LINEAR DEPENDENCE IN MORDELL-WEIL GROUPS

Wojciech Gajda and Krzysztof Górnisiewicz

Abstract. Let A be an abelian variety defined over a number field F. Let P be a point in the Mordell-Weil group $A(F)$ and H a subgroup of $A(F)$. We consider the following local-global principle which originated with the support problem of Erdös for the integers: *the point P belongs to the group H, if for almost all primes v of F, the point P (modulo v) belongs to the group H (modulo v).* We prove that the principle holds for any abelian variety A, if H is a free submodule and the point P generates a free submodule of $A(F)$ over the ring $\mathrm{End}_F\, A$.

1. Introduction.

The main result of this paper is the following

Theorem A. *[Thm. 4.1, Cor. 4.5]*
Let A be an abelian variety defined over a number field F. Let $\mathcal{O}{:=}End_F\, A$ denote the ring of F-endomorphisms of A. Let l be a prime number such that the Tate module $T_l(A)$ of A is integrally semi-simple (cf. Definition 3.1). Let $\hat{\Lambda}$ be a submodule of $A(F)\otimes\mathbb{Z}_l$ which is free over the ring $\mathcal{O}\otimes\mathbb{Z}_l$, where $\mathbb{Z}_l$ denotes the ring of l-adic integers. Let $\hat{P}\in A(F)\otimes\mathbb{Z}_l$ be a point which generates a free $\mathcal{O}\otimes\mathbb{Z}_l$-submodule of $A(F)\otimes\mathbb{Z}_l$. Then the following local-global principle holds for A, $\hat{\Lambda}$ and $\hat{P}$:

The point $\hat{P}$ is contained in $\hat{\Lambda}$, if and only if, the point $\hat{P}$ (modulo v) is contained in the group $\hat{\Lambda}$ (modulo v), for almost all primes v of F.

The same local-global principle holds for any A, l and $\hat{P}$ as above, and for any $\hat{\Lambda}$ which is torsion-free over the ring $\mathcal{O}\otimes\mathbb{Z}_l$, provided the ring $\mathcal{O}\otimes\mathbb{Q}_l$ is a division algebra and $\mathcal{O}\otimes\mathbb{Z}_l$ is a maximal order.

We prove that any abelian variety defined over F is isogeneous (over F) to an abelian variety with all Tate modules integrally semi-simple cf. Proposition 3.5. This implies the following

The research was partially financed by a KBN grant

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem B. *[Theorem 5.1]*
Let A be an abelian variety defined over a number field F. Set $\mathcal{O} := End_F A$. Let Λ be a free $\mathcal{O}-$submodule of $A(F)$. Let P be a point in $A(F)$, which generates a free $\mathcal{O}-$submodule of $A(F)$. Then the following local-global principle holds. The P point is contained in the module Λ, if and only if, the point P (modulo v) is contained in the module Λ (modulo v), for almost all primes v of F.

The question of the local-global principle for detecting by reductions if a point belongs to a given subgroup of the Mordell-Weil group of an abelian variety originated with the support problem of Erdös. This question was formulated by the first author in 2002, in a letter to Kenneth Ribet. For an abelian variety A with $\mathcal{O}=\mathbb{Z}$ and $\dim A=2, 6$ or an odd integer, the local-global principle was proven in [3], Theorem 4.2, if $H=\Lambda$ is a free subgroup and P is a non torsion point of the Mordell-Weil group $A(F)$. Note that the assumption on the dimension of the variety in *loc. cit.* can be dropped. In order to see this, it suffices in the proof of Theorem 3.12, [3] to apply the stronger Proposition 2.2, [4] instead of Theorem 3.1, [3]. More generally, if A is an abelian variety with a commutative ring of endomorphisms, then due to a result of Thomas Weston (cf. [14], Theorem) the condition P *(modulo v) belongs to H (modulo v), for almost all v*, implies the relation $P \in H+A(F)_{tors}$, for any subgroup H of $A(F)$ and $P \in A(F)$ non torsion over $\mathbb{Z}$. One should note however, that neither the method of the proof of [3], Thm. 4.2, nor of the Theorem of Weston seem to extend to abelian varieties with non commutative ring of $F-$endomorphisms.

Our proof of Theorem A is based on methods of Kummer theory for abelian varieties and Galois cohomology developed in papers [3] and [4], augmented by an idea of Larsen and Schoof used in [9]. The combination of these methods 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. When this paper was revised, we learned that Antonella Perucca proved a similar result to our Theorem B by a different method cf. [15].

The organization of the rest of the paper is as follows. In Section 2 we introduce necessary notation and basic definitions from Kummer theory for abelian varieties developed by Ribet in [12]. In Section 3, following [9], we discuss the notion of integrally semi-simple Galois modules. The proof of Theorem A is contained in Section 4. In the last section of the paper we prove Theorem B and collect few corollaries which the reader may find of independent interest. In particular, Corollary 5.6 generalizes to isogeny classes of abelian varieties the solution of the multilinear version of the support problem of Erdös obtained by Stefan Barańczuk in [2].

