alternative proof of the following: for every torus T defined over a number field K, the exponent of $(T_a \cap T_d)(\bar{K})$ divides the degree of the smallest Galois extension of K where T splits.

Acknowledgments

The authors would like to thank Jan Van Geel for giving very helpful advice concerning the theory of maximal orders and Marc Hindry for useful explanations and comments. The authors are also indebted to Arno Fehm for providing a proof of Proposition 3.2, which permitted to get rid of a technical condition in the main result.

Appendix A

In this appendix, we construct an abelian variety for the counterexample in Section 6.1.

Let ζ_7 be a primitive seventh root of unity and consider $\tau := \zeta_7 + \zeta_7^{-1}$. The minimal polynomial of τ is $x^3 + x^2 - 2x - 1$. The number field $\mathbb{Q}(\tau)$ is totally real and Galois with ring of integers $\mathbb{Z}[\tau]$. The ring $R := \mathbb{Z}[2\tau, 2\tau^2]$ is a non-maximal order in $\mathbb{Q}(\tau)$. Let $\mathfrak{m} := (2, 2\tau, 2\tau^2)$ be a maximal ideal in R with residue field $\mathbb{F}_2$.

Theorem A.1. *There exist a number field K and an abelian variety A defined over K which is absolutely simple of dimension* 6, *with $\mathrm{End}_{\bar{K}}(A) = R$ and such that $A[2] \simeq (R/2R)^2 \times (R/\mathfrak{m})^6$ as R-modules.*

The outline of the construction is the following: We define a lattice Λ in $\mathbb{C}^6$, by which we mean a discrete subgroup of $\mathbb{C}^6$ of rank 12. We show that the complex torus $\mathcal{A} := \mathbb{C}^6/\Lambda$ is an abelian variety by exhibiting a positive definite hermitian form on $\mathbb{C}^6$ whose imaginary part takes integer values on $\Lambda \times \Lambda$. We check that $\mathrm{End}_{\mathbb{C}}(\mathcal{A})$ is R and that $\mathcal{A}[2] \simeq (R/2R)^2 \times (R/\mathfrak{m})^6$ as R-modules. We conclude by applying a result on the specialization of abelian varieties.

Proof of Theorem A.1. Consider the following matrices, where $\mathbf{0}_3$ denotes the zero matrix of dimension 3 by 3:

$$M = \begin{pmatrix} 0 & 0 & 1 & & & \\ 1 & 0 & 2 & & \mathbf{0}_3 & \\ 0 & 1 & -1 & & & \\ & & & 0 & 0 & 1 \\ & \mathbf{0}_3 & & 1 & 0 & 2 \\ & & & 0 & 1 & -1 \end{pmatrix}; \qquad X = \begin{pmatrix} 2 & -1 & 2 & & & \\ -1 & 2 & -2 & & \mathbf{0}_3 & \\ 2 & -2 & 5 & & & \\ & & & 2 & -1 & 2 \\ & \mathbf{0}_3 & & -1 & 2 & -2 \\ & & & 2 & -2 & 5 \end{pmatrix}.$$

These matrices satisfy $XM = M^T X$. The minimal polynomial of M is $x^3 + x^2 - 2x - 1$. This implies that $\mathbb{Z}[M] = \{a_0 I_6 + a_1 M + a_2 M^2 \mid a_0, a_1, a_2 \in \mathbb{Z}\}$ is a commutative integral domain isomorphic to $\mathbb{Z}[\tau]$. The characteristic polynomial of X is $(x-1)^4(x-7)^2$ so in particular X is positive definite.

