Linear dependence in Mordell-Weil groups

Wojciech GAJDA and Krzysztof GORNISIEWICZ

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Septembre 2006

IHES/M/06/48

LINEAR DEPENDENCE IN MORDELL-WEIL GROUPS

Wojciech Gajda and Krzysztof Górnisiewicz

Abstract. We consider a local to global principle for detecting linear dependence of nontorsion points, by reduction maps, in the Mordell-Weil group of an abelian variety defined over a number field.

1. Introduction.

Let A be an abelian variety of dimension g, defined over a number field F, such that all algebraic endomorphisms of A are over F. For a prime v of good reduction for A we denote by $r_v : A(F) \longrightarrow A_v(\kappa_v)$ the reduction homomorphism, where κ_v is the residue field. Our main result in this paper is:

Main Theorem. *[Thm. 5.1* & *Cor. 6.1]*
In every nonempty isogeny class of abelian varieties over F, there exists an abelian variety A with the following property. Assume that $P_0, P_1, \ldots, P_r \in A(F)$ are points of the Mordell-Weil group, which are nontorsion over the ring of endomorphisms $\mathcal{O} = End\, A$ and such that $P_1, P_2, \ldots, P_r$ are linearly independent over $\mathcal{O}$. Denote by L the subgroup of $A(F)$ generated by $P_1, P_2, \ldots, P_r$. If $r_v(P_0) \in r_v(L)$ for almost all primes v, then there exist endomorphisms $f_1, f_2, \ldots, f_r \in \mathcal{O}$ such that

$$P_0 = f_1 P_1 + f_2 P_2 + \cdots + f_r P_r.$$

For an abelian variety A with $\mathcal{O}=\mathbb{Z}$ and $g = 2, 6$ or an odd integer, a stronger criterion for linear dependence was proven in [4], Theorem 4.2. More generally, if A is an abelian variety with the commutative ring of endomorphisms, then due to a result of Weston cf. [14], Theorem, the condition $r_v(P_0) \in r_v(L)$, for almost all v, implies a relation $P_0 \in L + A(F)_{tors}$. One should note however, that neither the method of the proof of [4], Thm. 4.2, nor the proof of Theorem of Weston, seem to extend to abelian varieties with noncommutative rings of endomorphisms.

Our proof of the main theorem is based on techniques of Kummer theory and Galois cohomology developed in papers [3], [4] and [5], augmented by an idea used

The research was partially financed by a KBN grant

in the proof of Theorem 5.2 of the preprint [10] by Larsen and Schoof. The combination of methods of [3], [4], [5] and [10] developed in the present work enabled us to treat the problem of detecting linear dependence by reductions for any abelian variety with no extra assumptions on the ring of endomorphisms nor on the dimension.

In Section 2 we introduce necessary notation and basic definitions of Kummer theory for abelian varieties which was developed by Ribet in [12]. In Section 3, following [10] we discuss the notion of integrally semisimple Galois modules. The proof of the main theorem is contained in Sections 4 and 5. In the last section of the paper we collected few corollaries which the reader may find of independent interest. In particular, using our Lemma 4.1 we strengthened the result of Weston mentioned above, by showing that one can remove the torsion ambiguity from the relation among the points P_0, P_1, ..., P_r cf. Corollary 6.2. As another corollary of the method of the proof of the main theorem we obtain the following genaralization of Theorem 8.2 of [2] on a multilinear version of the support problem of Erdös to arbitrary abelian varieties.

Corollary. *[Cor. 6.5]*
In every nonempty isogeny class of abelian varieties over F, there exists an abelian variety A with the following property. Let P_1, Q_1, P_2, Q_2, ..., P_r, $Q_r \in A(F)$ be points which are nontorsion over $\mathcal{O} = End\, A$ and such that the following condition holds true. For all sets of natural numbers $\{m_1, m_2, \dots, m_r\}$ and for almost all primes v of $\mathcal{O}_F$: if $m_1 r_v(P_1) + m_2 r_v(P_2) + \cdots + m_r r_v(P_r) = 0$, then $m_1 r_v(P_1) + m_2 r_v(Q_2) + \cdots + m_r r_v(Q_r) = 0$ in the group $A_v(\kappa_v)$.

Then there exist endomorphisms f_1, f_2, ..., $f_r \in \mathcal{O}$ and torsion points R_1, R_2, ..., $R_r \in A(F)_{tors}$ such that $Q_1 = f_1 P_1 + R_1$, $Q_2 = f_2 P_2 + R_2$, ..., $Q_r = f_r P_r + R_r$.

2. Kummer theory of abelian varieties.

Notation.

l	prime number
$\mathbb{Z}_l$	$l-$adic integers, $\mathbb{Q}_l$ field of fractions of $\mathbb{Z}_l$
$B[l^k]$	subgroup of l^k-torsion elements of an abelian group B
B_l	$= \bigcup_{k\geq 1} B[l^k]$, l-torsion subgroup of B
F	number field, $\mathcal{O}_F$ its ring of integers
G_F	$= G(\bar{F}/F)$, $\bar{F}$ fixed algebraic closure of F
v	prime ideal of $\mathcal{O}_F$, $\kappa_v = \mathcal{O}_F/v$ residue field at v
g_v	$= G(\overline{\kappa}_v/\kappa_v)$
A	abelian variety of dimension g, defined over F
$\mathcal{O}$	ring of algebraic endomorphisms of A
$T_l(A)$	Tate module of A at l, $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$

$\rho_l :$	$G_F \to Aut(T_l(A)) \cong Gl_{2g}(\mathbb{Z}_l)$ Galois representation of $T_l(A)$	
$\bar{\rho}_{l^k}$	residual representation $G_F \to GL(A[l^k])$ induced by ρ_l	
F_{l^k}	$=$	$F(A[l^k])$, for $k \geq 1$, is the field $\bar{F}^{ker \bar{\rho}_{l^k}}$
F_{l^∞}	$=$	$\bigcup_k F_{l^k}$
G_{l^k}	$=$	$G(F_{l^k}/F)$
G_{l^∞}	$=$	$G(F_{l^\infty}/F)$
H_{l^k}	$=$	$G(\overline{F}/F_{l^k})$
H_{l^∞}	$=$	$G(\overline{F}/F_{l^\infty})$
$H^i(G; M)$	cohomology group of continuous cochains for a profinite group G	

