Functiones et Approximatio
52.1 (2015), 83–107
doi: 10.7169/facm/2015.52.1.7

LINEAR RELATIONS AND ARITHMETIC ON ABELIAN SCHEMES

Piotr Rzonsowski

Abstract: We investigate linear relations in Mordell-Weil groups of abelian varieties over finitely generated fields over $\mathbb{Q}$. Based on important and classical results for abelian varieties over these fields and on lifts of abelian varieties to suitable abelian schemes, we prove theorems concerning the reduction maps on torsion and non-torsion elements in Mordell-Weil groups of these varieties. These theorems and the arithmetic of abelian schemes and their endomorphism algebras are our key tools in the solutions of linear relation problems we work with in the last chapter of this paper.

Keywords: abelian variety, abelian scheme, Mordell–Weil group, support problem.

1. Introduction

Let A/K be an abelian variety over finitely generated field extension $K/\mathbb{Q}$. The abelian variety A/K extends to an abelian group scheme $\mathcal{A}/S$ over an integral scheme $S = \operatorname{Spec} R$ such that $S \to \operatorname{Spec} \mathbb{Z}$ is a smooth morphism (cf [F2, p. 204]). The smoothness of $S \to \operatorname{Spec} \mathbb{Z}$ implies that S is normal scheme [ST, Lemma 33.14.2]. Hence, restricting to an open subset of S (cf. [Co] Rem 20.9 p. 148 and Remark 2.1 below), we observe that A/K extends to a projective abelian group scheme $\mathcal{A}/S$ over an integral scheme $S = \operatorname{Spec} R$ such that $S \to \operatorname{Spec} \mathbb{Z}$ is smooth. The ring R is a finitely generated $\mathbb{Z}$-algebra, K is its field of fractions and A/K is the generic fiber of $\mathcal{A}/S$. Since $A(K)$ is finitely generated we can choose S (restricting to an open subset) such that the natural map $\mathcal{A}(S) \to A(K)$ is surjective. This map is also injective since $\mathcal{A}/S$ is proper, hence separated.

For every point $s \in S$ there is a well defined reduction map $r_s : \mathcal{A}(S) \to \mathcal{A}_s\,(k(s))$. In this paper we investigate linear relations among nontorsion points in the Mordell-Weil group $A(K)$ by use of the reduction map $r_v : \mathcal{A}(S) \to \mathcal{A}_v(k_v)$

2010 Mathematics Subject Classification: primary: P11G10; secondary: 14G05, 14L15, 14Kxx for the closed points $v \in S$. Let us present below our main results of this paper and recall the origins of the problems we investigate. In 1975 A. Schinzel proved the following theorem.

Theorem ([Sch]). *Let F be a number field and let $\gamma, \gamma_1, \dots, \gamma_r \in \mathcal{O}_{F,S_0}^{\times}$ for some finite set S_0 of primes of $\mathcal{O}_F$. Suppose that for every $v \notin S_0$ the following congruence holds $\gamma \equiv \gamma_1^{n_{1,v}} \dots \gamma_r^{n_{r,v}} \mod v$ for some $n_{1,v}, \dots, n_{r,v} \in \mathbb{Z}$. Then the exist $n_1, \dots, n_r \in \mathbb{Z}$ such that $\gamma = \gamma_1^{n_1} \dots \gamma_r^{n_r}$ in $F^{\times}$.*

In 2002 C. Khare proved the theorem of Schinzel by different methods [Kh] and used this to investigate l-adic representations. Based on this in 2002 W. Gajda asked the following question:

Question. Let F be a number field. Let A/F be an abelian variety and $P \in A(F)$. Let Λ be a subgroup of $A(F)$. Suppose that for almost all $v \in \operatorname{Spec} \mathcal{O}_F$ the following condition holds

$$r_v(P) \in r_v(\Lambda).$$

Does it imply that $P \in \Lambda$?

This question has recently attracted attention of a number of mathematicians and many results were obtained in the direction of solving this question: ([B], [BGK1], [BGK2], [BK], [GG], [J], [K], [Pe1]), [We]. Nevertheless this question does not have a positive solution in full generality and explicit counterexamples to this question were presented in [BK], Section 6 and [JP].

In our paper we extend this question to abelian varieties over finitely generated field extensions $K/\mathbb{Q}$ and we prove the following theorem:

Theorem (Thm 7.2). *Let A be an abelian variety over K and $P, P_1, \dots, P_r$ be nontorsion points in $A(K)$. Let $P_1, \dots P_r$ be linearly independent over $\mathcal{R} := End_K(A)$ and Λ be a $\mathbb{Z}$-submodule generated by $P_1, P_2, \dots, P_r$. Assume that*

$$r_v(P) \in r_v(\Lambda)$$

for all closed points v in U where $U \subset S$ is an open subset. Then $P \in \Lambda$.

Theorem 7.2 in the case of a number field F with some extra assumption that $\mathcal{R}P$ is a free $\mathcal{R}$-module has been proven by G. Banaszak [B]. In the number field case this assumption was removed by P. Perruca.

The original inspiration of my next results is the following question formulated in 1988 by Paul Erdös. This question is called the *support problem*:

Question. Let $\operatorname{Supp}(n)$ denote the support of a natural number n, i.e. the set of all prime numbers dividing n. Suppose that for some positive integers x, y the following condition holds

$$\operatorname{Supp}(x^n - 1) = \operatorname{Supp}(y^n - 1)$$

for every natural number n. Does then $x = y$?

This question and its analogues for number fields and for elliptic curves over number fields has been solved by Corrales-Rodrigáñez and Schoof [C-RS]. The support problem for abelian varieties over number fields has been recently intensively investigated in many papers [BGK3], [KP], [Bar], [GG], [Lar], [Pe1]. The most general result was obtained by M. Larsen [Lar]. We prove that Larsen's result holds in the general case of abelian varieties over finitely generated fields.

Theorem (Cor 8.5). *Let A/K be an abelian variety defined over K. Let $P, Q \in A(K)$ be two given points. Suppose that there is an open subset $U \subset S$ such that for all $n \in \mathbb{Z}$ and all closed points $v \in U$, the following condition holds*

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0.$$

Then there exist a positive integer k and an endomorphism
$\varphi \in \operatorname{End}_K A \setminus \{0\}$ such that

$$\varphi(P) = kQ.$$

In adition we also prove in this general case the following theorem which is a vast generalization of a problem suggested to G. Banaszak by A. Schinzel in 1998 in the number field case. This theorem for abelian varieties over number fields, with commutative endomorphism ring that is a domain, was proved by S. Baranczuk [Bar].

Theorem. *Let A/K be an abelian variety defined over K.*
Let $P_0, P_1, \ldots, P_n, Q_0, Q_1, \ldots, Q_n \in A(K)$ be the points of infinite order. Assume that the following condition holds:

There is an open set $U \subset S$ such that for every set of nonnegative integers $m_1, \ldots, m_n$ and for all closed points $v \in U$, the following condition holds.

$$r_v(P_0) = \sum_{i=1}^{n} m_i r_v(P_i) \qquad \textit{implies} \qquad r_v(Q_0) = \sum_{i=1}^{n} m_i r_v(Q_i)$$

Then there exist $\alpha_i \in \operatorname{End}_K(A) \setminus \{0\}$ and $k_i \in \mathbb{N} \setminus \{0\}$ such that $\alpha_i P_i = k_i Q_i$ for all $i = 0, 1, \ldots, n$.

The main technical results of the paper are Theorems 2.3, 6.3 and 6.4, which allow us to control images of torsion and nontorsion points via reduction maps. These theorems, based on numerous results concerning the arithmetic of abelian schemes and the properties of endomorphism rings $\operatorname{End}_K(A)$ are very useful tools in this paper. Moreover these theorems make the proofs of our main results very straightforward and in some cases even simpler then the corresponding results in the number field case.

Acknowledgements. This paper is part of my Ph. D. thesis. I thank my thesis advisor G. Banaszak for many suggestions, comments and encouragement. I also thank J.P. Serre, D. Ulmer and Y. Zarhin who shared with my thesis advisor very important information concerning the arithmetic of abelian varieties. This information was very crucial for my thesis. The research was financed by a grant of Polish Ministry of Science and Education no. 5289/B/H03/2010/38.

