ACTA ARITHMETICA
110.1 (2003)

Kummer theory of abelian varieties and reductions of Mordell–Weil groups

by

TOM WESTON (Berkeley, CA)

Let A be an abelian variety over a number field F. We write $\mathrm{red}_v : A(F) \to A(k_v)$ for the reduction map at a place v of F with residue field k_v. W. Gajda has posed the following question.

QUESTION. *Let Σ be a subgroup of $A(F)$. Suppose that x is a point of $A(F)$ such that $\mathrm{red}_v x$ lies in $\mathrm{red}_v \Sigma$ for almost all places v of F. Does it then follow that x lies in Σ?*

In this paper we use methods of Kummer theory to provide the following partial answer to this question.

THEOREM. *Let A be an abelian variety over a number field F and assume that $\mathrm{End}_F A$ is commutative. Let Σ be a subgroup of $A(F)$ and suppose that $x \in A(F)$ is such that $\mathrm{red}_v x \in \mathrm{red}_v \Sigma$ for almost all places v of F. Then $x \in \Sigma + A(F)_{\mathrm{tors}}$.*

It does not appear that the torsion ambiguity can be eliminated with our present approach, and it is not clear to the author how to modify the arguments for the non-commutative case. We note that our theorem applies in particular to products of non-isogenous elliptic curves.

Gajda's question has its origins in the support problem of P. Erdős: if x and y are positive integers such that for any $n \geq 1$ the set of primes dividing $x^n - 1$ is the same as the set of primes dividing $y^n - 1$, then must x equal y? Corrales-Rodrigáñez and Schoof gave an affirmative answer to this question in [3] and also answered the corresponding question for elliptic curves; this was generalized by Banaszak, Gajda and Krasoń in [1] to certain abelian varieties with complex or real multiplication and $\mathrm{End}_F A$ a commutative maximal order. Recently Larsen [7] has given a proof of the support problem for arbitrary abelian varieties; see also [6] for results of Kowalski on a closely

2000 *Mathematics Subject Classification*: 11G10, 14K15, 13F05.
Partially supported by an NSF postdoctoral fellowship.

related question. In this context the support problem takes the following form.

QUESTION. *Let $x, y \in A(F)$ be non-torsion points. Suppose that the order of* $\mathrm{red}_v x$ *divides the order of* $\mathrm{red}_v y$ *for almost all places v of F. Does it follow that x and y satisfy an* $\mathrm{End}_F A$*-linear relation in $A(F)$?*

If we take $\Sigma = \mathrm{End}_F A \cdot y$, the support problem implies a weak form of our main theorem in the case when Σ is a cyclic $\mathrm{End}_F A$-module. The more precise question of Gajda we consider is one possible modification of the support problem for abelian varieties to a non-cyclic setting. The approach we use here is quite different from that of [3] and [1], relying more on the study of the Mordell–Weil group of A as a module for $\mathrm{End}_F A$ and less on Galois cohomology.

We now give an overview of our argument in the simplest case. Assume that A is simple, that $\mathcal{O} := \mathrm{End}_F A$ is integrally closed (so that it is a Dedekind domain), and that $A(F)$ is a free $\mathcal{O}$-module. With $\Sigma \subseteq A(F)$ and $x \in A(F)$ as in the theorem, it suffices to prove that $x \in \Sigma \otimes \mathbb{Z}_{(p)}$ for every prime p (with $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ away from p). Fix, then, a prime p and suppose that $x \notin \Sigma \otimes \mathbb{Z}_{(p)}$. The first step, which is purely algebraic, is to show that under this assumption one can choose an $\mathcal{O}$-basis $y_1, \ldots, y_r$ of $A(F)$ such that $\psi_1(x) \notin \psi_1(\Sigma) + p^a\mathcal{O}$ for some $a > 0$; here $\psi_1 : A(F) \to \mathcal{O}$ is the projection onto the y_1-coordinate.

The next step is to choose an appropriate place v of F. We work instead over the extensions $F(A[p^n])$ of F. Using Kummer theory and the Chebotarev density theorem, we show that there is a $b > 0$ such that for any sufficiently large n there is a place w of $F(A[p^n])$ with $\mathrm{red}_w y_2, \ldots, \mathrm{red}_w y_r \in p^n A(k_w)$, while $\mathrm{red}_w y_1 \notin \mathfrak{p}_i^b A(k_w)$ for any i; here $p\mathcal{O} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ is the ideal factorization of p in $\mathcal{O}$.

Fix $n \geq a+b$ and choose such a place w. By hypothesis we have $\mathrm{red}_w x = \mathrm{red}_w y$ for some $y \in \Sigma$. If we expand in terms of our chosen basis of $A(F)$, the choice of w implies that

$$(\psi_1(x) - \psi_1(y))\,\mathrm{red}_w y_1 \in p^n A(k_w).$$

On the other hand, using the properties of ψ_1 and of w, one can show directly that

$$(\psi_1(x) - \psi_1(y))\,\mathrm{red}_w y_1 \notin p^{a+b} A(k_w).$$

As $n \geq a+b$, we have a contradiction, so that we must have had $x \in \Sigma \otimes \mathbb{Z}_{(p)}$. This completes our sketch of the argument in this case.

We now review the contents of this paper in more detail. We begin in Section 1.1 with a review of Kummer theory and in Section 1.2 we adapt the methods of Bashmakov–Ribet as in [9] to prove that the cokernel of the p-adic Kummer map is bounded. In Section 1.3 we discuss the relation between Kummer theory and reduction maps.

In the sketch above we assumed that $\mathcal{O}$ was an integrally closed domain and that $A(F)$ was free over $\mathcal{O}$. The algebra required to eliminate these assumptions is developed in Section 2. These results are combined with Kummer theory to produce places w as above in Section 3.1, and the proof of our main theorem is given in Section 3.2.