Let $\rho_l : G_F \longrightarrow Gl_{2g}(\mathbb{Z}_l)$ be the representation of the absolute Galois group $G_F := Gal(\bar{F}/F)$, which is associated with Tate module of A at the prime l. For $k \geq 1$, we denote by $\bar{\rho}_{l^k} : G_F \longrightarrow Gl_{2g}(\mathbb{Z}/l^k)$ the residual representation attached to the action of G_F at torsion points $A[l^k] := A(\bar{F})[l^k]$. We put $V_l(A) {:=} T_l(A) \otimes \mathbb{Q}_l$. Define groups: $H_{l^k} {:=} ker \bar{\rho}_{l^k}$, $H_{l^\infty} {:=} ker \rho_l$, $G_{l^k} {:=} Im \bar{\rho}_{l^k}$ and $G_{l^\infty} {:=} Im \rho_l$. Define fields of division points: $F_{l^k} {:=} \bar{F}^{H_{l^k}}$ and $F_{l^\infty} {:=} \bar{F}^{H_{l^\infty}}$. Consider the long exact sequence in Galois cohomology:

$$H^0(G_F, A(\overline{F})) \xrightarrow{\times l^k} H^0(G_F, A(\overline{F})) \xrightarrow{\delta} H^1(G_F, A[l^k]) \longrightarrow$$

induced by the exact sequence of Galois modules:

$$0 \longrightarrow A[l^k] \longrightarrow A(\overline{F}) \xrightarrow{\times l^k} A(\overline{F}) \longrightarrow 0.$$

The boundary homomorphism δ induces:

$$\phi^{(k)} : A(F)/l^k A(F) \hookrightarrow H^1(G_F; A[l^k]),$$

for $H^0(G_F, A(\overline{F})) = A(F)$. By definition of δ (cf. [6], p. 97), we have:

$$\phi^{(k)}(P + l^k A(F))(\sigma) = \sigma(R) - R,$$

where $P \in A(F)$, $\sigma \in G_F$ and $R \in A(\overline{F})$ is a point such that $l^k R = P$. One checks that changing the choice of R changes the cocyle $\phi^{(k)}(P + l^k A(F))$ by a coboundary. There are commutative diagrams:

$$\begin{tikzcd} A(F)/l^k A(F) \arrow[r, hook, "\phi^{(k)}"] \arrow[d, "\times l"] & H^1(G_F; A[l^k]) \arrow[d, "H^1(G_F; \times l)"] \\ A(F)/l^{k-1} A(F) \arrow[r, hook, "\phi^{(k-1)}"] & H^1(G_F; A[l^{k-1}]) \end{tikzcd} \tag{2.1}$$

which after passing to the inverse limit over k give a monomorphism:

$$A(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow H^1(G_F; T_l(A)), \tag{2.2}$$

since $A(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l = \lim A(F)/l^k A(F)$, by finite generation of $A(F)$, and we have $\lim H^1(G_F; A[l^k]) = H^1(G_F; T_l(A))$, by finiteness of $H^0(G_F; A[l^k])$. Consider the restriction homomorphism in Galois cohomology:

$$res : H^1(G_F; T_l(A)) \longrightarrow H^1(H_{l^\infty}; T_l(A))^{G_{l^\infty}}, \tag{2.3}$$

of the embedding $H_{l^\infty} \hookrightarrow G_F$. The fixed point set is taken with respect to the action induced via the exact sequence of profinite groups:

$$0 \longrightarrow H_{l^\infty} \longrightarrow G_F \longrightarrow G_{l^\infty} \longrightarrow 0.$$

Since H_{l^∞} acts trivially at $T_l(A)$ by definition, we have:

$$H^1(H_{l^\infty}; T_l(A))^{G_{l^\infty}} = Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A)).$$

Lemma 2.4. *The restriction map (2.3) has a finite kernel.*

Proof. By the inflation-restriction sequence [6], p. 100:

$$0 \longrightarrow H^1(G_{l^\infty}, T_l(A)^{H_{l^\infty}}) \xrightarrow{inf} H^1(G_F; T_l(A)) \xrightarrow{res} H^1(H_{l^\infty}; T_l(A))^{G_{l^\infty}}$$

we get $ker(res) = H^1(G_{l^\infty}; T_l(A)^{H_{l^\infty}}) = H^1(G_{l^\infty}; T_l(A))$. On the other hand:

$$H^1(G_{l^\infty}; T_l(A)) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{l}] = H^1(G_{l^\infty}; T_l(A) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{l}]) = H^1(G_{l^\infty}; V_l(A))$$

where the last gruop vanishes due to the theorem of Serre [13], Cor.1, p. 734. Hence, the group $ker(res)$ consists of elements of finite orders. The lemma follows, since the Galois cohomology group $H^1(G_F; T_l(A))$ is a finitely generated $\mathbb{Z}_l$−module. □

Definition 2.5. We define the homomorphism:

$$\phi : A(F) \otimes \mathbb{Z}_l \longrightarrow Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A)),$$

by the composition of maps (2.2) and (2.3).

Lemma 2.6.
For every prime l: $ker\,\phi = A(F)_{tors} \otimes \mathbb{Z}_l$. In particular, the group $ker\,\phi$ is finite.

Proof. Clearly $Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A)) \subset Hom(H_{l^\infty}; T_l(A))$, but $T_l(A)$ is a free $\mathbb{Z}_l-$module, hence $Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A))$ is a free $\mathbb{Z}_l-$module. Let $\sum_j P_j \otimes \alpha_j \in A(F)_{tors} \otimes \mathbb{Z}_l$, and let $n \in \mathbb{N}$, be such that $nP_j = 0$ for every j. Then $0 = \phi(\sum_j nP_j \otimes \alpha_j) = n\phi(\sum_j P_j \otimes \alpha_j) \in Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A))$ and the last module is free, so $\phi(\sum_j P_j \otimes \alpha_j) = 0$. Hence, $\sum_j P_j \otimes \alpha_j \in ker\phi$. To finish the proof we apply Lemma 2.4, since $(A(F) \otimes \mathbb{Z}_l)_{tors} = A(F)_{tors} \otimes \mathbb{Z}_l$. $\square$

We fix a finitely generated $\mathcal{O}-$submodule Λ of $A(F)$ and points $P_1, P_2, \dots, P_r \in \Lambda$ which are linearly independent over $\mathcal{O}$ and generate Λ. All modules over $\mathcal{O}$ considered in this paper are by definition left $\mathcal{O}-$modules. For $P \in A(F)$ and $k \in \mathbb{N}$ we define the Kummer map:

$$\phi_P^{(k)} : H_{l^k} \to A[l^k] \tag{2.7}$$

$$\phi_P^{(k)}(\sigma) = \sigma(\frac{1}{l^k}P) - \frac{1}{l^k}P,$$

where $H_{l^k} = G(\overline{F}/F_{l^k})$ and $\frac{1}{l^k}P = R \in A(\overline{F})$ is such a point that $l^k R = P$. Observe that by definition:

$$\phi_P^{(k)} = res^{(k)}(\phi^{(k)}(P + l^k A(F))),$$

where

$$res^{(k)} : H^1(G_F, A[l^k]) \to H^1(H_{l^k}, A[l^k])^{G_{l^k}} = Hom_{G_{l^k}}(H_{l^k}, A[l^k])$$

is the restriction map. We define:

$$\Phi^{(k)} : H_{l^k} \to \bigoplus_{i=1}^{r} A[l^k]$$

$$\Phi^{(k)} = (\phi_{P_1}^{(k)}, \phi_{P_2}^{(k)}, \dots, \phi_{P_r}^{(k)}).$$

For $k > 1$, the following diagram commutes.

$$\begin{tikzcd} H_{l^k} \arrow[r, "\phi_P^{(k)}"] \arrow[d] & A[l^k] \arrow[d, "\times l"] \\ H_{l^{k-1}} \arrow[r, "\phi_P^{(k-1)}"] & A[l^{k-1}] \end{tikzcd}$$

We denote by:

$$\phi_P : H_{l^\infty} \to T_l(A) \tag{2.8}$$

the group homomorphism obtained by passing to the inverse limit. Note that by Definition 2.5 $\phi_P = \phi(P)$. Let

$$\Phi : H_{l^\infty} \to \bigoplus_{i=1}^{r} T_l(A)$$

be defined by the formula:

$$\Phi = (\phi_{P_1}, \dots, \phi_{P_r}).$$

Proposition 2.9.
The image of Φ is an open subset of $\bigoplus_{i=1}^{r} T_l(A)$ with respect to the $l-$adic topology.