Notation

l	is a prime number
F	is a number field
K	is finitely generated fields over $\mathbb{Q}$
C_l	$:= \bigcup_{k\geqslant 1} C[l^k]$ the l-primary part of an abelian group C
S	is a base scheme
R	is finitely generated $\mathbb{Z}-$ algebra such that K is fraction field
$\mathcal{A}_s$	$= \mathcal{A} \times_S \operatorname{Spec} k(s)$
$T_l(A)$	Tate module
K_{l^k}	$= K(A_l[l^k]),$ for any $k > 0$
K_{l^∞}	$:= K(A[l^\infty])$
H_{l^∞}	$:= G(\overline{K}/K_{l^\infty})$
H_{l^k}	$:= G(\overline{K}/K_{l^k})$
G_K	$= G(\overline{K}/K)$
G_{l^k}	$= G(K_{l^k}/K)$
G_{l^∞}	$= G(K_{l^\infty}/K)$
g_s	$= G_{k(s)} = G(\overline{k(s)}/k(s))$

2. Galois and Kummer theory of abelian schemes

Let $\mathcal{A}/S$ be an abelian scheme over a base scheme S (see [FC] Chap. I, [Mi1] Chap. 20). If $s \in S$ is a point, not necessarily closed then $\mathcal{A}_s := \mathcal{A} \times_S \operatorname{Spec} k(s)$ denotes the fibre of $\mathcal{A}/S$ at s. By the properties of abelian schemes and universality of fibre product we get the reduction map homomorphism

$$r_s : \mathcal{A}(S) \to \mathcal{A}_s(k(s))$$

Take a point $\tilde{P} \in \mathcal{A}(S)$. It is given by a section $\tilde{P} : S \to \mathcal{A}$ of the map $\mathcal{A} \to S$. Let l be prime to the residue characteristics of S. The multiplication by l^k on $\mathcal{A}/S$ is an étale map [Mi2, Prop. 20.7]. Hence the pull back of the l^k-multiplication map by the map $\tilde{P}$:

$$\begin{tikzcd} \frac{1}{l^k}\tilde{P} \arrow[r] \arrow[d] & S \arrow[d, "\tilde{P}"] \\ \mathcal{A} \arrow[r, "l^k"] & \mathcal{A} \end{tikzcd} \tag{2.1}$$

gives a finite scheme $\frac{1}{l^k}\tilde{P}$ which is étale over S. In particular if $\tilde{e} := S \to \mathcal{A}$ is the the unit section then $\mathcal{A}[l^k] := \frac{1}{l^k}\tilde{e}$ is a finite group scheme, étale over S, of order l^{2gk}. So if the base scheme S is integral by the universality of fiber product one can also check that for any point $s \in S$ there is a natural isomorphism $\frac{1}{l^k}\tilde{P} \times_S \operatorname{Spec} k(s) \cong \frac{1}{l^k} r_s(\tilde{P})$. Hence if K is the function field of S and A/K is the generic fibre of $\mathcal{A}/S$ then $\mathcal{A}[l^k] \times_S \operatorname{Spec} K \cong A[l^k]$. Let S be a normal integral scheme. Consider all finite extensions of L/K and $L \subset \overline{K}_s$ such that the normalization S' of S in L gives an extension of schemes S'/S, unramified at all points of S. If K^{ur} denotes the union of all such fields L in $\overline{K}_s$ then by [Mi1] I, Example 5.2 (b) $\pi_1(S) := \pi_1(S, \eta) = G(K^{ur}/K)$. In particular if $S = \operatorname{Spec} R$ is an affinie scheme with R normal in K and L is such that the integral closure R' of R in L gives an affine scheme $S' = \operatorname{Spec} R'$ unramified over S we can define R^{ur} to be the union of all the rings R'. Then $\widetilde{S} := \operatorname{Spec} R^{ur}$ will be called the universal cover of S.

Put for simplicity $G_K := G(\overline{K}/K)$ and $g_s := G_{k(s)} = G(\overline{k(s)}/k(s))$. There is the following commutative diagram:

$$\begin{tikzcd}
A(K)_l \arrow[d] & \mathcal{A}(S)_l \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d] & \mathcal{A}_s(k(s))_l \arrow[d] \\
\varprojlim_k A(K)/l^k \arrow[d] & \varprojlim_k \mathcal{A}(S)/l^k \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d] & \varprojlim_k \mathcal{A}_s(k(s))/l^k \arrow[d] \\
H^1(G_K, T_l(A))_l \arrow[d, "="] & H^1(\pi_1(S), T_l(\mathcal{A}))_l \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d, "="] & H^1(g_s, T_l(\mathcal{A}_s))_l \arrow[d, "="] \\
H^0(G_K, A[l^\infty])/Div & H^0(\pi_1(S), \mathcal{A}[l^\infty])/Div \arrow[l, "r_\eta"'] \arrow[r, "r_s"] & H^0(g_s, \mathcal{A}_s[l^\infty])/Div
\end{tikzcd}$$

where Div denotes the maximal divisible subgroup in an appropriate group. We also used often in the diagram the notation C_l for the l-torsion part of an abelian group C (see the Notation at the end of the introduction).

Remark 2.1. If A/K is an abelian variety over a field K then A is projective, say $A \subset \mathbb{P}^n$. If K is the function field of an integral noetherian scheme S then we can take the Zariski closure of A in $\mathbb{P}^n/S$ to get a projective scheme $\mathcal{A}/S$. Over some open subset $U \subset S$ the scheme $\mathcal{A}/U$ will become a projective abelian scheme (see [Mi1] Remark 20.9.)

Remark 2.2. If $\mathcal{A}/S$ is an abelian scheme over an integral base scheme S, and $\tilde{S} \to S$ is the normalization of S we can change the base to get an abelian scheme $\tilde{\mathcal{A}} := \mathcal{A} \times_S \tilde{S}$ over a normal base scheme $\tilde{S}$. Hence we can find an open subset $\tilde{U} \subset \tilde{S}$ such that $\tilde{\mathcal{A}}/\tilde{U}$ is a projective abelian scheme over an integral normal base scheme $\tilde{U}$.

Theorem 2.3 (Banaszak). *Let $\mathcal{A}/S$ be an abelian scheme over an integral, normal base scheme S with generic fibre A/K. Let l be prime to the residue characteristics of S. Let $s \in S$ be a point of S. Assume that $H^0(g_s, \mathcal{A}_s[l^\infty])$ is finite. Then the natural map*

$$r_s : \mathcal{A}(S)_l \to \mathcal{A}_s(k(s))_l$$

is a monomorphism.

Proof. Since the finite group scheme $\mathcal{A}[l^k] = A[l^k]$ is étale over S for all $k \geqslant 1$ then the action of G_K on $A[l^k]$ factors through the action of $\pi_1(S) = G(K^{ur}/K)$.

Since $\mathcal{A}[l^k]/S$ is a finite étale scheme over S for every $k \geqslant 1$, then $G(K(A[l^\infty])/K)$ is a quotient of $\pi_1(S)$ and $G(k_s(\mathcal{A}_s[l^\infty])/k_s)$ is a quotient of $G(K(A[l^\infty])/K)$. For every $s \in S$ we have $Div = 0$ in $H^0(g_s, \mathcal{A}_s[l^\infty])$ by finiteness assumption. Hence the bottom right horizontal arrow in the diagram above is an embedding. In the diagram above the upper vertical arrows are monomorphism by the appropriate cohomology long exact sequences application. The bottom vertical maps are equalities by the Theorem of Tate [T, Proposition 2.3 p. 261]. ■

Let $S := \operatorname{Spec} R$. Assume that S is an integral, normal base scheme. Let $\mathcal{A}/S$ be an abelian scheme whose generic fibre is abelian variety A/K. We put $\mathcal{A}(R) := \mathcal{A}(S)$. Assume that S is such that all points of $A(K)$ lift to $\mathcal{A}(S)$. In other words we assume that the natural map

$$\mathcal{A}(S) \to A(K) \tag{2.2}$$

is surjective. This map is also injective since $\mathcal{A}/S$ is proper, hence separated. Hence the reduction map can be written as follows:

$$r_s : A(K) \to \mathcal{A}_s(k(s)).$$

Taking further R to be a finitely generated $\mathbb{Z}$-algebra its field of fractions K is a finitely generated field over $\mathbb{Q}$. Since in this case $A(K)$ is finitely generated by Mordell-Weil and Lang-Néron (see Theorem 5.1) we can find an open subset $U \subset S$ such that the natural map

$$\mathcal{A}(U) \to A(K) \tag{2.3}$$

is surjective. Since base change transforms proper maps into proper maps, without loss of generality in this paper, we will always assume that S is such that the natural map (2.3) is an isomorphism. Let v be a closed point of S which corresponds to a maximal ideal of R denoted also by v. Let $k_v := k(v) = R/v$. In this case the reduction map has the following form:

$$r_v : A(K) \to \mathcal{A}_v(k_v). \tag{2.4}$$

Corollary 2.4. *Let R be a finitely generated $\mathbb{Z}$-algebra such that $S = \operatorname{Spec} R$ is an integral and normal scheme. Let $\mathcal{A}/S$ be an abelian scheme with generic fibre A/K. Let l be prime to the residue characteristics of S. Let $v \in S$ be a closed point. Then the natural map*

$$r_v : A(K)_l \to \mathcal{A}_v(k_v)_l,$$

is a monomorphism.

Proof. By the proper and smooth base change theorem [Mi2, Chap. VI, Sec. 4, Cor 4.2] applied to the constant sheaves $\mathbb{Z}/l^k$ on $\mathcal{A}$, for each $k \geqslant 1$ we have a natural isomomorphism $H^1(A, \mathbb{Z}/l^k) \cong H^1(\mathcal{A}_v, \mathbb{Z}/l^k)$ of $g_v := G(\overline{k_v}/k_v)$-modules for every $k \geqslant 1$. Taking inverse limit on k and passing to $\mathbb{Z}_l$ duals we get a natural isomorphism $T_l(A) \cong T_l(\mathcal{A}_v)$ of $\mathbb{Z}_l$ and g_v-modules. Tensoring with $\mathbb{Q}_l/\mathbb{Z}_l$ gives an isomorphism $A[l^\infty] \cong \mathcal{A}_v[l^\infty]$ of g_v-modules. The group g_v acts on these modules by its quotient $G(k_v(\mathcal{A}_v[l^\infty])/k_v)$. Since k_v is a finite field, we know by the Weil conjecture proven by Deligne that $H^0(g_v, \mathcal{A}_v[l^\infty])$ is finite. Hence $H^0(G_K, A[l^\infty])$ and $H^0(\pi_1(S), \mathcal{A}[l^\infty])$ are also finite. Hence the Corollary follows from Theorem 2.3. ■

From now on, when working with reduction map, we always consider abelian scheme $\mathcal{A}/S$ such that the assumptions of corollary 2.4 hold. Moreover we can take $S \to \operatorname{Spec}\mathbb{Z}$ to be a smooth morphism (cf [F2, p. 204]). The smoothness of $S \to \operatorname{Spec}\mathbb{Z}$ implies that S is normal scheme [ST, Lemma 33.14.2] . Tensoring the reduction map (2.4) by $\mathbb{Z}_l$ gives the following reduction map

$$r_v : A(K) \otimes \mathbb{Z}_l \to \mathcal{A}_v(k_v)_l$$

which we are going to use later in this paper.