The author wishes to thank Ken Ribet for suggesting this problem, Mark Dickinson for helpful conversations, and the referee for several corrections.

1. Kummer theory

1.1. *Review of Kummer theory.* Let A be an abelian variety over a number field F; set $\mathcal{O} = \mathrm{End}_F A$. For $\alpha \in \mathcal{O}$ we set $F_\alpha = F(A[\alpha])$ and $G_\alpha = \mathrm{Gal}(F_\alpha/F)$. The *Kummer map*

$$\kappa_\alpha : A(F)/\alpha \to \mathrm{Hom}_{G_\alpha}(\mathrm{Gal}(\overline{F}/F_\alpha), A[\alpha])$$

is defined as the composition

$$A(F)/\alpha \hookrightarrow H^1(F, A[\alpha]) \xrightarrow{\text{res}} H^1(F_\alpha, A[\alpha])^{G_\alpha}$$

with the first map a coboundary map for the $\mathrm{Gal}(\overline{F}/F)$-cohomology of the Kummer sequence

$$0 \to A[\alpha] \to A(\overline{F}) \xrightarrow{\alpha} A(\overline{F}) \to 0$$

and the second map restriction to F_α. (Concretely, for $x \in A(F)$, $\kappa_\alpha(x)$ is the homomorphism sending $\gamma \in \mathrm{Gal}(\overline{F}/F_\alpha)$ to $\gamma\big(\frac{x}{\alpha}\big) - \frac{x}{\alpha} \in A[\alpha]$ where $\frac{x}{\alpha}$ is some fixed αth root of x in $A(\overline{F})$.)

If Γ is an $\mathcal{O}$-submodule of $A(F)$ and $\alpha \in \mathcal{O}$, we write $F_\alpha\big(\frac{1}{\alpha}\Gamma\big)$ for the extension of F_α generated by all αth roots of elements of Γ; alternately, $F_\alpha\big(\frac{1}{\alpha}\Gamma\big)$ is the fixed field of the intersection of the kernels of the homomorphisms $\kappa_\alpha(\Gamma)$. The Galois group $\mathfrak{g}_\alpha(\Gamma) := \mathrm{Gal}\,\big(F_\alpha\big(\frac{1}{\alpha}\Gamma\big)/F_\alpha\big)$ is an $\mathcal{O}[G_\alpha]$-module and κ_α restricts to an $\mathcal{O}$-linear map

$$\Gamma/\alpha \to \mathrm{Hom}_{G_\alpha}(\mathfrak{g}_\alpha(\Gamma), A[\alpha]).$$

We write the $\mathcal{O}[G_\alpha]$-dual of this map as

$$\lambda_\alpha^\Gamma : \mathfrak{g}_\alpha(\Gamma) \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\Gamma, A[\alpha]).$$

1.2. *p-adic Kummer theory.* Fix a rational prime p; set $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$ and $K_p = \mathcal{O} \otimes \mathbb{Q}_p$. The Tate module $T_pA := \varprojlim A[p^n]$ (resp. Tate space $V_pA := T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$) is naturally an $\mathcal{O}_p[G_{p^\infty}]$-module (resp. $K_p[G_{p^\infty}]$-module) where $G_{p^\infty} = \mathrm{Gal}(F(A[p^\infty])/F)$. It follows from [8, Section 19, Corollary 2] that there is a decomposition

$$K_p = \prod M_{n_i} K_i \tag{1.1}$$

where $M_{n_i}K_i$ is the central simple algebra of $n_i \times n_i$-matrices over the division ring K_i. Corresponding to (1.1) is a decomposition $V_pA = \bigoplus V_iA^{n_i}$ of V_pA into $K_i[G_{p^\infty}]$-modules. By [5, Theorem 4], we have

$$\mathrm{End}_{\mathbb{Q}_p[G_{p^\infty}]} V_iA = K_i \tag{1.2}$$

for each i; in particular, each V_iA is an irreducible $K_i[G_{p^\infty}]$-module. We record a second immediate consequence of (1.2) in the next lemma.

Lemma 1.1. *Let Γ be an $\mathcal{O}$-module. Then the evaluation map*

$$\Gamma \otimes_{\mathcal{O}} K_i \to \mathrm{Hom}_{K_i[G_{p^\infty}]}(\mathrm{Hom}_{\mathcal{O}}(\Gamma, V_iA), V_iA)$$

is an isomorphism.

Fix an $\mathcal{O}$-submodule Γ of $A(F)$. The inverse limit $\mathfrak{g}_{p^\infty}(\Gamma)$ of the $\mathfrak{g}_{p^n}(\Gamma)$ is naturally an $\mathcal{O}_p[G_{p^\infty}]$-module endowed with an injection

$$\lambda^{\Gamma}_{p^\infty} : \mathfrak{g}_{p^\infty}(\Gamma) \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\Gamma, T_pA).$$

More generally, since $\mathcal{O}_p/p^n \cong \mathcal{O}/p^n$ for all n, for any $\mathcal{O}$-module $\Gamma \subseteq A(F)\otimes \mathbb{Z}_p$ we can still define $\mathfrak{g}_{p^n}(\Gamma)$ and $\lambda^{\Gamma}_{p^n}$ for $n \le \infty$. In any case, there is a $K_p[G_{p^\infty}]$-module decomposition

$$\mathfrak{g}_{p^\infty}(\Gamma) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \bigoplus \mathfrak{g}_i(\Gamma)^{n_i} \tag{1.3}$$

(with n_i as in (1.1)) into $K_i[G_{p^\infty}]$-modules, and there are natural injections

$$\lambda^{\Gamma}_i : \mathfrak{g}_i(\Gamma) \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\Gamma, V_iA).$$

The decomposition (1.3) is functorial in the sense that there is a natural surjection $\mathfrak{g}_i(\Gamma) \twoheadrightarrow \mathfrak{g}_i(\Gamma')$ for any $\mathcal{O}$-submodule Γ' of Γ.