Proof. [4], Lemma 2.13.

3. Integrally semisimple G_F-modules.

In this section we collect material on integrally semisimple Galois modules following Section 4 of [10]. The main technical result in this section is Proposition 3.6, which generalizes [10], Lemma 4.5.

Definition 3.1.
Let T be a free $\mathbb{Z}_l-$module equipped with a continuous action of the Galois group G_F and let $V = T \otimes \mathbb{Q}_l$ be the associated rational Galois representation. We say that the module T is integrally semisimple, if for every G_F-subrepresentation $W \subset V$ the following exact sequence of $\mathbb{Z}_l[G_F]-$modules splits.

$$0 \longrightarrow T \cap W \longrightarrow T \longrightarrow T/T \cap W \longrightarrow 0$$

Lemma 3.2.
Let V be a finitely dimensional $\mathbb{Q}_l-$vector space with a continuous action of G_F such that the associated representation is semisimple. There exists a lattice $T \subset V$ which is an integrally semisimple G_F-module.

Proof. Without loss of generality we can assume that $V = V_1 \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^k$ for an irreucible representation V_1 of G_F and $k \in \mathbb{N}$. Since G_F is compact, there exists a G_F-stable lattice $T_1 \subset V_1$. Let $T = T_1 \otimes_{\mathbb{Z}_l} \mathbb{Z}_l^k \subset V_1 \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^k$. We check that T is integrally semisimple. Let then $W \subset V$ be a subrepresentation of V. Then $W = V_1 \otimes_{\mathbb{Q}_l} W_0$, for a subspace W_0 of $\mathbb{Q}_l^k$. Hence:

$$W \cap T = (V_1 \otimes_{\mathbb{Q}_l} W_0) \cap (T_1 \otimes_{\mathbb{Z}_l} \mathbb{Z}_l^k) = (T_1 \otimes_{\mathbb{Z}_l} W_0) \cap (T_1 \otimes_{\mathbb{Z}_l} \mathbb{Z}_l^k) = T_1 \otimes_{\mathbb{Z}_l} (\mathbb{Z}_l^k \cap W_0).$$

Consider the exact sequence of $\mathbb{Z}_l-$modules:

$$0 \longrightarrow \mathbb{Z}_l^k \cap W_0 \longrightarrow \mathbb{Z}_l^k \longrightarrow Q \longrightarrow 0. \tag{3.3}$$

Since W_0 is a $l-$divisible group, the quotient group $Q = \mathbb{Z}_l^k/(\mathbb{Z}_l^k \cap W_0)$ is nontorsion, so Q is a free goup, and the exact sequence (3.3) splits. Tensoring by T_1 we obtain the exact sequence of $\mathbb{Z}_l[G_F]$-modules:

$$0 \longrightarrow T \cap W \longrightarrow T \longrightarrow T_1 \otimes_{\mathbb{Z}_l} Q \longrightarrow 0$$

which splits. $\square$

Observe that the representation $V_l = T_l \otimes \mathbb{Q}_l$ is semisimple, if the module T_l is integrally semisiple in the sense of Definition 3.1.

Lemma 3.4.
If A is an abelian variety defined over a number field F, then for l sufficiently large, Tate module $T_l(A)$ of A is integrally semisimple.

Proof. We fix an embedding of F in the field of complex numbers $\mathbb{C}$. Let $M = H_1(A(\mathbb{C}); \mathbb{Z}) \cong \mathbb{Z}^{2g}$. Then $\mathcal{O} := End A$ acts at M, i.e., there is an embedding $\mathcal{O} \longrightarrow End(M) \cong M_{2g,2g}(\mathbb{Z})$. Let $h : End(M) \longrightarrow Hom(\mathcal{O}, End(M))$ be defined by the formula: $h(m)(r) = rm - mr$. Define the commutant $C := ker\, h$. Let $\mathcal{O}_l := \mathcal{O} \otimes \mathbb{Z}_l$, $C_l := C \otimes \mathbb{Z}_l$. By comparision of singular and étale cohomology we get: $End_{\mathbb{Z}_l}(T_l(A)) = End(M) \otimes \mathbb{Z}_l \cong M_{2g,2g}(\mathbb{Z}_l)$. By the theorem of Faltings [8], Satz 4 and Bemerkung 2, for every l, the commutant of $\mathcal{O}_l$ in $End(T_l(A))$ equals the $\mathbb{Z}_l-$module generated by matrices from the image of $\rho_l(G_F)$. If $(W \cap T_l(A)) \otimes \mathbb{Q}_l$ is a G_F-submodule, then it follows that $T_l(A)/(W \cap T_l(A))$ is a finitely generated, nontorsion C_l-module. On the other hand, for l big enough, C_l is a maximal order in $C \otimes \mathbb{Q}_l$. By [7], Thm. 26.12, it follows that any finitely generated, nontorsion C_l-module is projective, if l is big enough. Hence, the exact sequence of $\mathbb{Z}_l[G_F]-$modules:

$$0 \longrightarrow W \cap T_l(A) \longrightarrow T_l(A) \longrightarrow T_l(A)/(W \cap T_l(A)) \longrightarrow 0,$$

splits for $l \gg 0$. $\square$

Proposition 3.5.
Every nonempty isogeny class of abelian varieties defined over a number field F contains an abelian variety A such that for every l, Tate module $T_l(A)$ is integrally semisimple.

Proof. Observe that an isogeny of degree a power of a prime $l' \neq l$ does not change the module $T_l(A)$. Hence, by Lemma 3.4, it is enough to show that for every rational prime l, there exists an abelian variety B isogenous to A, for which $T_l(B)$

is integrally semisimple. The vector space $T_l(A) \otimes \mathbb{Q}_l$ contains a lattice Λ which is integrally semisimple by Lemma 3.2. Multiplying by a power of l, if necessary, we can assume that $\Lambda \subset T_l(A)$. The quotient group $T_l(A)/\Lambda$ defines a finite G_F-stable, $l-$torsion subgroup D of A. To finish the proof we put $B = A/D$. $\square$

Proposition 3.6.
Let M, N be free, finitely generated $\mathbb{Z}_l-$modules with continuous actions of G_F. Let N be integrally semisimple. Assume that there are homomorphisms of $\mathbb{Z}_l[G_F]-$modules:

$$\alpha_1, \alpha_2, \dots, \alpha_r, \beta : M \to N$$

such that for every $m \in M$ and every $k \in \mathbb{N}$:

$$\textit{if} \quad \alpha_1(m), \alpha_2(m), \dots, \alpha_r(m) \in l^k N, \quad \textit{then} \quad \beta(m) \in l^k N.$$

Then there exists a homomorphism of $\mathbb{Z}_l[G_F]-$modules:

$$\gamma : \bigoplus_{i=1}^{r} N \to N$$

such that $\gamma \circ (\alpha_1, \alpha_2, \dots, \alpha_r) = \beta$.