3. Homorphisms of abelian schemes

Theorem 3.1 (Raynaud). *Let S be noetherian integral scheme and G, H be two abelian schemes over S. Assume that there exists a dense open subscheme U of the scheme S and there exists a homomorphism $\psi_U : H|_U \to G|_U$. Then there is the unique extension of ψ_U to homomorphism $\psi : H \to G$ over S.*

Proof. See [FC, Prop 2.7, p. 9] ■

Let $\mathcal{A}/S$ and $\mathcal{B}/S$ be two projective abelian schemes with respective generic fibers A/K and B/K. Then by [FC, Prop 2.7, p. 9] we have

$$Hom_K(A, B) = Hom_S(\mathcal{A}, \mathcal{B})$$

because every homomorphism $\phi \in Hom_K(A, B)$ extends to an element of $Hom_U(\mathcal{A}_{|U}, \mathcal{B}_{|U})$ for an open subset $U \subset S$. In particular $End_K(A) = End_S(\mathcal{A})$. For an abelian scheme $\mathcal{A}/S$ there is a finite field extension L/K such that there is an isogeny $\phi : A \to \prod_{i=1}^t A_i^{e_i}$ over L where A_i is a simple abelian variety over L. If L/K is separable, S normal and $\tilde{S}$ is the normalization of S in L then we can choose an open subset $\tilde{U} \subset \tilde{S}$ such that $\tilde{U}/S$ is étale, hence smooth [Mi2] I, Theorem 3.21. Put $\tilde{\mathcal{A}} := \mathcal{A} \times_S \tilde{S}$. By remark 2.1 we can require that $\tilde{U} \subset \tilde{S}$ is such that A_i gives rise to an abelian projective scheme $\tilde{\mathcal{A}}_i$ over $\tilde{U}$. We will assume without loss of generality in our work that $\tilde{U} = \tilde{S}$. Since

$$Hom_L(A, \prod_{i=1}^t A_i^{e_i}) = Hom_{\tilde{S}}(\tilde{\mathcal{A}}, \prod_i \tilde{\mathcal{A}}_i^{e_i}),$$

the isogeny ϕ lifts to a homomorphism $\tilde{\phi} \in Hom_{\tilde{S}}(\tilde{\mathcal{A}}, \prod_i \tilde{\mathcal{A}}_i^{e_i})$. If $S \to \operatorname{Spec}\mathbb{Z}$ is smooth then $\tilde{S} \to \operatorname{Spec}\mathbb{Z}$ is also smooth since smoothness is preserved by composition.

4. Homomorphisms of abelian varieties and nontorsion points of Mordell-Weil groups

In this section K will denote any field.

Let V and W be algebraic varieties over K. For any field extension L/K the symbol $Hom_L(V,W)$ denotes the set of all morphisms from V to W defined over L. The Galois group $G(\overline{K}/K)$ acts on $Hom_{\overline{K}}(V,W)$ (see eg. [Sil, p. 15]) as follows. For $\phi \in Hom_{\overline{K}}(V,W)$ and $\sigma \in G(\overline{K}/K)$ and any $P \in V$ we define $\sigma(\phi)(P) := \sigma \circ \phi \circ \sigma^{-1}(P) = \sigma(\phi(\sigma^{-1}P))$. We have $Hom_{\overline{K}}(V,W)^{G(\overline{K}/K)} = Hom_K(V,W)$ cf., [Sil, p. 20]. Hence for any Galois extension L/K, $L \subset \overline{K}$ the group $G(\overline{K}/K)$ acts on $Hom_L(V,W)$ via its quotient $G(L/K)$ and $Hom_L(V,W)^{G(L/K)} = Hom_K(V,W)$.

In particular, for two abelian varieties A and B defined over K and for any finite Galois extension L/K there is a well defined trace homomorphism between the groups:

$$Tr_{L/K} : Hom_L(A,B) \to Hom_K(A,B)$$

$$Tr_{L/K}(\phi) := \sum_{\sigma \in G(L/K)} \sigma(\phi).$$

Consider the natural imbedding:

$$Hom_L(A,B) \otimes \mathbb{Z}_l \to Hom_{G(\overline{K}/L)}(T_l(A), T_l(B)).$$

Then the image of $\sigma(\phi)$ via this map equals $\sigma_l \circ \phi_l \circ \sigma_l^{-1}$, where ϕ_l is the image of ϕ and σ_l denotes the action of σ on both $T_l(A)$ and $T_l(B)$. Let $\tilde{Tr} : End^0_{\overline{K}}(A) \to \mathbb{Q}$ be the trace see [Mi1, p. 125]. Then by [Mi1, Prop 12.9] we get $\tilde{Tr}(\sigma(\phi)) = Tr(\sigma_l \circ \phi_l \circ \sigma_l^{-1}) = Tr(\phi_l) = \tilde{Tr}(\phi)$. The bilinear form $(\alpha, \beta) \to \tilde{Tr}(\alpha\beta)$ is positive definite [Mi1, Theorem 17.3]. In particular, if $\beta \neq 0$ then $\tilde{Tr}(\beta^\star \beta) > 0$ where $\star$ is the Rosati involution.

Theorem 4.1 (Ribet [Ri, Prop 1.5]). *Let A be an abelian variety over K. Let $\mathcal{R} := End_K(A)$ and for any field extension L/K let $\mathcal{R}_L := \mathrm{End}_L(A)$. Let $P_1, \ldots, P_r \in A(K)$ and let L/K be a finite, separable field extension. Then $P_1, \ldots, P_r$ are independent over $\mathcal{R}$ if and only if $P_1, \ldots, P_r$ are independent over $\mathcal{R}_L$.*

Proof. If $P_1, \ldots, P_r$ are independent over $\mathcal{R}_L$ then it is clear that they are independent over $\mathcal{R}$. Asume that $P_1, \ldots, P_r$ are independent over $\mathcal{R}$. We can assume that L/K is Galois. Let $\beta_1, \ldots, \beta_r \in \mathcal{R}_L$, not all equal to zero, be such that $\sum_{i=1}^r \beta_i P_i = 0$. If $\beta_j \neq 0$ we can find a scalar $b \in \mathbb{N}$ such that $Tr_{L/K}(b\beta_j^\star \beta_i) \in \mathbb{N}$. Multiplying out by $b\beta^\star$ and applying $Tr_{L/K}$ we get

$$\sum_{i=1}^r Tr_{L/K}(b\beta_j^\star \beta_i) P_i = 0 \tag{4.1}$$

because $P_i \in A(K)$ for all $1 \leqslant i \leqslant r$. By the discussion before this Lemma we note that

$$\tilde{Tr}(Tr_{L/K}(b\beta_j^\star\beta_j)) = \sum_{\sigma\in G(L/K)} \tilde{Tr}(\sigma(b\beta_j^\star\beta_j)) \tag{4.2}$$
$$= [L:K]\tilde{Tr}(b\beta_j^\star\beta_j) > 0.$$

Hence $Tr_{L/K}(b\beta_j^\star\beta_j) \neq 0$. But equation (4.1) gives a linear dependence of points $P_1, \ldots, P_r$ over $\mathcal{R}$ with coefficient $Tr_{L/K}(b\beta_j^\star\beta_j) \neq 0$. A contradiction. ■

Below we collect three elementary lemmas that will be usefull in our proofs in Section 6.

Lemma 4.2. *Let A be an abelian variety $A = A_1 \times \cdots \times A_s$, where A_i/K is an abelian variety for each $1 \leqslant i \leqslant s$. Let $Q_1, \ldots, Q_r \in A(K)$. Write $Q_i = [Q_i^j]_{1\leqslant j\leqslant s}$ with $Q_i^j \in A_j(K)$ for each $1 \leqslant j \leqslant s$.*

1. *If $Q_1, \ldots, Q_r \in A(K)$ are linearly independent over $End_K(A)$ then $Q_1^j, \ldots Q_r^j$ are linearly independent over $End_K(A_j)$ for every $1 \leqslant j \leqslant r$.*
2. *If in addition $Hom(A_i, A_j) = \{0\}$ for all $j \neq i$, then the following conditions are equivalent*
   - (a) *$Q_1, \ldots, Q_r \in A(K)$ are linearly independent over $End_K(A)$*
   - (b) *$Q_1^j, \ldots Q_r^j$ are linearly independent over $End_K(A_j)$ $\forall_{1\leqslant j\leqslant r}$.*

Proof. (1) Follows from the following inclusion:

$$End_K(A_1) \times \cdots \times End_K(A_t) \subset End_K(A_1 \times \cdots \times A_t).$$

(2) Follows from the following isomorphism:

$$End_K(A_1) \times \cdots \times End_K(A_t) \cong End_K(A_1 \times \cdots \times A_t).$$ ■

Lemma 4.3. *Let A be a simple abelian variety over K and let $e \in \mathbb{N}$. Let $Q_1, \ldots, Q_r \in A^e(K) = A(K)^e$. Write $Q_i := [Q_i^j]_{1\leqslant j\leqslant e}$, with $Q_i^j \in A(K)$. The following conditions are equivalent*