We would like to thank Grzegorz Banaszak for stimulating discussions and for some help with an argument in the proof of Theorem 4.1. W.G. would like to thank John Cremona, Gerhard Frey, Christian Kaiser and Don Zagier for helpful comments and remarks concerning the results of this work.

Finally, we greatfully acknowledge the work of two anonymous referees whose critical reports helped us to strengthen the results and to improve the exposition.

2. Kummer theory for abelian varieties.

Preliminaries on Galois cohomology.

Let A be an abelian variety of dimension g, defined over a number field F. We denote by $\mathcal{O}$:=End$_F A$ the ring of $F-$endomorphisms of A. For a prime number l, let $\rho_l : G_F \longrightarrow \mathrm{Gl}_{2g}(\mathbb{Z}_l)$ be the representation of the absolute Galois group $G_F := Gal(\bar{F}/F)$, which is associated with the Tate module of A at l. For $k \geq 1$, we denote by $\bar{\rho}_{l^k} : G_F \longrightarrow \mathrm{Gl}_{2g}(\mathbb{Z}/l^k)$ the residual representation attached to the action of G_F on torsion points $A[l^k] := A(\bar{F})[l^k]$. We put $V_l(A){:=}T_l(A) \otimes \mathbb{Q}_l$. Define the groups: $H_{l^k}{:=}\mathrm{ker}\bar{\rho}_{l^k}$, $H_{l^\infty}{:=}\mathrm{ker}\rho_l$, $G_{l^k}{:=}\mathrm{Im}\bar{\rho}_{l^k}$ and $G_{l^\infty}{:=}\mathrm{Im}\rho_l$ and the fields of division points on A: $F_{l^k}{:=}\bar{F}^{H_{l^k}}$ 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 Kummer exact sequence:

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

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. [5], p. 97): $\phi^{(k)}(P{+}l^k A(F))(\sigma) = \sigma(Q) - Q$, where $P \in A(F)$, $\sigma \in G_F$ and $Q \in A(\overline{F})$ is a point such that $l^k Q = P$. There are commutative diagrams:

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

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

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

(note that $A(F) \otimes \mathbb{Z}_l = \lim_{\leftarrow} A(F)/l^k A(F)$, by finite generation of the Mordell-Weil group $A(F)$, and $\lim_{\leftarrow} H^1(G_F; A[l^k]){=}H^1(G_F; T_l(A))$, by finiteness of $H^0(G_F; A[l^k])$). Consider the restriction map in Galois cohomology:

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

induced by the embedding $H_{l^\infty} \hookrightarrow G_F$. The fixed point set on the right hand side of (2.3) is computed 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 on $T_l(A)$ by definition, we have:

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

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

Proof. By the inflation-restriction sequence [5], p. 100:

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

we get $\ker(\mathrm{res}) = H^1(G_{l^\infty}; T_l(A)^{H_{l^\infty}}) = H^1(G_{l^\infty}; T_l(A))$. 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 group vanishes due to the theorem of Serre [13], Cor.1, p. 734. Hence, ker(res) is a torsion group. 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. Define the homomorphism:

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

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 $\mathrm{Hom}_{G_{l^\infty}}(H_{l^\infty}; T_l(A)) \subset \mathrm{Hom}(H_{l^\infty}; T_l(A))$, but $T_l(A)$ is a free $\mathbb{Z}_l-$module, hence $\mathrm{Hom}_{G_{l^\infty}}(H_{l^\infty}; T_l(A))$ 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 $0 = \phi(\sum_j nP_j \otimes \alpha_j) = n\phi(\sum_j P_j \otimes \alpha_j) \in \mathrm{Hom}_{G_{l^\infty}}(H_{l^\infty}; T_l(A))$, so $\phi(\sum_j P_j \otimes \alpha_j) = 0$, and $\sum_j P_j \otimes \alpha_j \in \ker\phi$. To finish the proof apply Lemma 2.4, and use the equality $(A(F) \otimes \mathbb{Z}_l)_{tors} = A(F)_{tors} \otimes \mathbb{Z}_l$. □

Kummer maps and reductions.

Let $\hat{\Lambda}$ be a finitely generated, free $\mathcal{O}_l := \mathcal{O} \otimes \mathbb{Z}_l-$submodule of $A(F) \otimes \mathbb{Z}_l$. All modules over the ring $\mathcal{O}$ (respectively, over $\mathcal{O}_l$) considered in this paper are by definition, left $\mathcal{O}-$modules (resp., left $\mathcal{O}_l-$modules). For $\hat{P} \in A(F) \otimes \mathbb{Z}_l$ and $k \in \mathbb{N}$, define the Kummer map:

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

by $\phi_{\hat{P}}^{(k)}(\sigma) = \sigma(\hat{Q}) - \hat{Q}$, where $H_{l^k} = G(\overline{F}/F_{l^k})$ and $\hat{Q} \in A(\overline{F}) \otimes \mathbb{Z}_l$ is a point such that $l^k \hat{Q} = \hat{P}$. It is easy to check that the map (2.7) does not depend on the choice of the point $\hat{Q}$. For the rest of the paper, any point $\hat{Q}$ such that $l^k \hat{Q} = \hat{P}$ will be denoted by $\frac{1}{l^k} \hat{P}$.