Proof. Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_r) : M \longrightarrow \bigoplus_{i=1}^{r} N$. We will denote: $W_\alpha := Im\alpha \otimes \mathbb{Q}_l$, $W_\beta := Im\beta \otimes \mathbb{Q}_l$ and $V := \bigoplus_{i=1}^{r} N \otimes \mathbb{Q}_l$. Since $\bigcap_{k=1}^{\infty} l^k M = 0$, by assumption, if $\alpha_i(m) = 0$, for every $i \in \{1, 2, \dots, r\}$, then $\beta(m) = 0$. Hence, $ker\alpha \subset ker\beta$ and the space $W_\beta = M/ker\beta \otimes \mathbb{Q}_l$ is the quotient of the linear space $W_\alpha = M/ker\alpha \otimes \mathbb{Q}_l$. Let $\xi : W_\alpha \longrightarrow W_\beta$ denote the quotient map. Since N is integrally semisimple, the $\mathbb{Z}_l[G_F]-$module, $\bigoplus_{i=1}^{r} N$ is also integrally semisimple and there exists a $\mathbb{Z}_l[G_F]-$module $P \subset \bigoplus_{i=1}^{r} N$, which is the complement of $W_\alpha \cap \bigoplus_{i=1}^{r} N$ in $\bigoplus_{i=1}^{r} N$. We denote by $\pi : \bigoplus_{i=1}^{r} N \longrightarrow W_\alpha \cap \bigoplus_{i=1}^{r} N$ the quotient map, which is a homomorphism of $\mathbb{Z}_l[G_F]-$modules. Define the homomorhpism $\gamma : \bigoplus_{i=1}^{r} N \longrightarrow N \otimes \mathbb{Q}_l$ by the composition:

$$\begin{tikzcd}
\bigoplus_{i=1}^{r} N \arrow[rr, "\gamma"] \arrow[d, "\pi"] & & N \otimes \mathbb{Q}_l \\
W_\alpha \cap \bigoplus_{i=1}^{r} N \arrow[r, hook] & W_\alpha \arrow[r, "\xi"] & W_\beta \arrow[u, hook]
\end{tikzcd}$$

By construction, for every $m \in M$ we have $\gamma(\alpha(m)) = \beta(m)$. To finish the proof it is enough to show that $Im\gamma \subset N$. Since π (hence γ also) is trivial map at the submodule P, it is enough to show that $\gamma(W_\alpha \cap \bigoplus_{i=1}^{r} N) \subset N$. If $n \in W_\alpha \cap \bigoplus_{i=1}^{r} N$, then there is $k \geq 0$, such that $l^k n \in \alpha(M)$, so $l^k n = \alpha(m)$ for an $m \in M$. If $k > 0$, then by asumption $\beta(m) \in l^k N$, hence:

$$\gamma(n) = l^{-k} \gamma(l^k n) = l^{-k} \gamma(\alpha(m)) = l^{-k} \beta(m) \in N. \quad \square$$

4. Three lemmas.

To simplify notation in this section we put: $T_l := T_l(A)$, $T_l^r = \bigoplus_{i=1}^r T_l$, $A_v(\kappa_v)_l := A_v(\kappa_v)_{l-tors}$ and $A[m]^r = \bigoplus_{i=1}^r A[m]$.

Lemma 4.1.
Let $P_1, \dots, P_r \in A(F)$ be points which are linearly independent over $\mathcal{O} = End\, A$ and let l be a rational prime. Consider the reduction maps:

$$r_v : A(F) \longrightarrow A_v(\kappa_v)_{l-torsion}$$

at primes v of good reduction for A such that $v \nmid l$. There exists a set Π of prime ideals of $\mathcal{O}_F$, such that Π has positive density and

$$r_v(P_1) = r_v(P_2) = \dots = r_v(P_r) = 0$$

for every $v \in \Pi$.

Proof. The argument is similar to the proof of [4], Thm. 3.1, see also [5]. Define fields: $F_{l^k}(\frac{1}{l^k}\hat{\Lambda}) := \overline{F}^{ker\Phi^{(k)}}$ and $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}) := \overline{F}^{ker\Phi}$. Consider the following commutative diagram:

$$\begin{tikzcd}
G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda})/F_{l^\infty}) \arrow[r] \arrow[d] & T_l^r/l^m T_l^r \arrow[d] \\
G(F_{l^{k+1}}(\frac{1}{l^{k+1}}\hat{\Lambda})/F_{l^{k+1}}) \arrow[r] \arrow[d] & (A[l^{k+1}])^r/l^m(A[l^{k+1}])^r \arrow[d] \\
G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda})/F_{l^k}) \arrow[r] & (A[l^k])^r/l^m(A[l^k])^r
\end{tikzcd}$$

where the horizontal maps are induced by Kummer maps Φ, $\Phi^{(k+1)}$, $\Phi^{(k)}$ and $m \in \mathbb{N}$ such that $l^m T_l^r \subset \mathrm{Im}\Phi$. Such a number m exists by Proposition 2.9. For $k \geq m$ images of the homomorphisms:

$$G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda})/F_{l^k}) \to (A[l^k])^r/l^m(A[l^k])^r$$

and

$$G(F_{l^{k+1}}(\frac{1}{l^{k+1}}\hat{\Lambda})/F_{l^{k+1}}) \to (A[l^{k+1}])^r/l^m(A[l^{k+1}])^r$$

are isomorphic. Hence, the homomorphism:

$$G(F_{l^{k+1}}(\frac{1}{l^{k+1}}\hat{\Lambda})/F_{l^{k+1}}) \to G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda})/F_{l^k})$$

is surjective, so:

$$F_{l^k}(\frac{1}{l^k}\hat{\Lambda}) \cap F_{l^{k+1}} = F_{l^k},$$

for $k \geq m$. For such k we have the following tower of fields:

$$\begin{tikzcd}[column sep=small]
 & F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}) \arrow[dl, dash] \arrow[dr, dash] & \\
F_{l^k}(\frac{1}{l^k}\hat{\Lambda}) \arrow[dr, dash, "id"] & & F_{l^{k+1}} \arrow[dl, dash, "h"'] \\
 & F_{l^k} \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