1. *$Q_1, \ldots, Q_r \in A(K)$ are linearly independent over $End_K(A^e)$*
2. *the points $Q_i^j, \forall_{1\leqslant i\leqslant r, 1\leqslant j\leqslant e}$ are linearly independent over $End_K(A)$.*

Proof. Follows from simple observation that:

$$\sum_{i=1}^r \begin{bmatrix} \alpha_i^{11} & \cdots & \alpha_i^{1e} \\ \vdots & \ddots & \vdots \\ \alpha_i^{e1} & \cdots & \alpha_i^{ee} \end{bmatrix} \begin{bmatrix} Q_i^1 \\ \vdots \\ Q_i^e \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

if and only if $\sum_{i=1}^r \sum_{j=1}^e \alpha_i^{kj} Q_i^j = 0$ for every $1 \leqslant k \leqslant e$. ■

Lemma 4.4. *Let $A = \prod_{i=1}^{t} A_i^{e_i}$ where A_i/K is simple for each $1 \leqslant i \leqslant t$ and A_i is not isogenous to A_j for all $i \neq j$. Let $Q_1, \ldots, Q_r \in A(K)$. Write $Q_i = [Q_i^j]_{1 \leqslant j \leqslant t}$ with $Q_i^j \in A_j^{e_j}(K)$, and write $Q_i^j = [Q_i^{j,k}]_{1 \leqslant k \leqslant e_i}$ for $Q_i^{j,k} \in A_j(K)$.*

The following conditions are equivalent

1. *$Q_1, \ldots, Q_r \in A(K)$ are linearly independent over $End_K(A)$,*
2. *For every $1 \leqslant j \leqslant t$ the points $(Q_i^{j,k})_{1 \leqslant i \leqslant r, 1 \leqslant k \leqslant e_i}$ are linearly independent over $End_K(A_j)$.*

Proof. Follows immediately from Lemmas 4.2 and 4.3. ■

5. *l*-adic representations for abelian varieties over finitely generated fields

In this section we collect some classical results about abelian varieties A/K for K a finitely generated field over $\mathbb{Q}$. As explained at the beginning of the introduction A/K extends to a projective, abelian group scheme $\mathcal{A}/S$ over an integral scheme $S = \operatorname{Spec} R$ such that $S \to \operatorname{Spec} \mathbb{Z}$ is smooth and such that:

$$\mathcal{A}(S) \xrightarrow{\cong} A(K).$$

Let $\overline{K}_s$ denote a separable closure of K. Let $v \in S$ be a closed point an let $Fr_v \in G(\overline{K}_s/K)$ be any element of the conjugacy class of the canonical generator of $G(\overline{k_v}/k_v) \subset \pi_1(S)$. The elements will be called Frobenius elements for v.

Theorem 5.1 (Mordell-Weil, Lang-Néron). *Let A be an abelian variety over K. Then $A(K)$ is a finitely generated abelian group.*

Proof. See [L] Theorem 4.1 and Theorem 4.2 and Corollary 4.3 p. 27-28. ■

Theorem 5.2 (Chebotarev). *Let A/K be an abelian variety. The set $\{Fr_v :$ v closed point of $S\}$ is dense in $\pi_1(S)$.*

Proof. See [FW, pp. 206-207], [Se3, pp. 91]. ■

Theorem 5.3 (Faltings). *For any abelian variety A/K and any prime number l:*

(i) *$End(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to End_{G_F}\big(T_l(A)\big)$ is an isomorphism,*
(ii) *$V_l(A)$ is a semisimple $\mathbb{Q}_l[G_{l^\infty}]$ module.*

Proof. See [FW, Theorem 1, p. 204]. ■

Theorem 5.4 (Zarhin). *For any abelian variety A/K and for any prime number l:*

(i) *$End_K(A) \otimes \mathbb{Z}/l \to End_{G_K}\big(A[l]\big)$ is an isomorphism,*
(ii) *$A[l]$ is semisimple $\mathbb{Z}/l[G_l]$ module for $l \gg 0$*

Proof. See [S-Z, Prop. 3.4] ■

Theorem 5.5 (Serre). *Let A/K be abelian variety and let*

$$\rho_l : G_K \longrightarrow GL\big(T_l(A)\big)$$

be the l-adic representation associated with A. Then the index

$$e_l := \Big[\mathbb{Z}^\times Id_{T_l(A)} : \rho_l(G_K) \cap \mathbb{Z}_l^\times Id_{T_l(A)}\Big]$$

is bounded independently of l.

The Theorem 5.5 in the case when K is a number field is proven in [Se1] and it was suggested in loc. cit. that the Theorem holds for A/K over a finitely generated field $K/\mathbb{Q}$. Since the proof for finitely generated fields is not in the literature we will give two proofs of this theorem below. Proof 1 was explained to G. Banaszak by J-P. Serre.

Proof 1 (Serre). The proof goes by induction on $n = tr. \deg .K$. If $n > 0$, we may view K as the function field of a smooth curve C over a field K_0 with $tr. \deg K_0$ equal to $n - 1$. The abelian variety A/K defines an abelian group scheme $\widetilde{\mathcal{A}}$ over an open dense subset U of C. Choose a closed point P in U and let v be the discrete valuation of K defined by P; its residue field k_v is a finite extension of K_0. If m is any integer > 0, the field extension $K(A[m])/K$ is unramified at v. The corresponding Galois group $G(K(A[m])/K)$ has a decomposition group at v which is isomorphic to $G(k_v(\widetilde{\mathcal{A}}_v[m])/k_v)$ where $\widetilde{\mathcal{A}}_v$ is the fiber of $\widetilde{\mathcal{A}}$ at v. This shows, by taking a projective limit on m, that the image of

$$Gal(\overline{K}/K) \to \prod_l GL\big(T_l(A)\big)$$

contains the image of

$$Gal(\overline{k_v}/k_v) \to \prod_l GL\big(T_l(\widetilde{\mathcal{A}}_v)\big),$$

where $GL\big(T_l(A)\big) \cong GL\big(T_l(\widetilde{\mathcal{A}}_v)\big) \cong GL_{2g}(\mathbb{Z}_l)$. By induction the image of $Gal(\overline{k_v}/k_v) \to \prod_l GL\big(T_l(\widetilde{\mathcal{A}}_v)\big)$ contains the e-powers of homotheties for some $e > 0$. Hence the image of $Gal(\overline{K}/K) \to \prod_l GL\big(T_l(A)\big)$ contains also the e-powers of homotheties. ■

Proof 2 (Banaszak). The proof is done in four steps.

Step 1. There is a smooth, geometrically irreducible scheme S over L (= the algebraic closure of $\mathbb{Q}$ in K) with generic point $\eta = \operatorname{Spec} K$ such that A is the generic fibre of $\mathcal{A} \to S$, an abelian scheme (= proper, smooth morphism with geometrically connected fibers) [F1, p. 1] Moreover there is a closed point $P \in S(L)$ [F2, p. 212]. So we have $A = \mathcal{A} \times_S \eta$. Put $\mathcal{A}_P := \mathcal{A} \times_S P$.

Step 2. Put $G_K := G(\overline{K}/K)$ and $G_L := G(\overline{L}/L)$. The natural map $G_K \to \pi_1(S)$ is surjective and the decomposition group $D_P \subset \pi_1^{et}(S)$ is isomorphic to G_L, where $\pi_1^{et}(S) := \pi_1^{et}(S,\eta)$. Moreover G_K acts on $T_l(A)$ via its quotient $\pi_1^{et}(S)$ [F2, p. 212]

Step 3. By [Se2] the index

$$e_l = [\mathbb{Z}_l^\times Id_{T_l(A_P)} : \rho_{L,l}(D_P) \cap \mathbb{Z}_l^\times Id_{T_l(A_P)}]$$

is bounded as l varies where

$$\rho_{L,l} : G_L \to GL(T_l(A_P)).$$

Step 4. By proper and smooth base change theorem [Mi2, Chap. VI, Sec. 4, Cor 4.2] applied to the constant sheaves $\mathbb{Z}/l^k$ on $\mathcal{A}$, for each $k \geqslant 1$, we have a natural isomorphism $T_l(A) \cong T_l(A_P)$ of $\mathbb{Z}_l[D_P]$ modules such that D_P acts on $T_l(A)$ as a subgroup of $\pi_1^{et}(S)$. Hence $\tilde{e}_l \leqslant e_l$. ■

Corollary 5.6 (Bogomolov). *Let A/K be abelian variety and let l be a prime number. Let $\rho_l : G_K \longrightarrow GL\big(T_l(A)\big)$ be the l-adic representation associated with A. Then $\rho_l(G_K) \cap \mathbb{Z}_l^\times Id_{T_l(A)}$ is open in $\mathbb{Z}_l^\times Id_{T_l(A)}$*

Proof. Follows immediately from Theorem 5.5. ■

Theorem 5.7 (Serre). *For any abelian variety over K and for any prime number l:*

(i) $H^n\,(G_{l^\infty}\ ;\ V_l(A)) = 0$
(ii) $H^n\,(G_{l^\infty}\ ;\ T_l(A))$ *is finite*

Proof. See [Se2] Corollaire and Remarque 2 p. 734. ■

Theorem 5.8. *Let A be an abelian variety over K and let l be a prime number. Then:*

(i) $H^n\big(G_{l^{k'}}; A[l^k]\big) = 0$ *for* $l \gg 0$ *and* $k' \geqslant k \geqslant 1$
(ii) $H^n\big(G_{l^\infty}; T_l(A)\big) = 0$ *for* $l \gg 0$