The main result of Kummer theory we need is the following. The proof is a straightforward adaptation of the methods of Bashmakov and Ribet.

Proposition 1.2. *Fix a rational prime p and let Γ be an $\mathcal{O}$-submodule of $A(F)$. Then the cokernel of $\lambda^{\Gamma}_{p^n}$ is bounded independent of n.*

Proof. First consider the cyclic case $\Gamma = \mathcal{O}\cdot x$ for $x \in A(F)$. If $\Gamma \cong \mathcal{O}$, then $\mathbb{Z}\cdot x$ is Zariski dense in A; the proposition thus follows from [2, Theorem 2] in this case. More generally, let A' denote the largest abelian subvariety of A, defined over F, in which $\mathbb{Z}\cdot x$ is Zariski dense; set $\mathcal{O}' = \mathrm{End}_F A'$. Using the Poincaré reducibility theorem (see [8, Section 19, Theorem 1]), one easily checks that

$$\mathrm{Hom}_{\mathcal{O}}(\Gamma, V_pA) \cong \mathrm{Hom}_{\mathcal{O}'}(\Gamma, V_pA'),$$

so that the general cyclic case follows from [2, Theorem 2] applied to A'. In fact, one has $\mathrm{coker}\, \lambda^{\mathcal{O}\cdot x}_{p^\infty} = \mathrm{coker}\, \lambda^{\mathcal{O}\cdot x'}_{p^\infty}$ whenever $x, x' \in A(F)$ are sufficiently p-adically congruent, so that the same arguments apply for arbitrary $x \in A(F)\otimes \mathbb{Z}_p$.

For general Γ it suffices to show that each of the injections λ_i^Γ is an isomorphism. Suppose, then, that some λ_i^Γ is not surjective. As $\mathrm{Hom}_{\mathcal{O}}(\Gamma, V_i A)$ is a direct sum of copies of the irreducible $K_i[G_{p^\infty}]$-module $V_i A$ (and thus in particular is a semisimple $K_i[G_{p^\infty}]$-module), it follows that there exists a $K_i[G_{p^\infty}]$-surjection

$$\varphi : \mathrm{Hom}_{\mathcal{O}}(\Gamma, V_i A) \twoheadrightarrow V_i A$$

annihilating $\mathfrak{g}_i(\Gamma)$. By Lemma 1.1 the map φ is given by evaluation at some $x \in \Gamma \otimes_{\mathcal{O}} K_i$; using the injection $K_i \hookrightarrow K_p$ and scaling φ if necessary, we may in fact assume that $x \in \Gamma \otimes \mathbb{Z}_p$. There is then a commutative diagram

$$\begin{array}{ccc} \mathfrak{g}_i(\Gamma) & \xhookrightarrow{\lambda_i^\Gamma} & \mathrm{Hom}_{\mathcal{O}}(\Gamma, V_i A) \\ \downarrow & & \downarrow \varphi \\ \mathfrak{g}_i(\mathcal{O} \cdot x) & \xhookrightarrow{\lambda_i^{\mathcal{O}\cdot x}} & V_i A \end{array}$$

The clockwise composition is zero by construction, so that we must have $\lambda_i^{\mathcal{O}\cdot x} = 0$ as well. By the cyclic case considered above this implies that x maps to zero in $\Gamma \otimes_{\mathcal{O}} K_i$. But then φ, which is evaluation at x, is also zero. This contradicts the surjectivity of φ and thus proves the proposition. ∎

1.3. *Reductions and Frobenius elements.* We write k_w for the residue field of a finite extension F' of F at a place w, and $\mathrm{red}_w : A(F') \to A(k_w)$ for the reduction map.

LEMMA 1.3. *Fix $\alpha \in \mathcal{O}$ and $x \in A(F)$. Let w be a finite place of F_α, relatively prime to α, at which A has good reduction. Then* $\mathrm{red}_w x$ *lies in* $\alpha A(k_w)$ *if and only if* $\lambda_\alpha^{\mathcal{O}\cdot x}(\mathrm{Frob}_w) = 0$, *where* $\mathrm{Frob}_w \in \mathrm{Gal}\big(F_\alpha\big(\frac{x}{\alpha}\big)/F_\alpha\big)$ *is the Frobenius element at w.*

Proof. Fix an αth root $\frac{x}{\alpha}$ of x in $A(\overline{F})$ and a place w' of $F_\alpha\big(\frac{x}{\alpha}\big)$ over w. If $\lambda_\alpha^{\mathcal{O}\cdot x}(\mathrm{Frob}_w) = 0$, then w' is completely split over w so that $k_{w'} = k_w$. In particular, $\mathrm{red}_{w'}\frac{x}{\alpha} \in A(k_{w'})$ lies in $A(k_w)$; thus $\mathrm{red}_w x \in \alpha A(k_w)$ as claimed.