Remark 2.8. Note that, if $P \in A(F)$, then $\phi_{\hat{P}}^{(k)} = \mathrm{res}^{(k)}(\phi^{(k)}(P + l^k A(F)))$, where $\hat{P} = P \otimes 1$ and $\mathrm{res}^{(k)} : H^1(G_F, A[l^k]) \to H^1(H_{l^k}, A[l^k])^{G_{l^k}} = \mathrm{Hom}_{G_{l^k}}(H_{l^k}, A[l^k])$ is the restriction map in Galois cohomology.

Let us fix a basis $\hat{P}_1, \hat{P}_2, \dots, \hat{P}_r$ of the module $\hat{\Lambda}$ over the ring $\mathcal{O}_l$. We define the homomorphism: $\Phi^{(k)} : H_{l^k} \to \bigoplus_{i=1}^r A[l^k]$ by $\Phi^{(k)} = (\phi_{\hat{P}_1}^{(k)}, \phi_{\hat{P}_2}^{(k)}, \dots, \phi_{\hat{P}_r}^{(k)})$. There are commutative diagrams

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

which after passing to the inverse limit with k give the homomorphism:

$$\phi_{\hat{P}} : H_{l^\infty} \to T_l(A). \tag{2.9}$$

Observe that by Remark 2.8, for any $\hat{P} \in A(F) \otimes \mathbb{Z}_l$, we have: $\phi_{\hat{P}} = \phi(\hat{P})$. Let $\Phi : H_{l^\infty} \to \bigoplus_{i=1}^r T_l(A)$ be defined as $\Phi = (\phi_{\hat{P}_1}, \dots, \phi_{\hat{P}_r})$.

Proposition 2.10.
The image of Φ is an open subset of $\bigoplus_{i=1}^r T_l(A)$ with respect to the $l-$adic topology.

Proof. [3], Lemma 2.13.

For a prime v of good reduction for A, and for a prime number l, we denote by $\hat{r}_v$ the map $r_v \otimes \mathbb{Z}_l : A(F) \otimes \mathbb{Z}_l \longrightarrow A_v(\kappa_v)_{l-torsion}$, where $\kappa_v := \mathcal{O}_F/v$ is the residue field at v, and $r_v : A(F) \longrightarrow A_v(\kappa_v)$ is the reduction map at v.

Proposition 2.11.
Let $\hat{\Lambda}$ be a free $\mathcal{O}_l$-submodule of $A(F) \otimes \mathbb{Z}_l$. There exists a set Π of prime ideals of the ring $\mathcal{O}_F$ of algebraic integers of F, such that Π has positive density and $\hat{r}_v(\hat{\Lambda}) = 0$, for every $v \in \Pi$.

Proof. The proof is similar to the proof of Proposition 2.2 in [4]. For the convenience of the reader we give here the argument for the current setting, i.e., for the group $A(\bar{F}) \otimes \mathbb{Z}_l$. In order to simplify notation we put: $T_l = T_l(A)$, $T_l^r = \bigoplus_{i=1}^r T_l$, $A[m]^r = \bigoplus_{i=1}^r A[m]$ and $A_v(\kappa_v)_l := A_v(\kappa_v)_{l-torsion} = A_v(\kappa_v) \otimes \mathbb{Z}_l$. We fix an $\mathcal{O}_l$-basis $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_r$ of the module $\hat{\Lambda}$. Define the 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 $l^m T_l^r \subset \operatorname{Im} \Phi$. The number m exists by Proposition 2.10. For $k \geq m$, the 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 groups. 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:

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

By the theorem of Bogomolov ([1], Cor. 1, p.702), for k large enough, there exists a nontrivial homothety h in the image of ρ_l, which acts on T_l by multiplication 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 the Chebotarev theorem (cf. [8], 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:

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

The vertical maps in this diagram are natural injections. Now we proceed as in Step 4 of the proof of Proposition 2.2 in [4]. Let l^{c_i} be the order of $\hat{r}_v(\hat{P}_i) \in A_v(\kappa_v)_l$, where $c_i \geq 0$ and $i \in \{1, \ldots, r\}$. The point $\hat{Q}_i := \frac{1}{l^k}\hat{P}_i \in A(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda})) \otimes \mathbb{Z}_l$ such that $l^k\hat{Q}_i = \hat{P}_i$, maps to the point $\hat{r}_w(\hat{Q}_i) \in A_w(\kappa_w)_l$ of order l^{c_i+k}, because $l^{c_i+k}\hat{r}_w(\hat{Q}_i) = 0$. By the choice of v we get:

$$h(\hat{r}_w(\hat{Q}_i)) = (1+l^k u_0)\hat{r}_w(\hat{Q}_i),$$

where h is the homothety chosen before. The choice of v implies also that $\hat{r}_w(\hat{Q}_i) \in A_v(\kappa_v)_l$, hence $h(\hat{r}_w(\hat{Q}_i)) = \hat{r}_w(\hat{Q}_i)$, so $l^k\hat{r}_w(\hat{Q}_i) = 0$. This is possible only if $c_i = 0$. Hence, $\hat{r}_v(\hat{P}_i)$ is zero. □

Lemma 2.12.
Let $\hat{P} \in A(F) \otimes \mathbb{Z}_l$ be such that the $\mathcal{O}_l-$module $\mathcal{O}_l\hat{P}$ generated by $\hat{P}$ is free. Let $k \in \mathbb{N}$ and let $\hat{Q} \in A(\overline{F}) \otimes \mathbb{Z}_l$ be such that $l^k\hat{Q} = \hat{P}$. Let $F_{l^k}(\frac{1}{l^k}\hat{P}) := \overline{F}^{ker\,\phi_{\hat{P}}^{(k)}}$, where $\phi_{\hat{P}}^{(k)}$ is the Kummer homomorphism (2.7). Let $w \nmid l$ be a nonzero prime ideal of $\mathcal{O}_{F_{l^k}}$ at which A has good reduction. Then the following two conditions are equivalent:

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

The proof of Lemma 2.12 is an easy exercise which we leave for the reader.

3. Integrally semi-simple G_F-modules.

In this section we collect material on integrally semi-simple Galois modules following Section 4 of [9]. The main technical result in this section is Proposition 3.6, which generalizes [9], 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 semi-simple, if for every G_F-subrepresentation $W \subset V$ the exact sequence:

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

of $\mathbb{Z}_l[G_F]-$modules splits.

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 semi-simple. There exists a lattice $T \subset V$ which is an integrally semi-simple G_F-module.

Proof. Since every G_F-invariant subspace W admits a decomposition into isotypic components corresponding to the isotypic decomposition of V, without loss of generality we can assume that $V = V_1 \otimes_{\mathbb{Q}_l} \mathbb{Q}_l^k$, for an irreducible 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 semi-simple. 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:

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

Since W_0 is an $l-$divisible group, the quotient group $Q = \mathbb{Z}_l^k/(\mathbb{Z}_l^k \cap W_0)$ is torsion-free, so Q is a free group, 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. □

Observe that the representation $V_l = T_l \otimes \mathbb{Q}_l$ is semi-simple if the module T_l is integrally semi-simple 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, the Tate module $T_l(A)$ of A is integrally semi-simple.

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 $\mathcal{O} = \operatorname{End} A$ acts on M, i.e., there is an embedding $\mathcal{O} \longrightarrow \operatorname{End}(M) \cong M_{2g,2g}(\mathbb{Z})$. Let C denote the commutant of $\mathcal{O}$ in $\operatorname{End}(M)$. We put $\mathcal{O}_l := \mathcal{O} \otimes \mathbb{Z}_l$, $C_l := C \otimes \mathbb{Z}_l$. By comparison of the singular and étale cohomology we get: $\operatorname{End}_{\mathbb{Z}_l}(T_l(A)) = \operatorname{End}(M) \otimes \mathbb{Z}_l \cong M_{2g,2g}(\mathbb{Z}_l)$. By the theorem of Faltings [7], Satz 4 and Bemerkung 2, for every l, the commutant of $\mathcal{O}_l$ in $\operatorname{End}(T_l(A))$ 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 large enough, C_l is a maximal order in $C \otimes \mathbb{Q}_l$. By [6], Thm. 26.12, it follows that any finitely generated, non torsion C_l-module is projective, if l is large 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 $l \gg 0$. □

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

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 semi-simple. The vector space $T_l(A) \otimes \mathbb{Q}_l$ contains a lattice Λ which is integrally semi-simple 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 $B = A/D$. □

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

$$\alpha : M \longrightarrow \bigoplus_{i=1}^{r} N \quad \textit{and} \quad \beta : M \to N$$

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

$$\textit{if} \quad \alpha(m) \in l^k(\bigoplus_{i=1}^{r} N), \quad \textit{then} \quad \beta(m) \in l^k N.$$

Then there exists a homomorphism of $\mathbb{Z}_l[G_F]-$modules: $\gamma : \bigoplus_{i=1}^r N \to N$ such that $\gamma \circ \alpha = \beta$.