Proof. By Theorem 5.5 there is $e \in \mathbb{N}$ such that $e_l \leqslant e$ for all l. Take $l \gg 0$ such that $l > e+1$. Because $\mathbb{Z}_l^\times \cong \big(\mathbb{Z}/l\big)^\times \times (1 + l\mathbb{Z}_l)$ there is $h := cId_{T_l(A)} \in \big(\mathbb{Z}/l\big)^\times Id_{T_l(A)} \subset \mathbb{Z}_l^\times Id_{T_l(A)}$, $c \not\equiv\ 1$ *mod l.*

Let Δ be the subgroup of G_{l^∞} generated by $cId_{T_l(A)}$, $\mid \Delta \mid \Big| l-1$ Observe that Δ maps isomorphicaly to its image $G_{l^\infty} \to G_{l^k}\quad \forall_k \geqslant 1$. Note that $\Delta \subset Z(G_{l^\infty})$ and $\Delta \subset Z(G_{l^k})$ for $\forall_{k\geqslant 1}$. Consider the spectral sequence

$$E_2^{i,j} = H^i\bigg(G_{l^{k'}}/\Delta; H^j(\Delta\ ;\ A[l^k])\bigg) \Rightarrow H^{i+j}\big(G_{l^{k'}}; A[l^k]\big)$$

Observe that $H^j(\Delta\ :\ A[l^k]) = 0$ for all $j > 0$ because $|\Delta||l-1$. Moreover by definition of Δ it is clear that $H^0(\Delta : A[l^k]) = A[l^k]^\Delta = 0$. This implies that $H^n(G_{l^{k'}} : A[l^k]) = 0$ for all $n \geqslant 0, l > e+1$ and for all $k' \geqslant k \geqslant 0$. Hence $H^n\big(G_{l^\infty}; T_l(A)\big) = \varprojlim_k \varinjlim_{k'} H^n(G_{l^{k'}}; A[l^k]) = 0$ for $l > e+1$. ■

6. Reduction of torsion and nontorsion points

In this section we apply all results of the previous sections to prove a theorem on the reduction of nontorsion elements in $A(K)$. This result is an extension of Theorem 3.3 [BK] and Proposition 11 [Pe2] to the case of finitely generated field K. This section reminds Section 3 of [BK] but we include complete proofs for the convenience of the reader.

Let $A = A_1 \times \cdots \times A_t$ be a product of simple nonisogenous abelian varieties A_i defined over K. Let $\mathcal{R}_i := End_K(A_i)$. Let $P_{i1}, \dots, P_{ir_i} \in A_i(K)$ be linearly independent over $\mathcal{R}_i$ for each $1 \leqslant i \leqslant t$. Put $K_{l^\infty} := K(A[l^\infty])$, $G_K = G(\overline{K}/K)$, $G_{l^\infty} := G(K_{l^\infty}/K)$, $H_{l^\infty} := G(\overline{K}/K_{l^\infty})$ and $H_{l^k} := G(\overline{K}/K_{l^k})$ for all $k \geqslant 1$. For each $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant r_i$ let

$$\phi_{ij} : H_{l^\infty} \to T_l(A_i)$$

denote the inverse limit over k of the Kummer maps:

$$\phi_{ij}^{(k)} : H_{l^k} \to A_i[l^k],$$

$$\phi_{ij}^{(k)}(\sigma) := \sigma(\frac{1}{l^k} P_{ij}) - \frac{1}{l^k} P_{ij}.$$

Lemma 6.1. *If $\alpha_{11}, \dots, \alpha_{1r_1} \in \mathcal{R}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_l, \dots, \alpha_{t1}, \dots, \alpha_{tr_t} \in \mathcal{R}_t \otimes_{\mathbb{Z}} \mathbb{Z}_l$ are such that $\sum_{i=1}^t \sum_{j=1}^{r_t} \alpha_{ij}\phi_{ij} = 0$, then $\alpha_{ij} = 0$ in $\mathcal{R}_i$ for all $1 \leqslant i \leqslant t$, $1 \leqslant j \leqslant r_i$.*

Proof. Let Ψ be the composition of maps:

$$A(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow H^1(G_K; T_l(A)) \longrightarrow H^1(H_{l^\infty}; T_l(A)) = Hom\,(H_{l^\infty}; T_l(A)).$$

Note that $\phi_{ij} = \Psi(P_{ij} \otimes 1)$. By Theorem 5.7 the group $H^1(G_{l^\infty}; T_l(A))$ is finite hence $\ker \Psi \subset (A(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)_{tor}$. Let $c := |A(K)_{tor}|$. Since Ψ is an $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_l$-homomorphism, we have:

$$0 = \sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}\phi_{ij} = \Psi\left(\sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}(P_{ij} \otimes 1)\right).$$

Hence

$$c \sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}(P_{ij} \otimes 1) = 0$$

in $A(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$. Since $P_{i1} \otimes 1, \dots, P_{ir_i} \otimes 1$ are linearly independent over $\mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Z}_l$ in $A_i(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ we obtain $c\alpha_{ij} = 0$ hence $\alpha_{i1} = \cdots = \alpha_{ir_i} = 0$, because $\mathcal{R}_i$ is a free $\mathbb{Z}$-module for each $1 \leqslant i \leqslant t$. ■

Define the following maps:

$$\Phi_i^k : H_{l^k} \to A_i[l^k]^{r_i}$$

$$\Phi_i^k(\sigma) := \left(\phi_{i1}^{(k)}(\sigma), \ldots, \phi_{ir_i}^{(k)}(\sigma)\right)$$

Then define the map $\Phi^k : H_{l^k} \to \bigoplus_{i=1}^t A_i[l^k]^{r_i}$ as follows

$$\Phi^k := \bigoplus_{i=1}^t \Phi_i^k.$$

Define the following maps:

$$\Phi_i : H_{l^\infty} \to T_l(A_i)^{r_i}$$

$$\Phi_i(\sigma) := (\phi_{i1}(\sigma), \ldots, \phi_{ir_i}(\sigma))$$

Again define the map $\Phi : H_{l^\infty} \to \bigoplus_{i=1}^t T_l(A_i)^{r_i}$ as follows

$$\Phi := \bigoplus_{i=1}^t \Phi_i.$$

Lemma 6.2. *The image of the map Φ is open in $\bigoplus_{i=1}^t T_l(A_i)^{r_i}$.*

Proof. Let $T := \bigoplus_{i=1}^t T_l(A_i)^{r_i}$ and let $W := T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \bigoplus_{i=1}^t V_{il}^{r_i}$ where $V_{il} := T_l(A_i) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Denote by $\Phi \otimes 1$ the composition of Φ with the obvious natural inclusion $T \hookrightarrow W$. Put $M := Im(\Phi \otimes 1) \subset W$. Both M and W are $\mathbb{Q}_l[G_{l^\infty}]$-modules. It is enough to show that $Im\Phi$ has a finite index in T (cf, [Ri, Th. 1.2]. Hence it is enough to show that $\Phi \otimes 1$ is onto. Observe that V_{il} is a semisimple $\mathbb{Q}_l[G_{l^\infty}]$-module for each $1 \leqslant i \leqslant t$ because it is a direct summand of the semisimple $\mathbb{Q}_l[G_{l^\infty}]$-module $V_l(A) = \bigoplus_{i=1}^t V_{il}$ by results of Faltings and Zarhin (see Theorem 5.3 (ii)). Note that G_{l^∞} acts on V_{il} via the quotient $G(L(A_i[l^\infty])/L)$. If $\Phi \otimes 1$ is not onto we have a decomposition $W = M \oplus M_1$ of $\mathbb{Q}_l[G_{l^\infty}]$-modules with M_1 nontrivial.

Let $\pi_{M_1} : W \to W$ be the projection onto M_1 and let $\pi_i : W \to V_{il}$ be a projection that maps M_1 nontrivially. Denote $\widetilde{\pi_i} := \pi_i \circ \pi_{M_1}$. Again it follows by results of Faltings and Zarhin (see Theorem 5.3 (i)) that $Hom_{G_{l^\infty}}(V_{il}; V_{i'l}) \cong Hom_L(A_i; A_{i'}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = 0$ for all $i \neq i'$. Hence

$$\widetilde{\pi_i}(v_{ij}) = \sum_{j=1}^{r_i} \beta_{ij} v_{ij},$$

for some $\beta_{ij} \in \mathcal{R}_i \otimes \mathbb{Q}_l$. Since π_i is nontrivial on M_1, we see that some β_{ij} is nonzero. On the other hand

$$\widetilde{\pi_i}(\Phi(h) \otimes 1) = \sum_{j=1}^{r_i} \beta_{ij}(\phi_{ij}(h) \otimes 1) = 0,$$

for all $h \in H_{l^\infty}$. Multiplying the last equality by a suitable power of l we get:

$$0 = \sum_{j=1}^{r_i} \alpha_{ij}(\phi_{ij}(h) \otimes 1),$$

for some $\alpha_{ij} \in \mathcal{R}_i \otimes \mathbb{Z}_l$. Since the maps $\mathcal{R}_i \otimes \mathbb{Z}_l \hookrightarrow \mathcal{R}_i \otimes \mathbb{Q}_l$ and $\mathrm{Hom}(H_{l^\infty}, T_l) \hookrightarrow \mathrm{Hom}(H_{l^\infty}, V_l)$ are imbeddings of $\mathcal{R} \otimes \mathbb{Z}_l$-modules, we obtain $\sum_{j=1}^{r_i} \alpha_{ij}\phi_{ij} = 0$. By Lemma 6.1 we get $\alpha_{i1} = \cdots = \alpha_{ir_i} = 0$, hence $\beta_{i1} = \cdots = \beta_{ir_i} = 0$ because $\mathcal{R}$ is torsion free. This contradiction shows that $M_1 = 0$. ■