For $i = 1, \dots, 6$ we call $\mathbf{e}_i$ the column vector that has only one non-zero entry, located at the i-th row and of value 1. Notice that we have

$$\mathbf{e}_2 = M\mathbf{e}_1; \qquad \mathbf{e}_3 = M^2\mathbf{e}_1; \qquad \mathbf{e}_5 = M\mathbf{e}_4; \qquad \mathbf{e}_6 = M^2\mathbf{e}_4.$$

Let $\alpha_1, \dots, \alpha_9$ be real numbers such that $\{1, \alpha_1, \dots, \alpha_9\}$ is a $\mathbb{Q}$-linearly independent set. Let ω be a positive real number such that ω^2 is not equal to $f(\alpha_1, \dots, \alpha_9)$ for any polynomial $f \in \mathbb{Q}[x_1, \dots, x_9]$ of degree at most 2. Write

$$\mathbf{r} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \end{pmatrix}; \qquad \mathbf{s} = \begin{pmatrix} \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \\ \alpha_8 \\ \alpha_9 \end{pmatrix}$$

and define

$$\begin{aligned} \mathbf{e}_7 &= \mathbf{r} + (\omega \mathrm{i})\mathbf{e}_1; & \mathbf{e}_{10} &= \mathbf{s} + (\omega \mathrm{i})\mathbf{e}_4; \\ \mathbf{e}_8 &= 2M\mathbf{e}_7 = 2M\mathbf{r} + (2\omega \mathrm{i})\mathbf{e}_2; & \mathbf{e}_{11} &= 2M\mathbf{e}_{10} = 2M\mathbf{s} + (2\omega \mathrm{i})\mathbf{e}_5; \\ \mathbf{e}_9 &= 2M^2\mathbf{e}_7 = 2M^2\mathbf{r} + (2\omega \mathrm{i})\mathbf{e}_3; & \mathbf{e}_{12} &= 2M^2\mathbf{e}_{10} = 2M^2\mathbf{s} + (2\omega \mathrm{i})\mathbf{e}_6. \end{aligned}$$

By the choice of the α_i's and of ω, the vectors $\mathbf{e}_1, \dots, \mathbf{e}_{12}$ are $\mathbb{R}$-linearly independent. We define Λ to be the $\mathbb{Z}$-span of $\{\mathbf{e}_1, \dots, \mathbf{e}_{12}\}$ inside $\mathbb{C}^6$.

Consider the following positive definite hermitian form on $\mathbb{C}^6$:

$$H(\mathbf{x}, \mathbf{y}) = \left(\bar{\mathbf{x}}^T X \mathbf{y}\right)\omega^{-1}.$$

Let E be the imaginary part of H, which is an $\mathbb{R}$-bilinear alternating form on $\mathbb{C}^6$. Since $XM = M^T X$, we have $E(M\mathbf{x}, \mathbf{y}) = E(\mathbf{x}, M\mathbf{y})$. Using this property, one can easily check that $E(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}$ for all $\mathbf{x}$ and $\mathbf{y}$ in Λ. Thus the complex torus $\mathcal{A} := \mathbb{C}^6/\Lambda$ is an abelian variety of dimension 6 [11, Corollary, p. 35].

We can write $\Lambda = \mathbb{Z}^6 + \Omega\mathbb{Z}^6$, where $\Omega = (\mathbf{e}_7|\mathbf{e}_8|\mathbf{e}_9|\mathbf{e}_{10}|\mathbf{e}_{11}|\mathbf{e}_{12})$. The imaginary part of Ω is

$$\Im(\Omega) = (\mathbf{e}_1|2\mathbf{e}_2|2\mathbf{e}_3|\mathbf{e}_4|2\mathbf{e}_5|2\mathbf{e}_6)\omega.$$

The real part $\Re(\Omega)$ is a matrix whose entries are linear combinations of the α_i's.

The $\mathbb{C}$-endomorphisms of $\mathcal{A}$ are the $\mathbb{C}$-linear maps $\sigma : \mathbb{C}^6 \to \mathbb{C}^6$ such that $\sigma(\Lambda) \subseteq \Lambda$. Let S be a 6×6 matrix over $\mathbb{C}$ defining an endomorphism. We first show that S has integer coefficients, and then that it belongs to $\mathbb{Z}[2M, 2M^2]$.