Proof. We put: $W_\alpha := \operatorname{Im} \alpha \otimes \mathbb{Q}_l$, $W_\beta := \operatorname{Im} \beta \otimes \mathbb{Q}_l$ and $V := \bigoplus_{i=1}^r N \otimes \mathbb{Q}_l$. Since $\bigcap_{k=1}^\infty l^k M{=}0$, by assumption, if $\alpha(m){=}0$, 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 semi-simple, the $\mathbb{Z}_l[G_F]-$module, $\bigoplus_{i=1}^r N$ is also integrally semi-simple 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 (and hence also γ) has trivial restriction to 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 assumption $\beta(m) \in l^k N$, hence:

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

4. Proof of Main Theorem.

Theorem 4.1.
Let A be an abelian variety defined over a number field F. Let $\mathcal{O}{:=}End_F\, A$ denote the ring of F-endomorphisms of A. Let l be a prime number with the following

properties. We assume that the Tate module $T_l(A)$ of A at l is an integrally semisimple G_F-module. Let $\hat{\Lambda}$ be a submodule of $A(F)\otimes\mathbb{Z}_l$ which is free over the ring $\mathcal{O}_l{:=}\mathcal{O}\otimes\mathbb{Z}_l$. Let $\hat{P}\in A(F)\otimes\mathbb{Z}_l$ be a point for which the cyclic module $\mathcal{O}_l\hat{P}$ is free over the ring $\mathcal{O}_l$. Then the following local-global principle holds for: A, $\hat{\Lambda}$ and $\hat{P}$. The point $\hat{P}$ is contained in $\hat{\Lambda}$, if and only if, the point $\hat{r}_v(\hat{P})$ is contained in the group $\hat{r}_v(\hat{\Lambda})$, for almost all primes v of F.

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

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

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 $\hat{H}_{l^\infty}\longrightarrow T_l(A)$ of $\mathbb{Z}_l-$modules. Hence, the Kummer map ϕ of Definition 2.5 induces a homomorphism of $\mathbb{Z}_l-$modules:

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

such that the following diagram commutes.

(4.2)

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

The proof of the theorem will be in 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.
For a basis $\hat{P}_1,\hat{P}_2,\dots,\hat{P}_r$ of the $\mathcal{O}_l$-module $\hat{\Lambda}$ we denote by $\hat{\Phi}:\hat{H}_{l^\infty}\longrightarrow\bigoplus_{i=1}^{r}T_l(A)$ the map $\hat{\Phi}=(\hat{\phi}(\hat{P}_1),\dots,\hat{\phi}(\hat{P}_r))$. In the first step of the proof, we assume that for every basis $\hat{P}_1$, $\hat{P}_2$, $\dots$, $\hat{P}_r$ of the $\mathcal{O}_l$-module $\hat{\Lambda}$, for every $n\in\mathbb{N}$, and for every $\sigma\in\hat{H}_{l^\infty}$:

$$\text{(4.3)}\qquad \text{if}\quad \hat{\Phi}(\sigma)\in l^n(\bigoplus_{i=1}^{r}T_l(A)),\quad\text{then}\quad \hat{\phi}(\hat{P})(\sigma)\in l^nT_l(A).$$

We apply Proposition 3.6 to $M = \operatorname{Im}\hat{\Phi}$, $N = T_l(A)$, $\alpha = \hat{\Phi}$, and $\beta = \hat{\phi}(\hat{P})$. It implies that there is a homomorphism $g : \bigoplus_{i=1}^{r} T_l(A) \longrightarrow T_l(A)$ of $\mathbb{Z}_l[G_F]-$modules such that $g \circ \hat{\Phi}{=}\hat{\phi}(\hat{P})$. 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 of the direct sum $\bigoplus_{i=1}^{r} T_l(A)$. Hence, g_i is an $\mathbb{Z}_l[G_F]-$endomorphism of the module $T_l(A)$ and we have: $\sum_{i=1}^{r} g_i\hat{\phi}(\hat{P}_i) = \hat{\phi}(\hat{P})$. By the theorem of Faltings [7], Satz 4: $\operatorname{End}_{\mathbb{Z}_l[G_F]}(T_l(A)) \cong \mathcal{O}_l$. It follows that there is an element $\hat{f}_i \in \mathcal{O}_l$ 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 get:

$$\hat{\phi}(\sum_{i=1}^{r} \hat{f}_i\hat{P}_i) = \hat{\phi}(\hat{P}). \tag{4.4}$$

The diagram (4.2) and Lemma 2.6 imply that: $\ker\hat{\phi} \subset A(F)_{tors} \otimes \mathbb{Z}_l$. Hence, by (4.4): $\hat{P} = \sum_{i=1}^{r} \hat{f}_i\hat{P}_i + \hat{R}$ for some $\hat{R} \in A(F)_{tors} \otimes \mathbb{Z}_l$. To complete the first step of the proof, it is enough to show that $\hat{R} = 0$. By Proposition 2.11, there exist infinitely many v (even positive density) such that $\hat{r}_v(\hat{\Lambda}) = 0$. In particular $\hat{r}_v(\hat{Q}) = 0$ and also $\hat{r}_v(\hat{P}) = 0$ because $\hat{r}_v(\hat{P}) \in \hat{r}_v(\hat{\Lambda})$, by assumption. Hence, $\hat{r}_v(\hat{R}) = 0$, for infinitely many v. This implies that $\hat{R} = 0$, as it is well-known that, for almost all v, the restriction of the reduction map $\hat{r}_v$ to $A(F)_{tors} \otimes \mathbb{Z}_l$ is an injection.