Conversely, if there is $y \in A(k_w)$ with $\alpha y = \mathrm{red}_w x$, then $y - \mathrm{red}_{w'}\frac{x}{\alpha}$ lies in $A[\alpha]$. Since y and $A[\alpha]$ are both in $A(k_w)$ we conclude that $\mathrm{red}_{w'}\frac{x}{\alpha}$ is in $A(k_w)$ as well. In particular, we have

$$\mathrm{Frob}_w\big(\mathrm{red}_{w'}\tfrac{x}{\alpha}\big) - \mathrm{red}_{w'}\tfrac{x}{\alpha} = 0. \tag{1.4}$$

On the other hand, $\mathrm{Frob}_w\big(\frac{x}{\alpha}\big) - \frac{x}{\alpha}$ already lies in $A[\alpha]$, which injects into $A(k_{w'})$; (1.4) thus forces

$$\mathrm{Frob}_w\big(\tfrac{x}{\alpha}\big) - \tfrac{x}{\alpha} = 0 \quad \text{in } A(\overline{F}).$$

This says exactly that $\lambda_\alpha^{\mathcal{O}\cdot x}(\mathrm{Frob}_w) = 0$, as claimed. ∎

We assume now that $\mathcal{O}$ is commutative. Suppose that $\mathfrak{a}$ is an ideal of $\mathcal{O}$ such that $\beta\mathfrak{a} \subseteq \alpha\mathcal{O}$ for some $\alpha, \beta \in \mathcal{O}$. Multiplication by β then yields a map $A[\alpha] \to A[\mathfrak{a}]$.

LEMMA 1.4. *Let $\alpha, \beta, \mathfrak{a}$ be as above and fix $x \in A(F)$. Let w be a finite place of F_α, relatively prime to α, at which A has good reduction. If $\beta \cdot \lambda_\alpha^{\mathcal{O}\cdot x}(\mathrm{Frob}_w) \neq 0$, then $\mathrm{red}_w x \notin \mathfrak{a}A(k_w)$.*

Proof. We prove the contrapositive. Suppose that $\mathrm{red}_w x \in \mathfrak{a}A(k_w)$. Then

$$\beta\,\mathrm{red}_w x \in \beta\mathfrak{a}A(k_w) \subseteq \alpha A(k_w),$$

so that there is $y \in A(k_w)$ with $\beta\,\mathrm{red}_w x = \alpha y$. On the other hand, fixing an αth root $\frac{x}{\alpha}$ of x in $A(\overline{F})$ and a place w' of $F_\alpha\big(\frac{x}{\alpha}\big)$ lying above w, we also have $\beta\,\mathrm{red}_w x = \alpha\beta\,\mathrm{red}_{w'} \frac{x}{\alpha}$. Therefore

$$y - \beta\,\mathrm{red}_{w'} \tfrac{x}{\alpha} \in A[\alpha].$$

From here the argument proceeds as in the second half of the proof of Lemma 1.3 above to show that $\beta \cdot \lambda_\alpha^{\mathcal{O}\cdot x}(\mathrm{Frob}_w) = 0$. ∎

We remark that the converse of Lemma 1.4 holds in the case when $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{a}'$ with $\mathfrak{a}, \mathfrak{a}'$ relatively prime and $\beta \in \mathfrak{a}' \cap (1 - \mathfrak{a})$.

2. Modules over commutative, reduced, finite, flat $\mathbb{Z}$-algebras

2.1. *Projections.* Let $\mathcal{O}$ be a commutative, reduced, finite, flat $\mathbb{Z}$-algebra. The normalization $\widetilde{\mathcal{O}}$ of $\mathcal{O}$ decomposes as a product $\prod_{j=1}^h \widetilde{\mathcal{O}}_j$ of Dedekind domains. (See [4, Section 11.2], for example, for a discussion of the normalization of a reduced ring.) We say that a $\mathbb{Z}$-linear map $t : \mathcal{O} \to \mathbb{Z}$ is *full* if it is non-trivial on $\mathcal{O} \cap \widetilde{\mathcal{O}}_j$ for each j. Note that such a map always exists; indeed, this is clear for $\widetilde{\mathcal{O}}$ (simply take the sum of the trace maps $\widetilde{\mathcal{O}}_j \to \mathbb{Z}$), and multiplying a full map for $\widetilde{\mathcal{O}}$ by $[\widetilde{\mathcal{O}} : \mathcal{O}]$ yields a full map $\mathcal{O} \to \mathbb{Z}$.

LEMMA 2.1. *Fix a full map $t : \mathcal{O} \to \mathbb{Z}$. Then the map*

$$\mathrm{Hom}_{\mathcal{O}}(N, \mathcal{O}) \to \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z}), \qquad f \mapsto t \circ f \tag{2.1}$$

has finite cokernel for any finitely generated $\mathcal{O}$-module N.

Proof. Since $\mathcal{O}$ has finite index in $\widetilde{\mathcal{O}}$, it suffices to prove the result after replacing $\mathcal{O}$ by $\widetilde{\mathcal{O}}$ and N by $N \otimes_{\mathcal{O}} \widetilde{\mathcal{O}}$. We may therefore assume that $\mathcal{O}$ decomposes as a product $\prod \mathcal{O}_i$ of Dedekind domains. There is then a corresponding decomposition $N = \bigoplus N_i$, and by the definition of a full map it suffices to prove the lemma for each factor N_i; that is, we may assume that $\mathcal{O}$ is a Dedekind domain.

In this case every finitely generated $\mathcal{O}$-module has a free submodule of finite index; this allows one to reduce to the case when N is free, and then to the case when N is free of rank one. (2.1) is then a map

$$\mathcal{O} = \mathrm{Hom}_{\mathcal{O}}(\mathcal{O},\mathcal{O}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O},\mathbb{Z}) \tag{2.2}$$

between two free $\mathbb{Z}$-modules of the same rank, so that it suffices to prove that it is injective. For this, note that (2.2) is $\mathcal{O}$-linear; thus its kernel is an ideal of $\mathcal{O}$. However, every non-zero ideal of $\mathcal{O}$ has finite index and $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{O},\mathbb{Z})$ is torsion-free; therefore (2.2) must be either zero or injective. As t itself lies in the image, it is obviously non-zero. ∎

We now fix a finitely generated $\mathcal{O}$-module N and a $\mathbb{Z}$-submodule M of N containing the $\mathbb{Z}$-torsion submodule N_{tors} of N.