Since S maps $\mathbf{e}_1, \dots, \mathbf{e}_6$ into Λ, there exist two 6×6 matrices A_1 and A_2 with coefficients in $\mathbb{Z}$ such that $S = A_1 + \Omega A_2$. Similarly, $\mathbf{e}_7, \dots, \mathbf{e}_{12}$ get mapped into Λ so we have integer matrices B_1 and B_2 such that $S\Omega = B_1 + \Omega B_2$. By equating the two ways of writing $S\Omega$, we get

$$\Omega A_2 \Omega + (A_1 \Omega - \Omega B_2) - B_1 = 0.$$

Taking the real part of the above equation yields:

$$\begin{aligned}
&\Re(\Omega) A_2 \Re(\Omega) + \big(A_1 \Re(\Omega) - \Re(\Omega) B_2\big) - B_1 \\
&\quad = \Im(\Omega) A_2 \Im(\Omega) \\
&\quad = (\mathbf{e}_1 | 2\mathbf{e}_2 | 2\mathbf{e}_3 | \mathbf{e}_4 | 2\mathbf{e}_5 | 2\mathbf{e}_6) A_2 (\mathbf{e}_1 | 2\mathbf{e}_2 | 2\mathbf{e}_3 | \mathbf{e}_4 | 2\mathbf{e}_5 | 2\mathbf{e}_6) \omega^2.
\end{aligned}$$

The assumption on ω^2 then implies that $A_2 = 0$. Hence S is a matrix with integer coefficients.

Since S maps $\mathbf{e}_7$ into Λ, there exist $c_1, \dots, c_{12} \in \mathbb{Z}$ such that $S\mathbf{e}_7 = \sum_{i=1}^{12} c_i \mathbf{e}_i$. Define

$$\begin{aligned}
C_1 &:= c_1 \mathrm{I}_6 + c_2 M + c_3 M^2; & C_4 &:= c_4 \mathrm{I}_6 + c_5 M + c_6 M^2; \\
C_7 &:= c_7 \mathrm{I}_6 + 2c_8 M + 2c_9 M^2; & C_{10} &:= c_{10} \mathrm{I}_6 + 2c_{11} M + 2c_{12} M^2.
\end{aligned}$$

Then we have

$$S\mathbf{e}_7 = C_1 \mathbf{e}_1 + C_4 \mathbf{e}_4 + C_7 \mathbf{e}_7 + C_{10} \mathbf{e}_{10}.$$

The entries of $\Re(S\mathbf{e}_7)$ and of $\Re(C_7 \mathbf{e}_7 + C_{10} \mathbf{e}_{10})$ are linear combinations of $\alpha_1, \dots, \alpha_9$. Thus the entries of $(C_1 \mathbf{e}_1 + C_4 \mathbf{e}_4)$, which are integers, must be all zero. So we have $\Re((S - C_7)\mathbf{e}_7) = \Re(C_{10} \mathbf{e}_{10})$. By looking at the sixth entry, we get that a linear combination of $\alpha_1, \dots, \alpha_6$ is equal to

$$2c_{12}\alpha_7 + (2c_{11} - 2c_{12})\alpha_8 + (c_{10} + 2c_{11} + 6c_{12})\alpha_9.$$

By the independence of the α_i's, we deduce that $c_{10} = c_{11} = c_{12} = 0$; hence $C_{10} = 0$. So we have $S\mathbf{e}_7 = C_7 \mathbf{e}_7$. Again by the independence of the α_i's, we deduce that $S = C_7$. This means that S belongs to $\mathbb{Z}[2M, 2M^2]$.

It can easily be checked that every element in $\mathbb{Z}[2M, 2M^2]$ defines an endomorphism of $\mathcal{A}$. Since $\mathbb{Z}[2M, 2M^2] \simeq \mathbb{Z}[2\tau, 2\tau^2]$ as rings, we conclude that $\mathrm{End}_{\mathbb{C}}(\mathcal{A}) = R$.