Step 2.
We assume to the contrary that the condition (4.3) does not hold, i.e., that there exist: a basis $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_r$ of the $\mathcal{O}_l$-module $\hat{\Lambda}$, a natural number n and $\sigma \in \hat{H}_{l^\infty}$ such that

$$\hat{\Phi}(\sigma) \in l^n(\bigoplus_{i=1}^{r} T_l(A)) \quad \text{and} \quad \hat{\phi}(\hat{P})(\sigma) \notin l^nT_l(A).$$

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 $T_l(A)/l^nT_l(A){=}A[l^n]$, it follows by the definition of $\hat{\phi}(\hat{P})$ that $\tilde{\sigma}$ acts trivially on the points $\frac{1}{l^n}\hat{P}_1, \ldots, \frac{1}{l^n}\hat{P}_r$, and acts non trivially on the points $\frac{1}{l^n}\hat{P}$. Define the field $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P}) := F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda})F_{l^\infty}(\frac{1}{l^\infty}\hat{P})$. Consider the open set in the group $G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P})/F)$ consisting of elements which act in the same way as $\bar{\sigma} := \tilde{\sigma}|_{F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P})}$. 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 $\alpha \in \mathbb{Z}_l^\times$ is congruent to 1 modulo l. Lifting τ to a homothety $h \in G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}, \frac{1}{l^\infty}\hat{P})/F)$, we define the element $\gamma := h^{l^k}\bar{\sigma}$ which has the desired property, if k is sufficiently large. Next, we apply the Chebotarev density theorem to choose infinitely many prime ideals v in $\mathcal{O}_F$ in such a way that the Frobenius element Fr_v is close enough to γ, so Fr_v acts trivially on points of $A[l^k]$ and on points $\frac{1}{l^n}\hat{P}_i$ for $1 \leq i \leq r$, but acts non-trivially on all points $\frac{1}{l^n}\hat{P}$. 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, we obtain $A_v(\kappa_v)_l = (\mathbb{Z}/l^k)^{2g}$. It follows by Lemma 2.12 that the elements $\hat{r}_v(\hat{P}_1), \dots, \hat{r}_v(\hat{P}_r)$ are divisible by l^n, and that $\hat{r}_v(\hat{P})$ is not l^n-divisible in the group $A_v(\kappa_v)_l$. Hence, the orders of $\hat{r}_v(\hat{P}_1), \dots, \hat{r}_v(\hat{P}_r)$ 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 $\hat{r}_v(\hat{P})$ 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, $\hat{r}_v(\hat{P}) \notin \hat{r}_v(\hat{\Lambda})$, for infinitely many v, contrary to the assumption of the theorem. □

We are indebted to the referee for the following observation.

Corollary 4.5.
The same local-global principle holds for any A, l and $\hat{P}$ as in Theorem 4.1, and for any $\hat{\Lambda}$ which is torsion-free over the ring $\mathcal{O}_l$, provided that the ring $\mathcal{O} \otimes \mathbb{Q}_l$ is a division algebra and $\mathcal{O}_l$ is its maximal order.

Proof. This is an immediate corollary of Theorem 4.1, since any torsion-free, finitely generated module over the maximal $\mathbb{Z}_l-$order $\mathcal{O}_l$ contained in the division $\mathbb{Q}_l-$algebra $\mathcal{O} \otimes \mathbb{Q}_l$, is a free $\mathcal{O}_l-$module cf. [11], Exercise 1, p.181. □

5. Corollaries.

Theorem 5.1.
Let A be an abelian variety defined over a number field F. Let Λ be a free $\mathcal{O}-$submodule of $A(F)$. Let P be a point in $A(F)$, such that the module $\mathcal{O}P$ is free over $\mathcal{O}$. Then the following local-global principle holds. The point P is contained in the module Λ, if and only if, the point $r_v(P)$ is contained in the module $r_v(\Lambda)$, for almost all primes v of F.