By the theorem of Bogomolov ([1], Cor. 1, p.702) for k big enough there exists a nontrivial homothety h in the image of ρ_l, which acts at T_l by multiplcation by $1 + l^k u_0$, for $u_0 \in \mathbb{Z}_l^{\times}$. We choose

$$\gamma \in G(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})/F_{l^k}) \subset G(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})/F)$$

such that $\gamma|_{F_{l^k}(\frac{1}{l^k}\hat{\Lambda})} = id$, $\gamma|_{F_{l^{k+1}}} = h$. By Chebotarev density theorem ([9], Thm 10.4, p. 217) there exists a set Π of primes of $\mathcal{O}_F$, with positive density such that for $v \in \Pi$ the Frobenius element Fr_v in the extension $F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})/F$ equals γ. For such a v we fix an ideal w in $\mathcal{O}_{F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})}$ over v. Consider the commutative diagram:

$$\begin{tikzcd}
A(F) \arrow[r, "r_v"] \arrow[d] & A_v(\kappa_v)_l \arrow[d] \\
A(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})) \arrow[r, "r_w"] & A_w(\kappa_w)_l
\end{tikzcd}$$

Now we repeat Step 4 of the proof of Theorem 3.1 of [4]. Vertical maps in the diagram are natural injections. Let l^{c_i} be the order of $r_v(P_i) \in A_v(\kappa_v)_l$ for $c_i \geq 0$ and $i \in \{1, \ldots, r\}$. The the point $Q_i = \frac{1}{l^k}P_i \in A(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}))$ maps to the point $r_w(Q_i) \in A_w(\kappa_w)_l$ of order l^{c_i+k}, because $l^{c_i+k}r_w(Q_i) = 0$. By the choice of v we get:

$$h(r_w(Q_i)) = (1 + l^k u_0)r_w(Q_i),$$

where h is the homothety chosen before. The choice of v implies also that $r_w(Q_i) \in A_v(\kappa_v)_l$, hence $h(r_w)(Q_i) = r_w(Q_i)$, so $l^k r_w(Q_i) = 0$. This is possible only if $c_i = 0$. Hence, $r_v(P_i)$ is zero. $\square$

Lemma 4.2.
Let M be a finitely generated abelian group, $L \subset M$ a subgroup and $x \in M$. If for every rational prime l, $x \otimes 1 \in L \otimes \mathbb{Z}_l + (M \otimes \mathbb{Z}_l)_{tors}$, then $x \in L + M_{tors}$

Proof. Consider the short exact sequence of groups:

$$0 \longrightarrow L + M_{tors} \longrightarrow M \longrightarrow N \longrightarrow 0. \tag{4.3}$$

Tensoring with $\mathbb{Z}_l$ gives the exact sequence of $\mathbb{Z}_l-$modules:

$$0 \longrightarrow (L + M_{tors}) \otimes \mathbb{Z}_l \longrightarrow M \otimes \mathbb{Z}_l \longrightarrow N \otimes \mathbb{Z}_l \longrightarrow 0. \tag{4.4}$$

Observe that:

$$(L + M_{tors}) \otimes \mathbb{Z}_l = L \otimes \mathbb{Z}_l + M_{tors} \otimes \mathbb{Z}_l = L \otimes \mathbb{Z}_l + (M \otimes \mathbb{Z}_l)_{tors}.$$

Hence, by the exactness of (4.4): $x \otimes 1 \in L \otimes \mathbb{Z}_l + (M \otimes \mathbb{Z}_l)_{tors}$ if and only if $x \otimes 1$ goes to zero in $N \otimes \mathbb{Z}_l$. Denote by $\overline{x}$ the image of $x \in M$ in N in the sequence (4.3). Clearly, for x as in the assumption, $\overline{x} \otimes 1 = 0$ in $N \otimes \mathbb{Z}_l$, if and only if, $\overline{x}$ has order prime to l. Since l is arbitrary, $\overline{x} = 0$. Hence, by (4.3) we get $x \in L + M_{tors}$. □

Let $P \in A(F)$ be a point of infinite order and let $k \in \mathbb{N}$. We choose $R := \frac{1}{l^k} P \in A(\overline{F})$ such that $l^k R = P$. Let $F_{l^k}(\frac{1}{l^k}\hat{P}) := \overline{F}^{ker\, \phi_P^{(k)}}$, where $\phi_P^{(k)}$ denotes the Kummer homomorphism (2.7).

Lemma 4.5.
Let $w \nmid l$ be a nonzero prime ideal of $\mathcal{O}_{F_{l^k}}$, which is a prime of good reduction for A. Then the following two conditions are equivalent:

1. *$r_w(P) \in l^k A_w(\kappa_w)$, where $\kappa_w = \mathcal{O}_{F_{l^k}}/w$,*
2. *$Fr_w(R) = R$, where $Fr_w \in Gal(F_{l^k}(\frac{1}{l^k}\hat{P})/F_{l^k})$ is the Frobenius at w.*

Proof. Let w' be an ideal in $\mathcal{O}_{F_{l^k}(\frac{1}{l^k}\hat{P})}$ over w.

(2)$\Longrightarrow$ (1) If $Fr_w(R) = R$, then w' splits completely in $F_{l^k}(\frac{1}{l^k}\hat{P})/F_{l^k}$. In particular, $\kappa_{w'} = \kappa_w$, hence $r_{w'}(R) \in A_{w'}(\kappa_{w'}) = A_w(\kappa_w)$, so

$$r_w(P) = l^k r_{w'}(R) \in l^k A_w(\kappa_w).$$

(1) $\Longrightarrow$ (2) Consider the diagram:

$$\begin{tikzcd} A(F_{l^k}(\frac{1}{l^k}\hat{P})) \arrow[r, "r_{w'}"] & A_{w'}(\kappa_{w'}) \\ A(F_{l^k}) \arrow[r, "r_w"] \arrow[u, hook] & A_w(\kappa_w) \arrow[u, hook] \end{tikzcd} \tag{4.6}$$

which implies:

$$l^k r_{w'}(R) = r_{w'}(l^k R) = r_{w'}(P) = r_w(P).$$

By definition we have: $A(F_{l^k}(\frac{1}{l^k}\hat{P}))[l^k] = A(F_{l^k})[l^k] = A[l^k]$. This together with the commutativity of the diagram (4.6) gives $A_{w'}(\kappa_{w'})[l^k] = A_w(\kappa_w)[l^k]$ and that $r_{w'}|_{A[l^k]}$ is a monomorphism. Let $r_w(P) = l^k Q$ for $Q \in A_w(\kappa_w)$. Then

$$l^k[Q - r_{w'}(R)] = l^k Q - l^k r_{w'}(R) = r_w(P) - r_w(P) = 0,$$

hence $Q - r_{w'}(R) \in A_{w'}(\kappa_{w'})[l^k] = A_w(\kappa_w)[l^k]$, but $Q \in A_w(\kappa_w)$, so we get $r_{w'}(R) \in A_w(\kappa_w)$. In particular:

$$r_{w'}[Fr_w(R) - R] = Fr_w(r_{w'}(R)) - r_{w'}(R) = r_{w'}(R) - r_{w'}(R) = 0. \tag{4.7}$$