We now study the action of $\mathrm{End}_{\mathbb{C}}(\mathcal{A})$ on $\mathcal{A}[2]$. Define $T_i := \mathbf{e}_i/2 + \Lambda$ for all $i = 1, \dots, 12$. Since $\mathcal{A}[2] = (\frac{1}{2}\Lambda)/\Lambda$, it is clear that

$$\mathcal{A}[2] \simeq \bigoplus_{i=1}^{12} (\mathbb{Z}/2\mathbb{Z}) T_i.$$

For all $i = 1, \dots, 6$, we have $2MT_i = 0$ and also $2M^2 T_i = 0$. It follows that $(\mathbb{Z}/2\mathbb{Z})T_i$ is an R-module isomorphic to $R/\mathfrak{m}$. On the other hand, we have $2MT_7 = T_8$ and $2M^2 T_7 = T_9$. This implies that $\bigoplus_{i=7}^{9} (\mathbb{Z}/2\mathbb{Z}) T_i$ is an R-module isomorphic to $R/2R$. Similarly for $\bigoplus_{i=10}^{12} (\mathbb{Z}/2\mathbb{Z}) T_i$.

Let $F = \mathbb{Q}(z_1, \dots, z_s)$ be a finitely generated subfield of $\mathbb{C}$ such that $\mathcal{A}$ is defined over F, all 2-torsion points of $\mathcal{A}$ are F-rational and $\mathrm{End}_F(\mathcal{A}) = \mathrm{End}_{\mathbb{C}}(\mathcal{A})$. Call k the relative algebraic closure of $\mathbb{Q}$ in F, which is a number field. Choose an affine variety V over k whose function field is F. We can specialize $\mathcal{A}$ with respect to the $\bar{k}$-points of V. After replacing V by an open affine subvariety, we may assume that the specialization is injective on the finite set $\mathcal{A}[2]$ and that the dimension of the specialized variety is $\dim_{\mathbb{C}} \mathcal{A} = 6$. By [10, Theorem, Section 1] there exists a specialization A of $\mathcal{A}$ which is an abelian variety over a number field $K \supseteq k$ such that $\mathrm{End}_{\bar{K}}(A) = \mathrm{End}_{\mathbb{C}}(\mathcal{A}) = R$. Since $\mathcal{A}[2]$ is mapped injectively into $A[2]$, they are isomorphic as R-modules. Finally, A is absolutely simple by the Poincaré Reducibility Theorem because R has no zero divisors. □

References

[1] F.A. Bogomolov, Sur l'algébricité des représentations l-adiques, C. R. Acad. Sci. Paris Sér. A–B 290 (15) (1980) A701–A703.

[2] Armand Borel, Linear Algebraic Groups, second ed., Grad. Texts in Math., vol. 126, Springer-Verlag, 1991.

[3] Gerhard Frey, Moshe Jarden, Approximation theory and the rank of abelian varieties over large algebraic fields, Proc. Lond. Math. Soc. (3) 28 (1974) 112–128.

[4] Marc Hindry, Joseph Silverman, Diophantine Geometry, Grad. Texts in Math., vol. 201, Springer-Verlag, New York, 2000.

[5] C. Khare, Compatible systems of mod p Galois representations and Hecke characters, Math. Res. Lett. 10 (1) (2003) 71–83.

[6] C. Khare, D. Prasad, Reduction of homomorphisms mod p and algebraicity, J. Number Theory 105 (2) (2004) 322–332.

[7] Michael Larsen, The support problem for abelian varieties, J. Number Theory 101 (2) (2003) 398–403.

[8] Michael Larsen, René Schoof, Whitehead's lemma and Galois cohomology of abelian varieties, http://mlarsen.math.indiana.edu/~larsen/unpublished.html, 2004.

[9] Michael Larsen, René Schoof, A refined counter-example to the support conjecture for abelian varieties, J. Number Theory 116 (2) (2006) 396–398.

[10] D.W. Masser, Specializations of endomorphism rings of abelian varieties, Bull. Soc. Math. France 124 (3) (1996) 457–476.

[11] David Mumford, Abelian Varieties, Oxford University Press, 1970.

[12] Antonella Perucca, Prescribing valuations of the order of a point in the reductions of abelian varieties and tori, J. Number Theory 129 (2) (2009) 469–476.

[13] Antonella Perucca, Two variants of the support problem for products of abelian varieties and tori, J. Number Theory 129 (8) (2009) 1883–1892.

[14] Irving Reiner, Maximal Orders, London Math. Soc. Monogr. (N. S.), vol. 28, Oxford University Press, 2003.