Theorem 6.3. *Let $A = \prod_{i=1}^{t} A_i$ be abelian variety over finitely generated field K over $\mathbb{Q}$ such that $Hom_{\overline{K}}(A_i, A_j) = 0$ for all $j \neq i$. Let l be a prime number. Let $Q_{ij} \in A_i(K)$ for $1 \leqslant j \leqslant r_i$ be independent over $\mathcal{R}_i$ for each $1 \leqslant i \leqslant t$. Then for every open subset $U \subset S$ exists infinite many closed points $v \in U$ such such that $r_v(Q_{ij}) = 0$ in $A_{iv}(k_v)_l$ for all $1 \leqslant j \leqslant r_i$ and $1 \leqslant i \leqslant t$.*

Proof. *Step 1.* By lemma 6.2 there is an $m \in \mathbb{N}$ such that

$$l^m \bigoplus_{i=1}^{t} T_l(A_i)^{r_i} \subset \Phi\left(H_{l^\infty})\right) \subset \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}.$$

Let Γ be the $\mathcal{R}$-submodule of $A(K)$ generated by all the points Q_{ij}. Hence

$$\Gamma = \sum_{i=1}^{t}\sum_{j=1}^{r_i} \mathcal{R}_i Q_{ij}.$$

For $k \geqslant m$ consider the following commutative diagram.

$$\begin{tikzcd}
G(K_{l^\infty}(\frac{1}{l^\infty}\Gamma)/K_{l^\infty}) \arrow[r, "\overline{\Phi}"] \arrow[d] & \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}/l^m \bigoplus_{i=1}^{t} T_l(A_i)^{r_i} \arrow[d] \\
G\left(K_{l^{k+1}}(\frac{1}{l^{k+1}}\Gamma)/K_{l^{k+1}}\right) \arrow[r, "\overline{\Phi^{k+1}}"] \arrow[d] & \bigoplus_{i=1}^{t} \left(A_i[l^{k+1}]\right)^{r_i}/l^m \bigoplus_{i=1}^{t} \left(A_i[l^{k+1}]\right)^{r_i} \arrow[d, "="] \\
G\left(K_{l^k}(\frac{1}{l^k}\Gamma)/K_{l^k}\right) \arrow[r, "\overline{\Phi^k}"] & \bigoplus_{i=1}^{t} \left(A_i[l^k]\right)^{r_i}/l^m \bigoplus_{i=1}^{t} \left(A_i[l^k]\right)^{r_i}
\end{tikzcd}$$

The maps $\overline{\Phi}$ and $\overline{\Phi^k}$, for all $k \geqslant 1$, are induced naturally by Kummer maps. For $k \gg 0$ the images of the middle and bottom horizontal arrows in this diagram are isomorphic. Hence $G(K_{l^{k+1}}(\frac{1}{l^{k+1}}\Gamma)/K_{l^{k+1}})$ maps onto $G(K_{l^k}(\frac{1}{l^k}\Gamma)/K_{l^k})$ via the left bottom vertical arrow in the diagram because the map $\overline{\Phi^k}$ is injective for each $k \geqslant 1$. Consider the following tower of field

$$\begin{tikzcd}
& K_{l^{k+1}}\left(\frac{1}{l^{k+1}}\Gamma\right) \arrow[d, dash] & \\
& K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right) \arrow[dl, dash] \arrow[dr, dash] & \\
K_{l^k}\left(\frac{1}{l^k}\Gamma\right) \arrow[dr, dash] & & K_{l^{k+1}} \arrow[dl, dash] \\
& K_{l^k} &
\end{tikzcd}$$

It is clear that we have the following equality:

$$K_{l^k}(\frac{1}{l^k}\Gamma) \cap K_{l^{k+1}} = K_{l^k} \qquad \text{for } \; k \gg 0 \tag{6.1}$$

Step 2. Let $U_0 := \operatorname{Spec} R_0 \subset S$ be an open affine subset where R_0 is a localization of R. Let R_1 (resp. R_2) be integral closure of R_0 in $K_{l^{k+1}}(\frac{1}{l^k}\Gamma)$ (resp. in $K_{l^k}(\frac{1}{l^k}\Gamma)$). Let $U_1 := \operatorname{Spec} R_1$ and $U_2 := \operatorname{Spec} R_2$. We can choose U_0 such that $\mathcal{A}(U_1) \overset{\sim}{\to} A(K_{l^{k+1}}(\frac{1}{l^k}\Gamma))$, $\mathcal{A}(U_2) \overset{\sim}{\to} A(K_{l^k}(\frac{1}{l^k}\Gamma))$ and $\mathcal{A}(U_0) \overset{\sim}{\to} A(K)$ (See comment after Theorem 3.1).

By result of Bogomolov, Corollary 5.6, we can find $k \gg 0$ and $h \in G\left(K_{l^\infty}/K_{l^k}\right)$ which acts on $T_l A$ as a homothety $1 + l^k u$ for and some $u \in \mathbb{Z}_l^\times$. Let h also denote, by a slight abuse of notation, the projection of h onto $G\left(K_{l^{k+1}}/K_{l^k}\right)$. By (6) we can choose $\sigma \in G\left(K_{l^{k+1}}(\frac{1}{l^k}\Gamma)/K\right)$ such that $\sigma_{|K_{l^k}(\frac{1}{l^k}\Gamma)} = \mathrm{id}$ and $\sigma_{|K_{l^{k+1}}} = h$. By Chebotarev density theorem, (see Theorem (5.2)) there is a infinite set of closed points $v \in U_0$ such that there is a closed point $v_1 \in U_1$ over v whose Frobenius in $K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right)/K$ equals to σ.

Let $l^{c_{ij}}$ be the order of the element $r_v(Q_{ij})$ in the group $A_{iv}(k_v)_l$, for some $c_{ij} \geqslant 0$. Let v_2 be a closed point of U_2 below v_1. Consider the following commutative diagram:

$$\begin{tikzcd}
A_i(K) \arrow[r, "r_v"] \arrow[d] & A_{iv}(k_v)_l \arrow[d, "="] \\
A_i\left(K_{l^k}(\frac{1}{l^k}\Gamma)\right) \arrow[r, "r_{v_2}"] \arrow[d] & A_{i,v}(k_{v_2})_l \arrow[d] \\
A_i\left(K_{l^{k+1}}(\frac{1}{l^k}\Gamma)\right) \arrow[r, "r_{v_1}"] & A_{iv}(k_{v_1})_l
\end{tikzcd} \tag{6.2}$$

Observe that all vertical arrows in the diagram (6.2) are injective. Let $R_{ij} := \frac{1}{l^k}Q_{ij} \in A\left(K_{l^k}(\frac{1}{l^k}\Gamma)\right) \subset A\left(K_{l^{k+1}}(\frac{1}{l^k}\Gamma)\right)$. The element $r_{v_1}(R_{ij})$ has order $l^{k+c_{ij}}$ in the group $A_{iv_1}(k_{v_1})_l$ because

$$l^{k+c_{ij}} r_{v_1}(R_{ij}) = l^{c_{ij}} r_v(Q_{ij}) = 0.$$

By the choice of v, we have $k_v = k_{v_2}$ hence $r_{v_1}(R_{ij})$ comes from an element of $A_{iv}(k_v)_l$. If $c_{ij} \geqslant 1$ then

$$h\left(l^{c_{ij}-1}r_{v_1}(R_{ij})\right) = (1+l^k u)l^{c_{ij}-1}r_{v_1}(R_{ij})$$

since $l^{c_{ij}-1}r_{v_1}(R_{ij}) \in A_{iv}(k_v)\left[l^{k+1}\right]$. On the other hand, by the choice of v, Frobenius at v_1 acts on $l^{c_{ij}-1}r_{v_1}(R_{ij})$ via h. So $h\left(l^{c_{ij}-1}r_{v_1}(R_{ij})\right) = l^{c_{ij}-1}r_{v_1}(R_{ij})$ because $r_{v_1}(R_{ij}) \in A_{iv}(k_v)_l$. Hence, $l^{c_{ij}-1}ur_{v_1}(Q_{ij}) = 0$ but this is impossible since the order of $r_{v_1}(Q_{ij}) = 0$ is $l^{c_{ij}}$. Hence we must have $c_{ij} = 0$. ■

Theorem 6.4. *Let $A = \prod_{i=1}^t A_i$ be abelian variety over finitely generated field over $\mathbb{Q}$ such that $Hom_{\overline{K}}(A_i, A_j) = 0$ for all $j \neq i$. Let l be a prime number. Let $m \in \mathbb{N} \cup \{0\}$ for all $1 \leqslant j \leqslant r_i$ and $1 \leqslant i \leqslant t$. Let $P_{ij} \in A_i(K)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i\left[l^m\right]$ be aribitrary torsion elements for all $1 \leqslant j \leqslant r_i$ and $1 \leqslant i \leqslant t$. Let R' be integral closure of R in $K(A[l^m])$. Let ω' be a closed point in U' over v where $U' := \gamma^{-1}(U)$ and γ is natural map $\gamma : \operatorname{Spec} R' \to \operatorname{Spec} R$. Then exists infinitely many closed points $v \in U$ such that*

$$r_{w'}(T_{ij}) = r_v(P_{ij}) in A_{i,v}(k_v)_l$$

for all $1 \leqslant j \leqslant r_i$ and $1 \leqslant i \leqslant s$, where

$$r_{w'} : A_i\left(L(A_i[l^m])\right) \to A_{i,w}(k_{w'})$$

is the corresponding reduction map.