Proof. If P belongs to Λ, then $r_v(P)$ belongs to $r_v(\Lambda)$, for all primes v of F because r_v is a group homomorphism. In order to prove that the converse implication holds, we assume that $r_v(P) \in r_v(\Lambda)$, for almost all v. Fix a prime number l. Let $\alpha : A \longrightarrow B$ be an $F-$isogeny, where B is an abelian variety over F for which the Tate module $T_l(B)$ is integrally semi-simple. The isogeny α was constructed in the proof of Proposition 3.5. Note that the degree of α is a power of l. We put deg(α)= l^m. To simplify notation, we use the same letters to denote an $F-$isogeny and the associated group homomorphism on the $F-$points. We apply Theorem 4.1 to: the variety B, the point $\widehat{\alpha(P)}$:=$\alpha(P)\otimes 1$, and the module $\widehat{\alpha(\Lambda)}$:=$\alpha(\Lambda) \otimes \mathbb{Z}_l$. It is easy to verify that the assumptions are satisfied in this case. In particular, the module $\mathcal{O}_l\hat{P}$ where $\hat{P}$:=$P\otimes 1$, is free over $\mathcal{O}_l$ because the $\mathcal{O}-$module $\mathcal{O}P$ is free, by assumption. This implies that the cyclic module generated by the point $\widehat{\alpha(P)}$ over the ring $\mathrm{End}_F B \otimes \mathbb{Z}_l$ is free, as well. Hence, by Theorem 4.1 the point $\widehat{\alpha(P)}$

belongs to the module $\widehat{\alpha(\Lambda)}$. Let $\beta : B \longrightarrow A$ be the unique $F-$isogeny such that the compositions $\beta \circ \alpha$ and $\alpha \circ \beta$ are multiplications by l^m. By applying the map $\beta \otimes 1$ to the relation $\widehat{\alpha(P)} \in \widehat{\alpha(\Lambda)}$ we obtain the equation: $\hat{P} = \hat{Q} + \hat{R}$, for some $\hat{Q} \in \hat{\Lambda}$ and $\hat{R} \in A[l^m] \otimes \mathbb{Z}_l$. We prove that $\hat{R} = 0$ using Proposition 2.11, as in the first step of the proof of Theorem 4.1. This shows that the point $\hat{P} = P \otimes 1$ belongs to $\hat{\Lambda} = \Lambda \otimes \mathbb{Z}_l$, for every l. To prove that the point P belongs to the module Λ, it suffices to consider the subgroup X of the quotient group $A(F)/\Lambda$ generated by the coset of P, and use the fact that $X = 0$, if and only if, $X \otimes \mathbb{Z}_l = 0$, for every prime number l.

Remark 5.2. One can prove the local-global principle for detecting an inclusion between two free $\mathcal{O}$-submodules of $A(F)$ by reduction maps, by using the method of the proof of Theorem 5.1. We are indebted to John Cremona for this observation.

Remark 5.3. Weston showed in [14] that, if A is an abelian variety with a commutative ring of $F-$endomorphisms, then for any subgroup H and any point P in $A(F)$, the relation $P \in H + A(F)_{tors}$ holds, provided $r_v(P)$ belongs to $r_v(H)$, for almost all primes v. One can clear the torsion ambiguity in the statement of Weston's theorem by using Proposition 2.11, if H and $P\mathcal{O}$ are free $\mathcal{O}-$submodules of $A(F)$, as in the first step of the proof of Theorem 4.1.

Remark 5.4. Proposition 2.11 gives a proof of the following result of Richard Pink, which was proven in [10], Prop. 4.1 by another method: *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 $Q \in A(F)_{l-tors}$. 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* $r_v(Q)$. In order to see this, observe that the point $P - Q$ is of infinite order, and that the ring $\mathcal{O} \otimes \mathbb{Q}$ is a division algebra. It follows that $P - Q$ is nontorsion over $\mathcal{O}$. By Proposition 2.11 there exists a set of primes Π, with positive density, such that, if $v \in \Pi$, then $\hat{r}_v(\hat{P} - \hat{Q}) = 0$ in the group $A_v(\kappa_v)_{l-tors}$.

The method of the proof of Theorem 5.1 provides the following two corollaries. Note that Corollary 5.6 extends Theorem 8.2 of [2] to abelian varieties with non commutative algebras of endomorphisms.

Corollary 5.5.
The claim of Theorem 5.1 holds true, if we replace the condition: $r_v(P) \in r_v(\Lambda)$, *for almost all* v, by the following: *the order of $r_v(P)$ divides the orders of $r_v(P_1)$, $r_v(P_2)$, ..., $r_v(P_r)$ in the group $A_v(\kappa_v)$, where P_1, P_2, ..., P_r is an $\mathcal{O}-$basis of the free module* Λ.

Proof. The proof is very similar to the proof of Theorem 5.1. For a prime number l, we put $\hat{P} := P \otimes 1$, $\hat{P}_i := P_i \otimes 1$, for $1 \leq i \leq r$, and $\hat{\Lambda} := \Lambda \otimes \mathbb{Z}_l$. First we have to modify the argument in the proof of Theorem 4.1. In Step 1 of the proof, assuming the condition (4.3), we show that if the order of $\hat{r}_v(\hat{P})$ divides the orders of $\hat{r}_v(\hat{P}_1)$, $\hat{r}_v(\hat{P}_2)$, ..., $\hat{r}_v(\hat{P}_r)$ for almost all v, then the point $\hat{P} \in \hat{\Lambda}$. Then assuming that the condition (4.3) does not hold, we show that there exist infinitely many prime ideals v, such that the images of the points $\hat{P}_1, \dots, \hat{P}_r$ by the reduction $\hat{r}_v$ are not $l^{k-n+1}-$divisible, but $\hat{r}_v(\hat{P})$ is divisible by l^{k-n+1}, for $k \geq n$ chosen as in Step 2 of the proof of Theorem 4.1. Hence, the order of $\hat{r}_v(\hat{P})$ is larger then the orders of $\hat{r}_v(\hat{P}_i)$, for those v, and for $1 \leq i \leq r$, which contradicts the assumption of the corollary. The rest of the proof repeats the argument of the proof of Theorem 5.1. □