Lemma 2.2. *Fix $x \in N$ and suppose that p is a rational prime such that $x \notin M \otimes \mathbb{Z}_{(p)}$. Then there is an $\mathcal{O}$-linear map $\psi : N \to \mathcal{O}$ such that $\psi(x) \notin \psi(M) + p^n\mathcal{O}$ for sufficiently large n.*

Proof. Choose a $\mathbb{Z}$-basis $y_1,\dots,y_r \in N$ of N/N_{tors} such that there are integers $d_1,\dots,d_r$ with

$$M = \langle d_1y_1,\dots,d_ry_r\rangle \oplus N_{\mathrm{tors}}.$$

(Of course, some of the d_i may be zero.) Writing $x = a_1y_1 + \dots + a_ry_r + t$ with $a_i \in \mathbb{Z}$ and $t \in N_{\mathrm{tors}}$, the fact that $x \notin M \otimes \mathbb{Z}_{(p)}$ implies that there is some index i such that

$$\mathrm{ord}_p\, a_i < \mathrm{ord}_p\, d_i. \tag{2.3}$$

Let $\psi_0 : N \to \mathbb{Z}$ be $\#N_{\mathrm{tors}}$ times projection onto y_i; this is a well defined map, and it follows from (2.3) that $\psi_0(x) \notin \psi_0(M) + p^n\mathbb{Z}$ for sufficiently large n. (In fact, $n > \mathrm{ord}_p(a_i \cdot \#N_{\mathrm{tors}})$ suffices.)

Fix a full map $t : \mathcal{O} \to \mathbb{Z}$. By Lemma 2.1, we can find a non-zero integer b such that $b\psi_0$ is in the image of (2.1). Thus there is an $\mathcal{O}$-linear map $\psi : N \to \mathcal{O}$ with $b\psi_0 = t \circ \psi$. Since $t(p^n\mathcal{O}) \subseteq p^n\mathbb{Z}$, we conclude that $\psi(x) \notin \psi(M) + p^n\mathcal{O}$ for sufficiently large n, as desired. ∎

2.2. *Pre-bases.* We continue with $M \subseteq N$ as before. Fix $y \in N$ not in N_{tors} and let $\varphi : \mathcal{O} \twoheadrightarrow \mathcal{O}\cdot y$ be the $\mathcal{O}$-linear surjection sending 1 to y. We define $\eta_0(y)$ to be the least positive integer m such that there exists an $\mathcal{O}$-linear map $\psi : \mathcal{O}\cdot y \to \mathcal{O}$ with the composition

$$\mathcal{O}\cdot y \xrightarrow{\psi} \mathcal{O} \xrightarrow{\varphi} \mathcal{O}\cdot y$$

multiplication by m. (Let K_j denote the fraction field of $\widetilde{\mathcal{O}}_j$; since $\mathcal{O}\otimes\mathbb{Q} = \prod K_j$, to see that any maps ψ as above exist it suffices to prove the corresponding fact after replacing $\mathcal{O}$ by $\prod K_j$. In this context the map φ identifies with the quotient map

$$\prod K_j \to \prod_{j\in J} K_j$$

for some non-empty subset J of $\{1,\dots,h\}$, so that the existence of ψ is obvious.)

We say that $y_1,\dots,y_r \in N$ are an *$\mathcal{O}$-pre-basis* of N if:

- $y_i \notin N_{\mathrm{tors}}$ for all i;
- $(\mathcal{O}\cdot y_1)\oplus\ldots\oplus(\mathcal{O}\cdot y_r)$ injects into N with finite cokernel.

(Note that we do not require that the corresponding map $\mathcal{O}^r \to N$ is injective.) Let $\eta'(y_1,\dots,y_r)$ be the order of this cokernel and define

$$\eta(y_1,\dots,y_r)=\eta'(y_1,\dots,y_r)\cdot\eta_0(y_1)\ldots\eta_0(y_r).$$

It then follows from the definition of $\eta_0(y_i)$ that there are $\mathcal{O}$-linear maps

$$\psi_i^{y_1,\dots,y_r}: N\to\mathcal{O}$$

for $i=1,\dots,r$ such that

$$\eta(y_1,\dots,y_r)y=\psi_1^{y_1,\dots,y_r}(y)y_1+\ldots+\psi_r^{y_1,\dots,y_r}(y)y_r \tag{2.4}$$

for all $y\in N$. We usually just write η and ψ_i if the pre-basis $y_1,\dots,y_r$ is clear from context. A standard inductive procedure shows that pre-bases always exist.

PROPOSITION 2.3. *Fix $x\in N$ and suppose that p is a rational prime such that $x\notin M\otimes\mathbb{Z}_{(p)}$. Then there is an $\mathcal{O}$-pre-basis $y_1,\dots,y_r$ of N such that $\psi_1(x)\notin\psi_1(M)+p^n\mathcal{O}$ for sufficiently large n.*

Proof. By Lemma 2.2, we may choose an $\mathcal{O}$-linear map $\psi: N\to\mathcal{O}$ such that $\psi(x)\notin\psi(M)+p^n\mathcal{O}$ for sufficiently large n. Let K' denote the image of $\psi\otimes\mathbb{Q}$; we have $K'=\prod_{j\in J}K_j$ for some non-empty subset J of $\{1,\dots,h\}$. In particular, K' is a projective $\prod K_j$-module, so that there exists a map $\varphi_0: K'\to N\otimes\mathbb{Q}$ such that $(\psi\otimes\mathbb{Q})\circ\varphi_0$ is the identity on K'. Scaling φ_0 by an integer we obtain an $\mathcal{O}$-linear map $\varphi:\widetilde{\mathcal{O}}'\to N$ such that $\psi\circ\varphi$ is multiplication by some non-zero integer; here $\widetilde{\mathcal{O}}'=\prod_{j\in J}\widetilde{\mathcal{O}}_j$.