Proof. It follows immediately from Theorem 6.3 taking $L\left(A[l^m]\right)$ for L and putting $Q_{ij} := P_{ij} - T_{ij}$ for all $1 \leqslant j \leqslant r_i$ and $1 \leqslant i \leqslant t$. ■

7. Proof of Theorem A

By Poincare Irreducibility Theorem there is a finite extension L/K and isogeny $\varphi : A \to A_1^{e_1} \times \cdots \times A_t^{e_t}$ over L where A_i/L is a simple for every $1 \leqslant i \leqslant t$ and A_i is not isogenous to A_j for all $i \neq j$. We can always assume that L/K is Galois. We will use the field L introduced above in the following lemma.

Lemma 7.1. *Let A be an abelian variety over K and $P, P_1, \ldots, P_r$ be nontorsion points in $A(K)$. Let $P_1, \ldots P_r$ be linearly independent over $\mathcal{R}_L := End_L(A)$, $\mathcal{R} := End_K(A)$ and Λ be an $\mathbb{Z}$-submodule generated by $P_1, P_2, \ldots P_r$. Assume that*

$$r_v(P) \in r_v(\Lambda) \tag{7.1}$$

for all closed points v in an open subset $U \subset S$. Then $aP \in \sum_{i=1}^r \mathcal{R}P_i$ for some positive integer a.

Proof. *Case 1.* A a simple abelian variety. We first proof that $P, P_1, \ldots, P_r$ are not linearly independent over $\mathcal{R}$. Indeed, if $P, P_1, \ldots, P_r$ are independent over $\mathcal{R}$ then by theorems 6.3 and 6.4 there is closed point v in U s.t. $r_v(P)$ has big order

and
$r_v(P_i) = 0$ in $A_v(k_v)$ but this contradicts (7.1). Hence there are $\alpha, \alpha_1, \ldots, \alpha_r \in R$ and $\alpha \neq 0$ such that

$$\alpha P = \alpha_1 P_1 + \cdots + \alpha_r P_r \in A(F)$$

Since A is simple there is an isogeny $\widehat{\alpha}$ such that $\widehat{\alpha}\alpha = a \in \mathbb{N}$. Then

$$\widehat{\alpha}\alpha P = \widehat{\alpha}\alpha_1 P_1 + \cdots + \widehat{\alpha}\alpha_r P_r.$$

Hence $aP \in \sum_{i=1}^{r} \mathcal{R} P_i$.

Case 2. $A = A_1 \times \cdots \times A_s$ product of arbitrary simple abelian varieties (We do not assume that A_i's are not pairwise isogenous).

$$P = \begin{bmatrix} P^1 \\ \vdots \\ P^s \end{bmatrix}, \qquad P_i = \begin{bmatrix} P_i^1 \\ \vdots \\ P_i^s \end{bmatrix}$$

Now by lemma 4.2 we know that $\{P_i^j\}_{1 \leqslant i \leqslant r}$ are linearly independent over $\mathcal{R}_j := End(A_j)$ for every $1 \leqslant j \leqslant s$. By assumption (7.1) we get $r_v(P^j) \in \sum_{i=1}^{r} \mathbb{Z} r_v(P_i^j)$ for every $1 \leqslant j \leqslant s$. By Case 1 for every $1 \leqslant j \leqslant s$ there exist $\alpha_j^i \in End_K(A_j)$ and $a_j \in \mathbb{N}$ such that $a_j P^j = \sum_{i=1}^{s} \alpha_i^j P_i^j$. Putting $a := \mathrm{LCM}\{\mathrm{a_j : 1 \leqslant j \leqslant s}\}$ this gives $aP^j = \sum_{i=1}^{s} \beta_i^j P_i^j$ for some $\beta_i^j \in \mathcal{R}_j$. Hence we get

$$a \begin{bmatrix} P^1 \\ \vdots \\ P^s \end{bmatrix} = \sum_{i=1}^{r} \begin{bmatrix} \beta_i^1 & & \cdots & & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & \beta_i^j & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & & \beta_i^s \end{bmatrix} \begin{bmatrix} P_i^1 \\ \vdots \\ P_i^s \end{bmatrix}$$

So $aP \in \sum_{i=1}^{r} \mathcal{R} P_i$

Case 3. A an arbitrary abelian variety. By Poincare irreducibility theorem there is a finite extension L/K and isogeny $\varphi : A \to A_1^{e_1} \times \cdots \times A_s^{e_m}$ over L where A_i is simple for every $1 \leqslant i \leqslant m$ and A_i is not isogenous to A_j for all $i \neq j$. We can work over L since $A(K) \subset A(L)$ and $A_v(k_v) \subset A_v(k_w)$ for every closed point w over v in U_L (See comment after theorem 3.1 concerning the choice of U_L). To make notation easier put $B := A_1^{e_1} \times \cdots \times A_s^{e_m}$. By (7.1) we get the following property for A/L :

$$r_w(P) \in r_w(\Lambda) \tag{7.2}$$

for all closed points w in U_L. The points $\varphi(P), \varphi(P_1), \ldots, \varphi(P_r)$ are nontorsion in $B(L)$ and $\varphi(P_1), \ldots, \varphi(P_r)$ are linearly independent over $\mathcal{R}'_L := End_L(B)$ by asumption. Now by Case 2 we get $a\varphi(P) \in \sum_{i=1}^{r} \mathcal{R}' \varphi(P_i)$ in $B(L)$ for some $a \in \mathbb{N}$. There is an isogeny $\widehat{\varphi} : B \to A$ over L such that $\widehat{\varphi} \circ \varphi = a' \in \mathbb{N}$. Hence we get that

$a'aP \in \mathcal{R}_L P^i + T$ for some and $T \in A(L)_{tor}$. By Theorem 6.3 there are infinitely many $w \in U_L$ such that $r_w(P_i) = 0$ in $A_v(k_w)_l$ for every $1 \leqslant i \leqslant r$. Hence by property (7.2) we get $r_w(T) = 0$ for infinitely many w. But r_w is injection for torsion points (Theorem 2.3) so $T = 0$. Put $b = a'a$. We have $bP = \sum_{i=1}^r \beta_i P_i$ with $\beta_i \in \mathcal{R}_L := End_L(A)$. Recall that we assume that L/K is Galois. Note that since $P, P_1, \dots, P_r \in A(K)$ we get $b|G(L/K)|P = \sum_{i=1}^r Tr_{L/K}(\beta_i)P_i$. But $Tr_{L/K}(\beta_i) \in \mathcal{R}$ for every $1 \leqslant i \leqslant r$ ■

Theorem 7.2. *Let A be an abelian variety over K and $P, P_1, \dots, P_r$ be nontorsion points in $A(K)$. Let $P_1, \dots P_r$ be linearly independent over $\mathcal{R}_L := End_L(A)$ and Λ be a $\mathbb{Z}$-submodule generated by $P_1, P_2, \dots, P_r$. Assume that*

$$r_v(P) \in r_v(\Lambda) \tag{7.3}$$

for all closed points v in an open subset $U \subset S$. Then $P \in \Lambda$.

Proof. By Lemma (7.1) there is $a \in \mathbb{N}$ and $\alpha_i \in \mathcal{R}$ for $1 \leqslant i \leqslant r$ such that

$$aP = \sum_{i=1}^{r} \alpha_i P_i$$

Now we use an argument similar to an argument of [B].

Step 1. If $\alpha_i \in \mathbb{Z}$ for every $1 \leqslant i \leqslant r$ then using Theorem 6.3 the same arguments as of Step 1 of the proof of [B, Theorem 1.1] shows $P \in \Lambda$.

Step 2. Assume that $\alpha_i \notin \mathbb{Z}$ for some $1 \leqslant i \leqslant r$. For any prime number l consider the action of α_i on $T_l(A)$. By [Mi1, Proposition 12.9] we have $P_{\alpha_i}(n) = deg(\alpha_i - n)$ for every $n \in \mathbb{Z}$, where $P_{\alpha_i}(t)$ is the characteristic polynomial of α_i on $T_l(A)$ and $deg : End(A) \to \mathbb{Z}$ is the degree function. Hence $P_{\alpha_i}(t) \in \mathbb{Z}[t]$ and $P_{\alpha_i}(t)$ is monic. Let K be the splitting field of $P_{\alpha_i}(t)$. For any l that splits completely in K we can treat $\mathcal{O}_K$ as a subring of $\mathbb{Z}_l$. If $P_{\alpha_i}(t)$ has at least two different roots then we can easily find a vector $u \in T_l(A)$ which is not an eigenvector of α_i, simply take a sum of two eigenvectors corresponding to different eigenvalues. If $P_{\alpha_i}(t)$ has only one root $\lambda \in \mathcal{O}_K$ then $P_{\alpha_i}(t) = (t - \lambda)^{2g}$ and since $2g\lambda \in \mathbb{Z}$ we have $\lambda \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. By Theorem 5.3 we observe that $\alpha_i \neq \lambda Id_{T_l(A)}$ so the minimal polynomial for α_i on $T_l(A)$ has form $(t - \lambda)^k$ for some $1 < k \leqslant 2g$. Hence also in this case we can find a vector $u \in T_l(A)$ which is not an eigenvector of α_i. Rescaling if necessary, we can assume that $u \notin lT_l(A)$. Hence for $m \in \mathbb{N}$ and m big enough we can see that the coset $u + l^m T_l(A)$ is not an eigenvector of α_i acting on $T_l(A)/l^m T_l(A)$ see [B] proof of Theorem 1. We put $T \in A[l^m]$ to be the image of the coset $u + l^m T_l(A)$ via the natural isomorphism of Galois and $\mathcal{R}$ modules $T_l(A)/l^m T_l(A) \cong A[l^m]$. Put $L := F(A[l^m])$. We can work in $A(L)$. By Theorem 6.3 we choose a closed point w in U_L such that $r_w(P_j) = 0$ for all $j \neq i$ and $r_w(P_i) = r_w(T)$ in $A_w(k_w)_l$. Hence $ar_w(P) = \alpha_i r_w(T)$. By assumption (7.3) there is $d \in \mathbb{Z}$, such that $ar_w(P) = adr_w(P_i) = adr_w(T)$. Since r_w is injective, we get:

$$\alpha_i T = adT \qquad \text{in } A[l^m].$$

But this contradicts the fact that T is not an eigenvector of α_i acting on $A[l^m]$. Hence we must have $\alpha_i \in \mathbb{Z}$ for all $1 \leqslant i \leqslant r$, which is the step 1 of the proof. ■