On the other hand:

$$l^k[Fr_w(R) - R] = Fr_w(P) - P = 0.$$

Hence, $Fr_w(R) - R$ is in the group $A[l^k]$, at which $r_{w'}$ is injective. The equality (4.7) implies $Fr_w(R) = R$. $\square$

5. Proof of Main Theorem.

Theorem 5.1.
Let A be an abelian variety over a number field F such that $\mathcal{O}=End_F A=End_{\overline{F}} A$. We assume that for all rational primes l the Tate module $T_l(A)$ of A is integrally semisimple. Let $P_0, P_1, \ldots, P_r \in A(F)$ be points of the Mordell-Weil group which are nontorsion over the ring $\mathcal{O}$ and such that $P_1, P_2, \ldots, P_r$ are linearly idependent over $\mathcal{O}$. Denote by L the subgroup of $A(F)$ generated by $P_1, P_2, \ldots, P_r$. If $r_v(P_0) \in r_v(L)$ for almost all primes v of F, then $P_0 \in \mathcal{O}L$, i.e., there exist endomorphisms $f_1, f_2, \ldots, f_r \in \mathcal{O}$ such that

$$P_0 = f_1 P_1 + f_2 P_2 + \cdots + f_r P_r.$$

Proof. For a profinite group G and a rational prime l we denote by

$$\hat{G} = \lim_{\leftarrow} G^{ab}/l^k G^{ab}$$

the $l-$adic completion of the abelianization $G^{ab} = G/\overline{[G,G]}$ of G. Let $j_l : G \longrightarrow \hat{G}$ denote the natural homomorphism of topological groups. Every group homomorphism $H_{l^\infty} \longrightarrow T_l(A)$ induces a homomorphism of $\mathbb{Z}_l-$modules: $\hat{H}_{l^\infty} \longrightarrow$

$T_l(A)$. Hence, the Kummer map ϕ of Definition 2.5 induces a homomorphism of $\mathbb{Z}_l-$modules:

$$\hat{\phi} : A(F) \otimes \mathbb{Z}_l \longrightarrow Hom_{G_{l^\infty}}(\hat{H}_{l^\infty}; T_l(A)),$$

such that the following diagram commutes.

$$\begin{tikzcd}
 & Hom_{G_{l^\infty}}(H_{l^\infty}; T_l(A)) \\
A(F) \otimes \mathbb{Z}_l \arrow[ur, "\phi"] \arrow[dr, "\hat{\phi}"'] & \\
 & Hom_{G_{l^\infty}}(\hat{H}_{l^\infty}; T_l(A)) \arrow[uu, "Hom(j_l; T_l(A))"']
\end{tikzcd} \tag{5.2}$$

Observe that $\phi(\hat{P}) = \phi_P : H_{l^\infty} \longrightarrow T_l(A)$ is the Kummer map (2.8), where $\hat{P} = P \otimes 1 \in A(F) \otimes \mathbb{Z}_l$.

The proof of the theorem falls naturally into two steps. First we deduce the claim of the theorem from an additional condition. Then assuming that the extra condition does not hold, we obtain a contradiction with the assumption of the theorem.

Step 1.
Assume that for all rational primes l, all $n \in \mathbb{N}$ and all $\sigma \in \hat{H}_{l^\infty}$:

$$\text{if} \quad \hat{\phi}(\hat{P}_1)(\sigma), \hat{\phi}(\hat{P}_2)(\sigma), \dots, \hat{\phi}_{\hat{P}_r}(\sigma) \in l^n T_l(A), \quad \text{then} \quad \hat{\phi}(\hat{P}_0)(\sigma) \in l^n T_l(A). \tag{5.3}$$

Let $\hat{\Phi} : \hat{H}_{l^\infty} \longrightarrow \bigoplus_{i=1}^r T_l(A)$, be the map $\hat{\Phi}=(\hat{\phi}(\hat{P}_1), \dots, \hat{\phi}(\hat{P}_r))$. We apply Proposition 3.6 to $M=Im\hat{\Phi}$, $N=T_l(A)$ and $\alpha_1=\hat{\phi}(\hat{P}_1)$, $\alpha_2=\hat{\phi}(\hat{P}_2)$, $\dots$, $\alpha_r=\hat{\phi}(\hat{P}_r)$ and $\beta=\hat{\phi}(\hat{P}_0)$. Proposition 3.6 implies that there is a homomorphism of $\mathbb{Z}_l[G_F]-$modules

$$g : \bigoplus_{i=1}^r T_l(A) \longrightarrow T_l(A)$$

such that $g \circ \hat{\Phi} = \hat{\phi}(\hat{P}_0)$. Let $g_i : T_l(A) \longrightarrow T_l(A)$ for $1 \leq i \leq r$, be the restriction of g to the ith component $T_l(A)$ of $\bigoplus_{i=1}^r T_l(A)$. Hence, g_i is a $\mathbb{Z}_l[G_F]-$endomorfizmem of $T_l(A)$. We have: $\sum_{i=1}^r g_i \hat{\phi}(\hat{P}_i) = \hat{\phi}(\hat{P}_0)$. By the theorem of Faltings [8], Satz 4: $End_{\mathbb{Z}_l[G_F]}(T_l(A)) \cong \mathcal{O} \otimes \mathbb{Z}_l$. It follows that there is an element $\hat{f}_i \in \mathcal{O} \otimes \mathbb{Z}_l$ such that $g_i \hat{\phi}(\hat{P}_i) = \hat{\phi}(\hat{f}_i \hat{P}_i)$. Since $\hat{\phi}$ is a homomorphism of $\mathbb{Z}_l-$modules we obtain the equality:

$$\hat{\phi}(\sum_{i=1}^r \hat{f}_i \hat{P}_i) = \hat{\phi}(\hat{P}_0). \tag{5.4}$$

The diagram (5.2) and Lemma 2.6 imply that: $ker\,\hat{\phi} \subset A(F)_{tors} \otimes \mathbb{Z}_l$. Hence, by (5.4):

$$P_0 \otimes 1 = \hat{P}_0 \quad = \quad \sum_{i=1}^{r} \hat{f}_i \hat{P}_i + \hat{Q} \quad \in \quad \mathcal{O}L \otimes \mathbb{Z}_l + A(F)_{tors} \otimes \mathbb{Z}_l,$$

for some $\hat{Q} \in A(F)_{tors} \otimes \mathbb{Z}_l$. It follows by Lemma 4.2, applied to $\mathcal{O}L \subset M = A(F)$ and $x = P_0$, that

$$P_0 = \sum f_i P_i + Q$$

for some $f_i \in \mathcal{O}$ and $Q \in A(F)_{tors}$. To complete the first step of the proof we have to show that $Q = 0$. We have $Q = P_0 - \sum f_i P_i \in A(F)_{tors}$. By Lemma 4.1 there exist infinitely many v (even positive density) such that

$$r_v(P_1) = \ldots = r_v(P_r) = 0.$$

By assumption, $r_v(P) \in r_v(L)$, so we also have $r_v(P_0) = 0$. Hence, for infinitely many v :

$$r_v(Q) = r_v(P_0 - \sum f_i P_i) = r_v(P_0) - \sum f_i r_v(P_i) = 0.$$

It is well-known that for almost all v, the reduction map $r_v : A(F)_{tors} \longrightarrow A_v(\kappa_v)_l$ restricted to the torsion subgroup is an injection cf. [3], Lemma 2.13, hence Q must be zero.