Corollary 5.6.
In every isogeny class of abelian varieties defined over a number field F there exists an abelian variety A with the following property. Set $\mathcal{O}{=}End_F A$. Let P_1, Q_1, P_2, Q_2, $\dots$, P_r, $Q_r \in A(F)$ be points which generate free modules over $\mathcal{O}$ and such that the following condition holds. For all sets of natural numbers $\{m_1, m_2, \dots, m_r\}$, for almost all v, in the group $A_v(\kappa_v)$ we have:

if $\sum_{i=1}^r m_i r_v(P_i) = 0$, *then* $\sum_{i=1}^r m_i r_v(Q_i) = 0$.

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. Let A be an abelian variety for which all Tate modules are integrally semisimple. Such an abelian variety exists in every isogeny class by Proposition 3.5. We describe the changes in the proofs of Theorem 4.1 and Theorem 5.1 which suffice to deduce Corollary 5.6. The condition (4.3) is being replaced by: *Assume that for: all prime numbers l, all $n \in \mathbb{N}$, all $\sigma \in \hat{H}_{l^\infty}$, and $1 \leq i \leq r$:*

$$\text{(5.7)} \qquad \text{if} \quad \hat{\phi}(\hat{P}_i)(\sigma) \in l^n T_l(A), \quad \text{then} \quad \hat{\phi}(\hat{Q}_i)(\sigma) \in l^n T_l(A),$$

where $\hat{P}_i{:=}P_i \otimes 1$ and $\hat{Q}_i{:=}Q_i \otimes 1$, for $1 \leq i \leq r$. 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 4.1 repeats in this case, which shows that, for every l, $\hat{Q}_i = \hat{f}_i\hat{P}_i + \hat{R}_i$, for $\hat{f}_i \in \mathcal{O}_l$, a torsion point $\hat{R}_i$, and for every $1 \leq i \leq r$. This implies that $P_i \in \mathcal{O}Q_i + A(F)_{tors}$, for $1 \leq i \leq r$ (if the condition (5.7) holds). Note that this time we can not remove the torsion ambiguity because Proposition 2.11 does not apply. In the second step of the proof, we assume that the condition (5.7) does not hold for A and a prime l, i.e., there exists a natural number n, an element $\sigma \in \hat{H}_{l^\infty}$ and an index $1 \leq j \leq r$ 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 suffices to consider the reduction maps $\hat{r}_v : A(F) \otimes \mathbb{Z}_l \longrightarrow A_v(\kappa_v)_{l-torsion}$. In the same way as in Step 2 of the proof of Theorem 4.1, we find $k \geq n$, such that for infinitely many prime ideals v of $\mathcal{O}_F$, the order of $\hat{r}_v(\hat{P}_j)$ is bounded from above by l^{k-n} while the order of $\hat{r}_v(\hat{Q}_j)$ 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 $i \neq j$. □

Acknowledgements

The first author would like to thank the Swiss National Science Foundation, the Alexander von Humboldt foundation, the I.H.E.S., and the Max Planck Gesellschaft for financial support during visits to the EPFL in Lausanne, the Institut für Experimentalle Mathematik in Essen, Burres-sur-Yvette, and the MPI in Bonn, respectively, on various occasions between September 2004 and July 2007, when the work on this project continued. 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, *Detecting linear dependence by reduction maps*, the Journal of Number Theory **115** (2005), 322-342.

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

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

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

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

[8] G. Janusz, *Algebraic number theory*, Academic Press, London and New York, 1973.

[9] M. Larsen, R. Schoof, *Whitehead lemmas and Galois cohomology of abelian varieties*, preprint (2003).

[10] R. Pink, *On the order of reduction of a point on an abelian variety*, Math. Ann. **330** (2004), 275-291.

[11] I. Reiner, *Maximal Orders*, Academic Press, London and New York, 1975.

[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.

[15] A. Perucca, *The l-adic support problem for abelian varieties*, in preparation.

Department of Mathematics, Adam Mickiewicz University, Umultowska 87, 61614 Poznań, Poland

the Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany
E-mail address: gajda@amu.edu.pl

Department of Mathematics, Adam Mickiewicz University, Umultowska 87, 61614 Poznań, Poland
E-mail address: krisgorn@amu.edu.pl