Set $y_1=\varphi(1)$ and choose an $\mathcal{O}$-pre-basis $y_2,\dots,y_r$ for $\ker\psi$. Then $y_1,\dots,y_r$ is an $\mathcal{O}$-pre-basis of N and $\psi_1=m\psi$ for some non-zero integer m. It thus follows from the definition of ψ that $\psi_1(x)\notin\psi_1(M)+p^n\mathcal{O}$ for sufficiently large n, as desired. ∎

2.3. *Ideals.* We continue with $\mathcal{O}$ as above. Fix a rational prime p and write the $\mathbb{Z}$-exponent of $\widetilde{\mathcal{O}}/\mathcal{O}$ as cp^d with $d\geq 0$ and c relatively prime to p. Let

$$p\widetilde{\mathcal{O}}=\widetilde{\mathfrak{p}}_1^{e_1}\ldots\widetilde{\mathfrak{p}}_g^{e_g}$$

be the factorization of $p\widetilde{\mathcal{O}}$ into prime ideals of $\widetilde{\mathcal{O}}$; for each $i\in\{1,\dots,g\}$ we let $\mu_p(i)$ denote the unique $j\in\{1,\dots,h\}$ such that $\widetilde{\mathfrak{p}}_i$ is the pullback of a prime ideal on $\widetilde{\mathcal{O}}_j$. For $y\in N$ we define $I_p(y)\subseteq\{1,\dots,g\}$ to be the set of indices i such that the image of y in $N\otimes_{\mathcal{O}}\widetilde{\mathcal{O}}_{\widetilde{\mathfrak{p}}_i}$ is non-torsion. In fact, since every proper ideal of each $\widetilde{\mathcal{O}}_j$ has finite index, we have

$$I_p(y) = \{i;\ \mathrm{rank}_{\mathbb{Z}}((\mathcal{O} \cap \widetilde{\mathcal{O}}_{\mu_p(i)}) \cdot y) > 0\}. \tag{2.5}$$

For $i = 1, \ldots, g$ and any n, we define ideals of $\mathcal{O}$ by

$$\mathfrak{p}_{i,n} = \widetilde{\mathfrak{p}}_i^{e_i n} \cap \mathcal{O}.$$

The reader is invited to focus on the case $d = 0$, when $\mathfrak{p}_{i,n} = \mathfrak{p}_{i,1}^n$ and the analysis below is quite a bit simpler. In the general case, we have $cp^d \widetilde{\mathfrak{p}}_i^{e_i n} \subseteq \mathfrak{p}_{i,n}$; since the $\widetilde{\mathfrak{p}}_i$ are relatively prime, it follows that

$$c^{g-1} p^{d(g-1)} \mathcal{O} \subseteq \mathfrak{p}_{i,n} + \prod_{j \neq i} \mathfrak{p}_{j,n} \tag{2.6}$$

for all n. Furthermore, $p^n \widetilde{\mathcal{O}} \cap \mathcal{O} \subseteq p^{n-d} \mathcal{O}$ for $n \geq d$, so that

$$p^n \mathcal{O} \subseteq \mathfrak{p}_{1,n} \cap \ldots \cap \mathfrak{p}_{g,n} \subseteq p^{n-d} \mathcal{O}, \tag{2.7}$$

$$c^g p^{n+dg} \mathcal{O} \subseteq \mathfrak{p}_{1,n} \cdots \mathfrak{p}_{g,n} \subseteq p^{n-d} \mathcal{O} \tag{2.8}$$

for any $n \geq d$.

LEMMA 2.4. *Let N be a finitely generated $\mathcal{O}$-module. Fix $\alpha \in \mathcal{O}$ and $x \in N$. Suppose that there is an index i and non-negative integers a, b such that*:

(1) $\alpha \notin \mathfrak{p}_{i,a}$;
(2) $x \notin \mathfrak{p}_{i,b} N$;
(3) $N[p^{a+d}] \subseteq p^b N$.

Then $\alpha x \notin p^{a+b+d} N$.

Proof. We first replace $\mathcal{O}$ by $\varprojlim \mathcal{O}/\mathfrak{p}_{i,n}$, N by $\varprojlim N/\mathfrak{p}_{i,n}$, and $\widetilde{\mathcal{O}}$ by $\varprojlim \widetilde{\mathcal{O}}/\widetilde{\mathfrak{p}}_i^n$. Let $\widetilde{\mathfrak{p}}$ denote the maximal ideal of $\widetilde{\mathcal{O}}$, so that $\widetilde{\mathfrak{p}}^{e_i} = p\widetilde{\mathcal{O}}$, and set $\mathfrak{p}_n = \widetilde{\mathfrak{p}}^{e_i n} \cap \mathcal{O}$. With this notation we have $\alpha \notin \mathfrak{p}_a$ and $x \notin \mathfrak{p}_b N$, and it suffices to prove that $\alpha x \notin p^{a+b+d} N$. Note that $\alpha \notin \widetilde{\mathfrak{p}}^{e_i a}$, so that there is some $\beta \in \widetilde{\mathcal{O}}$ with $\alpha\beta = p^a$.