Step 2.
We assume to the contrary that the condition (5.3) does not hold, i.e., that there exists a prime l, a natural number n and $\sigma \in \hat{H}_{l^\infty}$ such that $\hat{\phi}(\hat{P}_i)(\sigma) \in l^n T_l(A)$, for $i \in 1, \ldots, r$, and $\hat{\phi}(\hat{P}_0)(\sigma) \notin l^n T_l(A)$. Since $H_{l^\infty}^{ab}$ is a profinite abelian group the $l-$adic completion $\hat{H}_{l^\infty}$ is isomorphic to a closed subgroup of $H_{l^\infty}^{ab}$. Let $\tilde{\sigma} \in H_{l^\infty}$ be a lifting of σ defined by this isomorphism. Since $T_l(A)/l^n T_l(A) = A[l^n]$, it follows by the definition of $\hat{\phi}(\hat{P})$ that $\tilde{\sigma}$ acts trivially at the points $\frac{1}{l^n} P_1, \ldots, \frac{1}{l^n} P_r$, and acts nontrvially at the points $\frac{1}{l^n} P_0$. Define the field $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P}_0) := F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}) F_{l^\infty}(\frac{1}{l^\infty}\hat{P}_0)$. Consider the open set in the Galois group $G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P}_0)/F)$ consisting of elements which act in the same way as $\bar{\sigma} := \tilde{\sigma}|_{F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P}_0)}$. We claim that there exists $k \geq n$ and an element γ in this open set, such that γ acts as a scalar congruent to 1 modulo l^k, but not modulo l^{k+1} on the Tate module $T_l(A)$. Indeed, by the theorem of Bogomolov [1], Cor. 1, p.702 in G_{l^∞} there exists a nontrivial homothety $\tau = \alpha I_{2g}$ such that $\alpha \in \mathbb{Z}_l^\times = \mathbb{Z}/(l-1) \oplus (1 + l\mathbb{Z}_l)$ is congruent to 1 modulo l. Lifting τ to a homothety $h \in G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P}_0)/F)$, we define the element $\gamma := h^{l^k}\bar{\sigma}$ which has the desired property, if k is sufficiently large. We use Chebotarev density theorem to choose infinitely many prime ideals v in $\mathcal{O}_F$ in such a way that Fr_v is close enough to γ, so Fr_v acts trivially at points of $A[l^k]$ and at points $\frac{1}{l^n} P_i$ for $1 \leq i \leq r$, but acts nontrivially at all points $\frac{1}{l^n} P_0$. Let w be

a prime in F_{l^k} which is over v. Since Fr_v is the identity in the extension F_{l^k}/F and $A_v(\overline{\kappa_v})[l^k] = A_w(\kappa_w)[l^k] = A_v(\kappa_v)[l^k] = (\mathbb{Z}/l^k)^{2g}$, reducing modulo v chosen above, we obtain $A_v(\kappa_v)_l = (\mathbb{Z}/l^k)^{2g}$. It follows by Lemma 4.5 that the elements $r_v(P_1), \dots, r_v(P_r)$ are divisible by l^n, and that $r_v(P_0)$ is not l^n-divisible in the group $A_v(\kappa_v)_l$. Hence, the orders of $r_v(P_1), \dots, r_v(P_r)$ are divisible by at most l^{k-n}, and the same is true for any element of the subgroup of $A_v(\kappa_v)_l = (\mathbb{Z}/l^k)^{2g}$ generated by these points. On the other hand, the order of $r_v(P_0)$ in $A_v(\kappa_v)_l$ is divisible by at least l^{k-n+1}. This holds true for infinitely many prime ideals v which we have chosen above. Hence, $r_v(P_0) \notin r_v(L)$ for infinitely many v, contrary to the assumption of the theorem. $\square$

6. Corollaries.

Corollary 6.1.
In every nonempty isogeny class of abelian varieties over F there exists a variety A for which the conclusion of Theorem 5.1 holds true, i.e., if $P_0, P_1, \dots, P_r \in A(F)$ are points which are nontorsion over the ring $\mathcal{O}$, and $P_1, P_2, \dots, P_r$ are linearly idependend over $\mathcal{O}$, and $r_v(P_0) \in r_v(L)$ for almost all primes v of F, then $P_0 \in \mathcal{O}L$, where L denotes the subgroup of $A(F)$ generated by $P_1, P_2, \dots, P_r$.

Proof. It follows by Theorem 5.1 and Proposition 3.5. $\square$

Lemma 4.1 has two immediate corollaries. Corollary 6.2 strengthens a result of Weston [14], Theorem. Corollary 6.3 gives a different proof of Theorem 4.1 from the paper [11] in the case of a simple abelian variety.

Corollary 6.2.
Let A be an abelian variety defined over a number field F such that $\mathcal{O} = End\, A$ is a commutative ring. Let L be a subgroup of the Mordell-Weil group $A(F)$ and $P \in A(F)$ a nontorsion point. If for almost all primes v of F we have $r_v(P) \in r_v(L)$, then $P \in L$.

Proof. Thomas Weston showed that under the assumptions we get the relation: $P \in L + A(F)_{tors}$ cf. [14], Theorem. We clear the torsion ambiguity in this relation using Lemma 4.1 in the same way as in the first step of the proof of Theorem 5.1. $\square$

Corollary 6.3.
Fix a rational prime l. Let A be a simple abelian variety defined over the number field F. Let $P \in A(F)$ be a point of infinite order and let $Q \in A(F)_{l-tor}$. Then there exists a set Π of primes of F of positive density, such that for $v \in \Pi$ the $l-$part of $r_v(P)$ coincides with $r_v(Q)$.

Proof. The point $P-Q$ is of infinite order. Since A is simple, the ring $\mathcal{O}\otimes\mathbb{Q}$ is a division algebra. It follows that $P-Q$ is nontorsion over $\mathcal{O}$. By Lemma 4.1 there exists a set of primes Π, with positive denstiy, such that if $v\in\Pi$, then $r_v(P-Q)=0$ in the group $A_v(\kappa_v)_l$. $\square$

The method of the proof of Theorem 5.1 provides the following two corollaries. Note that Corollary 6.5 extends Theorem 8.2 of [2] to abelian varieties with noncommutative algebras of endomorphisms.

Corollary 6.4.
The claim of Theorem 5.1 holds true, if we replace the condition: $r_v(P_0)\in r_v(L)$, *for almost all* v, *by the following: for almost all* v, *the order of* $r_v(P_0)$ *divides orders of* $r_v(P_1)$, $r_v(P_2)$, $\dots$, $r_v(P_r)$.

Proof. As in Step 1 of the proof of Theorem 5.1, assuming the condition (5.3), we show that $P\in\mathcal{O}L$. Then assuming that the condition (5.3) does not hold, we show that for infinitely many ideals v images of the points $P_1,\dots, P_r$ by the reduction r_v are not $l^{k-n+1}-$divisible, but $r_v(P_0)$ is divisible by l^{k-n+1}, for $k\geq n$ as in Step 2 of the proof of Theorem 5.1. Hence, the order of $r_v(P_0)$ does not divide the orders of $r_v(P_i)$ for those v, and for $1\leq i\leq r$, which contradicts the assumption. $\square$

Corollary 6.5.
Let A *be an abelian variety defined over a number field* F *such that* $\mathcal{O}=End_{\bar{F}}A=End_FA$ *and* $T_l(A)$ *is integrally semisimple for every prime* l. *Note that, due to Proposition 3.5, the assumption on* $T_l(A)$ *holds true for at least one variety in every nonempty isogeny class over* F. *Let* $P_1,\ Q_1,\ P_2,\ Q_2,\ \dots,\ P_r,\ Q_r\in A(F)$ *be points which are nontorsion over* $\mathcal{O}$ *such that the following condition holds true. For all sets of natural numbers* $\{m_1,m_2,\dots,m_r\}$ *and for almost all primes* v *of* $\mathcal{O}_F$: *if* $m_1r_v(P_1)+m_2r_v(P_2)+\cdots+m_rr_v(P_r)=0$, *then* $m_1r_v(P_1)+m_2r_v(Q_2)+\cdots+m_rr_v(Q_r)=0$ *in the group* $A_v(\kappa_v)$.

Then there exist endomorphisms $f_1,\ f_2,\ \dots,\ f_r{\in}\mathcal{O}$ *and torsion points* $R_1,\ R_2,\ \dots,\ R_r{\in}A(F)_{tors}$ *such that* $Q_1{=}f_1P_1+R_1,\ Q_2{=}f_2P_2+R_2,\ \dots,\ Q_r{=}f_rP_r+R_r$.

Proof. We describe the changes in the proof Theorem 5.1 which suffice to deduct Corollary 6.5. The condition (5.3) is replaced by: *Assume that for all rational primes* l, *all* $n\in\mathbb{N}$, *all* $\sigma\in\hat{H}_{l^\infty}$ *and* $1\leq i\leq r$:

$$\text{if}\quad \hat{\phi}(\hat{P}_i)(\sigma)\in l^nT_l(A),\quad\text{then}\quad \hat{\phi}(\hat{Q}_i)(\sigma)\in l^nT_l(A). \tag{6.6}$$

In the first step of the proof, we apply Proposition 3.6 to every pair of homomorphisms $\hat{\phi}(\hat{P}_j)$, $\hat{\phi}(\hat{Q}_j)$, for $1\leq i\leq r$. The first part of Step 1 of the proof of Theorem 5.1 repeats in this case, which shows that $Q_i=f_iP_i+R_i$ for $f_i\in\mathcal{O}$ and a torsion point R_i. Note that this time we can not remove the torsion ambiguity because

Lemma 4.1 does not apply. In the second step of the proof, we assume that the condition (6.6) does not hold, i.e., that there exist a prime l, a natural number n, $\sigma \in \hat{H}_{l^\infty}$ and $1 \leq j \leq r$ such that $\hat{\phi}(\hat{P}_j)(\sigma) \in l^n T_l(A)$ and $\hat{\phi}(\hat{Q}_j)(\sigma) \notin l^n T_l(A)$. Observe that to get a contradiction with the assumption of the corollary, it is enough to consider the reduction maps $r_v : A(F) \longrightarrow A_v(\kappa_v)_{l-torsion}$. In the same way as in Step 2 of the proof of Theorem 5.1, we find $k \geq n$, such that for infinitely many prime ideals v of $\mathcal{O}_F$, the order of $r_v(P_j)$ is bounded from above by l^{k-n} while the order of $r_v(Q_j)$ is bounded from below by l^{k-n+1}, and $A_v(\kappa_v)_l = (\mathbb{Z}/l^k)^{2g}$. To get the contradiction we take: $m_j = l^{k-n}$ and $m_i = l^k$, for $i \neq j$. $\square$

Remark 6.6. We conclude the paper with two naturally arising questions.

(1) Is it posssible to have integers for f_i's in the linear relation of the points in Theorem 5.1 ?
(2) Does there exist an abelian variety, defined over a number field, for which the claim of the main theorem of Introduction fails ?

Acknowledgements

The first named author would like to thank the Swiss National Science Foundation and the Alexander von Humboldt foundation for financial support during visits to the EPFL in Lausanne in September 2004 and to the Institut für Experimentelle Mathematik at Universität Duisburg-Essen in the summer of 2006, where his part of this work was done. He also thanks the Institute des Hautes Etudes Scientifiques in Bures-sur-Yvette for the hospitality and support in September 2006. The second author is pleased to acknowledge financial support of the Arithmetic Algebraic Geometry network of grants during his visit to Mathematics Department of Durham University in summer 2005.

References

[1] F.A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, vol. 290, C.R.Acad.Sci. Paris Sér. A-B, 1980, pp. A701-A703.

[2] S. Barańczuk, *On reduction maps and support problem in K-theory and abelian varieties*, preprint (2005), to appear in the Journal of Number Theory.

[3] G. Banaszak, W. Gajda, P. Krasoń, *Support problem for the intermediate jacobians of l-adic representations*, the Journal of Number Theory **100** (2003), 133-168.

[4] G. Banaszak, W. Gajda, P. Krasoń, *Detecting linear dependence by reduction maps*, the Journal of Number Theory **115** (2005), 322-342.

[5] G. Banaszak, W. Gajda, P. Krasoń, *On reduction map for the étale K-theory of curves*, Homotopy, Homology and Applications **7** (2005), 1-10.

[6] J.W.S. Cassels, A. Fröhlich (eds.), *Alegbraic Number Fields*, Academic Press, 1967.

[7] C.W. Curtis, I. Reiner, *Methodes of representation theory with applications to finite groups and orders*, vol. I, John Wiley & Sons, 1981.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. Math. **73** (1983), 349-366.

[9] G. Janusz, *Algebraic number theory*, Academic Press, London and New York, 1973.
[10] M. Larsen, R. Schoof, *Whitehead lemmas and Galois cohomology of abelian varieties*, preprint (2003).
[11] R. Pink, *On the order of reduction of a point on an abelian variety*, Math. Ann. **330** (2004), 275-291.
[12] K.A. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Mathematical Journal **46, No. 4** (1979), 745-761.
[13] J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes. II*, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 731-737.
[14] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, Acta Arithmetica **110.1** (2003), 77-88.

Department of Mathematics, Adam Mickiewicz University, Poznań, Poland

Current: IHES, Bures-sur-Yvette, France
E-mail address: gajda@amu.edu.pl

Department of Mathematics, Adam Mickiewicz University, Poznań, Poland
E-mail address: krisgorn@amu.edu.pl