Set $C = \widetilde{\mathcal{O}}/\mathcal{O}$ and $\widetilde{N} = N \otimes_{\mathcal{O}} \widetilde{\mathcal{O}}$; C is killed by p^d and there is an exact sequence

$$\mathrm{Tor}_1^{\mathcal{O}}(N, C) \to N \xrightarrow{\iota} \widetilde{N} \to N \otimes_{\mathcal{O}} C \to 0. \tag{2.9}$$

Suppose now that $\alpha x \in p^{a+b+d} N$. Applying ι and multiplying by β, we find that $p^a \iota(x) \in p^{a+b+d} \widetilde{N}$. By (2.9) we have $p^d \widetilde{N} \subseteq \iota(N)$, so that this implies that $p^a x - p^{a+b} n \in \ker \iota$ for some $n \in N$. Again by (2.9) this kernel is killed by p^d; we conclude that

$$p^{a+d} x \in p^{a+b+d} N.$$

Thus

$$x \in p^b N + N[p^{a+d}] \subseteq p^b N \subseteq \mathfrak{p}_b N.$$

Since $x \notin \mathfrak{p}_b N$ by hypothesis, this yields the desired contradiction. ∎

3. Reductions of Mordell–Weil groups

3.1. *Galois elements.* Let A be an abelian variety over a number field F. By [8, Section 19, Corollary 2] the ring $\mathcal{O} := \mathrm{End}_F$ is a reduced, finite, flat $\mathbb{Z}$-algebra. We further assume that it is commutative; we fix a rational prime p, and we continue with the notations of Section 2 for this ring $\mathcal{O}$ and prime p. By (2.6) we may fix $a_{i,n} \in \mathfrak{p}_{i,n}$ and $b_{i,n} \in \prod_{j\neq i} \mathfrak{p}_{j,n}$ such that $a_{i,n} + b_{i,n} = c^{g-1}p^{d(g-1)}$. By (2.8) the following map is well defined:

$$\varphi_n : A[p^{n-d}] \to A[\mathfrak{p}_{1,n}] \oplus \ldots \oplus A[\mathfrak{p}_{g,n}], \quad t \mapsto (b_{1,n}t, \ldots, b_{g,n}t).$$

LEMMA 3.1. *The cokernel of φ_n is bounded independent of n.*

Proof. Since $p^n \in \mathfrak{p}_{i,n}$ we can define a map

$$\psi_n : A[\mathfrak{p}_{1,n}] \oplus \ldots \oplus A[\mathfrak{p}_{g,n}] \to A[p^{n-d}], \quad (t_1, \ldots, t_g) \mapsto p^d(t_1 + \ldots + t_g).$$

As $c^{g-1}p^{d(g-1)} - b_{i,n} \in \mathfrak{p}_{i,n}$, the map $\varphi_n \circ \psi_n$ is just multiplication by $c^{g-1}p^{dg}$. The lemma follows from this. ∎

For an $\mathcal{O}$-submodule Γ of $A(F)$, we now write

$$\lambda^{\Gamma}_{\mathfrak{p}_{i,n+d}} : \mathfrak{g}_{p^n}(\Gamma) \to \mathrm{Hom}_{\mathcal{O}}(\Gamma, A[\mathfrak{p}_{i,n+d}])$$

for the composition of $\lambda^{\Gamma}_{p^n}$ with φ_{n+d} and projection to $A[\mathfrak{p}_{i,n+d}]$. In the next lemma we use the natural map $\mathfrak{g}_{p^n}(\Gamma) \to \mathfrak{g}_{p^m}(\Gamma)$ (corresponding to multiplication by p^{n-m} from $\mathrm{Hom}_{\mathcal{O}}(\Gamma, A[\mathfrak{p}_{i,n+d}])$ to $\mathrm{Hom}_{\mathcal{O}}(\Gamma, A[\mathfrak{p}_{i,m+d}])$) to regard $\lambda^{\Gamma}_{\mathfrak{p}_{i,m+d}}$ as a map from $\mathfrak{g}_{p^n}(\Gamma)$ for $n \geq m$.

LEMMA 3.2. *Let $y_1, \ldots, y_r$ be an $\mathcal{O}$-pre-basis of $A(F)$. Then there is an integer b such that for all sufficiently large n there is a $\sigma_n \in \mathfrak{g}_{p^n}(A(F))$ with*

$$\lambda^{\mathcal{O}\cdot y_j}_{p^n}(\sigma_n) = 0 \quad \textit{for } j = 2, \ldots, r; \qquad \lambda^{\mathcal{O}\cdot y_1}_{\mathfrak{p}_{i,b}}(\sigma_n) \neq 0 \quad \textit{for all } i \in I_p(y_1).$$

Proof. The cokernel of the natural map

$$\pi : \mathrm{Hom}_{\mathcal{O}}(A(F), A[p^n]) \to \bigoplus_{j=1}^{r} \mathrm{Hom}_{\mathcal{O}}(\mathcal{O} \cdot y_j, A[p^n])$$

is bounded independent of n by the definition of a pre-basis. Combined with Proposition 1.2, this implies that the cokernel of

$$\pi \circ \lambda^{A(F)}_{p^n} : \mathfrak{g}_{p^n}(A(F)) \to \bigoplus_{j=1}^{r} \mathrm{Hom}_{\mathcal{O}}(\mathcal{O} \cdot y_j, A[p^n])$$

is bounded independent of n. Finally, by Lemma 3.1 we conclude that the cokernel of the map

$$\mathfrak{g}_{p^n}(A(F)) \to \Big(\bigoplus_{i\in I_p(y_1)} \mathrm{Hom}_{\mathcal{O}}(\mathcal{O} \cdot y_1, A[\mathfrak{p}_{i,n+d}])\Big) \oplus \Big(\bigoplus_{j=2}^{r} \mathrm{Hom}_{\mathcal{O}}(\mathcal{O} \cdot y_j, A[p^n])\Big) \tag{3.1}$$

is bounded independent of n.

By the definition of the set $I_p(y_i)$, for each $i \in I_p(y_1)$ there is some $m > 0$ such that $p^{n+d-m}\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}\cdot y_1, A[\mathfrak{p}_{i,n+d}]) \neq 0$ for sufficiently large n. (That is, these groups grow with n.) Since the cokernel of (3.1) is bounded, it follows that there is an integer b such that for sufficiently large n there is $\sigma_n \in \mathfrak{g}_{p^n}(A(F))$ with

$$\begin{aligned} \sigma_n|_{\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}\cdot y_j, A[p^n])} &= 0 \quad \text{ for } j = 2, \ldots, r; \\ p^{n+d-b}\sigma_n|_{\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}\cdot y_1, A[\mathfrak{p}_{i,n+d}])} &\neq 0 \quad \text{ for all } i \in I_p(y_1). \end{aligned}$$

By the remarks preceding the lemma, this σ_n is the required element of $\mathfrak{g}_{p^n}(A(F))$. ∎

LEMMA 3.3. *Let $y_1, \ldots, y_r$ be an $\mathcal{O}$-pre-basis of $A(F)$. Then there is an integer b such that for all sufficiently large n there are infinitely many places w of F_{p^n} with*

$$\operatorname{red}_w y_j \in p^n A(k_w) \quad \textit{for } j = 2, \ldots, r; \qquad \operatorname{red}_w y_1 \notin \mathfrak{p}_{i,b} A(k_w) \quad \textit{for } i \in I_p(y_1).$$

Proof. Let n be sufficiently large and fix σ_n as in Lemma 3.2. If w is a place of F_{p^n} with $\operatorname{Frob}_w = \sigma_n$ in $\mathfrak{g}_{p^n}(A(F))$, then w satisfies the conditions of the lemma by Lemmas 1.3 and 1.4. Since the Chebotarev density theorem guarantees the existence of infinitely many such w, the lemma follows. ∎

3.2. *Reduction of subgroups.* We are now in a position to prove our main result.

PROPOSITION 3.4. *Let A be an abelian variety over a number field F; assume that $\mathcal{O} = \operatorname{End}_F A$ is commutative. Fix a rational prime p and let Σ be a subgroup of $A(F)$ containing $A(F)_{\mathrm{tors}}$. Suppose that $x \in A(F)$ is such that*

$$\operatorname{red}_v x \in \operatorname{red}_v \Sigma \tag{3.2}$$

for almost all places v of F. Then x lies in $\Sigma \otimes \mathbb{Z}_{(p)}$.

Proof. Suppose that $x \notin \Sigma \otimes \mathbb{Z}_{(p)}$. By Proposition 2.3 we can then choose an $\mathcal{O}$-pre-basis $y_1, \ldots, y_r$ of $A(F)$ such that there is an integer a with

$$\psi_1(x) \notin \psi_1(\Sigma) + p^a\mathcal{O}. \tag{3.3}$$

Let b be the integer determined by $y_1, \ldots, y_r$ in Lemma 3.3 and fix $n > a + b + 2d$. Let w be a place of F_{p^n} as in Lemma 3.3; by (3.2) we may further assume that there is a $y \in \Sigma$ with $\operatorname{red}_w x = \operatorname{red}_w y$. Multiplying by η, by (2.4) we have

$$\psi_1(x)\operatorname{red}_w y_1 + \ldots + \psi_r(x)\operatorname{red}_w y_r = \psi_1(y)\operatorname{red}_w y_1 + \ldots + \psi_r(y)\operatorname{red}_w y_r.$$

Thus

$$(\psi_1(x) - \psi_1(y))\operatorname{red}_w y_1 \in p^n A(k_w) \tag{3.4}$$

by the definition of w.

Set $\alpha = \psi_1(x) - \psi_1(y)$; by (3.3) and (2.7), $\alpha \notin \mathfrak{p}_{i,a+d}$ for some i. Fix such an i. Since $\alpha \in \operatorname{im}\psi_1$, by (2.5) we have $i \in I_p(y_1)$; thus we also have $\mathrm{red}_w y_1 \notin \mathfrak{p}_{i,b}A(k_w)$ by the definition of w. Since $A(k_w)[p^{a+2d}] \subseteq p^b A(k_w)$ (as $A[p^n] \subseteq A(k_w)$ and $a+b+2d < n$), we may therefore apply Lemma 2.4 to conclude that $\alpha\,\mathrm{red}_w\, y_1 \notin p^{a+b+2d}A(k_w)$. Since $a+b+2d < n$, this contradicts (3.4), and thus proves the proposition. ∎

Corollary 3.5. *Let A be an abelian variety over a number field F and assume that* $\mathrm{End}_F A$ *is commutative. Let Σ be a subgroup of $A(F)$ containing $A(F)_{\mathrm{tors}}$ and suppose that $x \in A(F)$ is such that* $\mathrm{red}_v x \in \mathrm{red}_v \Sigma$ *for almost all places v of Σ. Then $x \in \Sigma$.*

Proof. This is immediate from Proposition 3.4 applied for all primes p. ∎

References

[1] G. Banaszak, W. Gajda, and P. Krasoń, *A support problem for the intermediate jacobians of l-adic representations*, arXiv:ANT-0374.

[2] D. Bertrand, *Galois representations and transcendental numbers*, in: New Advances in Transcendence Theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, 37–55.

[3] C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, J. Number Theory 64 (1997), 276–290.

[4] D. Eisenbud, *Commutative Algebra*, Springer, New York, 1995.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366; Erratum, ibid. 75 (1984), 381.

[6] E. Kowalski, *Some local-global applications of Kummer theory*, preprint.

[7] M. Larsen, *The support problem for abelian varieties*, arXiv:math.NT/0211118.

[8] D. Mumford, *Abelian Varieties*, published for the Tata Institute of Fundamental Research, Bombay, by Oxford Univ. Press, London, 1970.

[9] K. A. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. 46 (1979), 745–761.

Department of Mathematics
University of California, Berkeley
Berkeley, CA, 94720-3840, U.S.A.
E-mail: weston@math.berkeley.edu

Received on 26.8.2002
and in revised form on 28.1.2003 (4352)