Proposition 7.3. *Let A be an abelian variety over K. Let $P_1, \dots, P_r$ be elements of $A(F)$ lineraly independent over $\mathcal{R} := \operatorname{End}_K(A)$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$ module. The following conditions are equivalent:*

1. $P \in \sum_{i=1}^r \mathcal{R}P_i$
2. $r_v(P) \in \sum_{i=1}^r \mathcal{R}r_v(P_i)$ *for all closed points v in an open subset $U \subset S$*

Proof. The proof is similar as in [B, Prop 2.8]. ■

8. Support Problem

Theorem 8.1. *Let A/K be an abelian variety defined over a fnitely generated feld K over $\mathbb{Q}$. As before A is the generic fiber of the abelian scheme $\mathcal{A}/S$. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties. Let $P, Q \in A(K)$ be two given points. Suppose that there is an open subset $U \subset S$ such that for all $n \in \mathbb{Z}$ and all closed points $v \in U$, the following condition holds.*

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0$$

Then there exist a positive integer k and an endomorphism $\varphi \in \operatorname{End}_K A \setminus \{0\}$ such that

$$\varphi(P) = kQ$$

Proof. Let

$$P = (P_1, \dots, P_t) \in A(K) \qquad \textit{and} \qquad Q = (Q_1, \dots, Q_t) \in A(K)$$

with $P_i, Q_i \in A_1^{e_i}(K)$ for each $1 \leqslant i \leqslant t$. We can write $P_i := (P_i^j)_{1 \leqslant j \leqslant e_i}, Q_i := (Q_i^j)_{1 \leqslant j \leqslant e_i}$ with $P_i^j, Q_i^j \in A_i(K)$ for all $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant e_i$. Recall that $\mathcal{R} := \operatorname{End} A$ and $\mathcal{R}_i := \operatorname{End} A_i$. Note that $D_i := \operatorname{End} A_i \otimes \mathbb{Q}$ is a division algebra. Hence for each $1 \leqslant i \leqslant t$ we can choose a maximal, linearly independent over $\mathcal{R}_i$ subset $\{P_i^{j_1}, \dots, P_i^{j_{s_i}}\} \subset \{P_i^1, \dots, P_i^{e_i}\}$. Then for every $1 \leqslant i \leqslant t, 1 \leqslant j \leqslant e_i$ there exists $c_{i,j} \in \mathbb{N}$ such that

$$c_{i,j} P_i^j = \sum_{k=1}^{s_i} \beta_k P_i^{j_k} \tag{8.1}$$

Let $c := LCM\{c_{i,j} : 1 \leqslant i \leqslant t, 1 \leqslant j \leqslant e_i.\}$ Assume that for some i and j the points Q_i^j and $P_i^{j_1}, \dots, P_i^{e_i}$ are linearly independent over $\mathcal{R}_i$. Then by Theorem 6.4 we can choose $v \in U$ such that $\operatorname{ord} r_v(P_i^{j_k}) = 0$ and $\operatorname{ord} r_v(Q_i^j)$ has prder lc. Then we see that $cr_v(P) = 0$ so it implies by our assumption that $cr_v(Q) = 0$. But this is a contradiction since the order of $r_v(Q)$ is lc by the choice of $v \in U$.

So for every $1 \leqslant i \leqslant t, 1 \leqslant j \leqslant e_i$. There exists $\alpha_i^j, \beta_i^{j_1}, \dots, \beta_i^{j_{s_i}} \in R_i$ with $\alpha_i^j \neq 0$ such that

$$\alpha_i^j Q_i^j = \sum_{k=1}^{s_i} \beta_i^{j_k} P_i^{j_k}$$

For each $1 \leqslant i \leqslant t$ put $B_i := diag[\alpha_i^1, \ldots, \alpha_i^{e_i}] \in M_{e_i}(\mathcal{R}_i)$. Hence equality (8.1) gives the following equality:

$$\begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B_t \end{bmatrix} Q = \varphi(P)$$

for some $\varphi \in \mathcal{R}$. But for every α_i^j there exists $\widehat{\alpha_i^j}$ such that $\alpha_i^j \circ \widehat{\alpha_i^j} = \widehat{\alpha_i^j} \circ \alpha_i^j = d_i^j$ for some $d_i^j \in \mathbb{N}$. For each $1 \leqslant i \leqslant t$ put $\widehat{B_i} := diag[\widehat{\alpha_i^1}, \ldots, \widehat{\alpha_i^{e_i}}] \in M_{e_i}(\mathcal{R}_i)$ and $D_i := diag[d_i^1, \ldots, d_i^{e_i}] \in M_{e_i}(\mathbb{Z})$. Hence multiplying the equality by the block diagonal matrix

$$\begin{bmatrix} \widehat{B_1} & 0 & \cdots & 0 \\ 0 & \widehat{B_2} & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \widehat{B_t} \end{bmatrix}$$

we get equality

$$\mathbb{D}Q = \varphi_1 P \tag{8.2}$$

for some $\varphi_1 \in \mathcal{R}$, where $\mathbb{D} := \mathrm{diag}[D_1, \ldots, D_t] \in \mathcal{R}$. Since $d_i^j \neq 0$ for all i, j then there are diagonal matrices $D_i' := \mathrm{diag}[d_i^{1\prime}, \ldots, d_i^{e_i\prime}] \in M_{e_i}(\mathbb{Z})$ such that $D_i' D_i = dI_{e_i}$. So multiplying the equality (8.2) by the matrix

$$\begin{bmatrix} D_1' & 0 & \cdots & 0 \\ 0 & D_2' & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & D_t' \end{bmatrix}$$

we get

$$dQ = \varphi_2(P)$$

for $d \in \mathbb{N}$ and some $\varphi_2 \in \mathcal{R}$. ■

Remark 8.2. Let $\varphi : A \to B$ be an isogeny and let $\psi : B \to A$ be the dual isogeny. Let $n := \deg \varphi = \psi \circ \varphi$. There exist lifts $\tilde{\varphi} : \mathcal{A} \to \mathcal{B}$, $\tilde{\psi} : \mathcal{B} \to \mathcal{A}$ to homomorphisms of abelian schemes by [FC] and Theorem Raynaud (see also Section 3) such that $n = \tilde{\psi} \circ \tilde{\varphi}$. Since $n : \mathcal{A} \to \mathcal{A}$ is an isogeny (quasi-finite S-map of abelian schemes over S) then $\tilde{\varphi}$ and $\tilde{\psi}$ are also quasi-finite hence they are isogenies. The map $d : S \to \mathbb{N}$, $d(s) = \deg \tilde{\varphi}_s$ is locally constant. In particular $|\ker \tilde{\varphi}_s| = \deg(\varphi)$ for every $s \in S$. For this reason one defines $\deg(\tilde{\varphi}) := \deg(\varphi)$.

Remark 8.3. Let $\varphi : A \to B$ be an isogeny. Let $P, Q \in A(K)$ any two given points and $U \subset S$ be an open subset such that the following condition holds

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0 \qquad \text{for all } n \text{ and all closed point } v \in U. \tag{8.3}$$

By remark 8.2 it follows that there is $c \in \mathbb{N}$

$$nr_v(\varphi(P)) = 0 \Rightarrow nr_v(\varphi(cQ)) = 0 \qquad \text{for all } n \text{ and all closed point } v \in U. \tag{8.4}$$

Remark 8.4. Let $\varphi : A \to B$ be an isogeny and let $P, Q \in A(K)$. Assume the support theorem holds for the abelian variety B which means that for any P', $Q' \in B(K)$ the condition

$$nr_v(P') = 0 \Rightarrow nr_v(Q') = 0 \qquad \text{for all } n \text{ and all closed point } v \in U. \tag{8.5}$$

implies that there is $b \in \mathbb{N}$ and $\beta \in \operatorname{End}_K(B)$ such that

$$bQ' = \beta P'. \tag{8.6}$$

Hence by Remark 8.3 we have

$$b\varphi(cQ) = \beta\varphi(P) \qquad \text{for same } \beta \in \operatorname{End}_K(B) \text{ and } b \in \mathbb{N} \tag{8.7}$$

Hence

$$[\deg \varphi]bcQ = \widehat{\varphi}\beta\varphi(P),$$

so the support theorem holds for the abelian variety A.

Corollary 8.5. *Let A/K be an abelian variety defined over K. Let $P, Q \in A(K)$ be two given points. Suppose that there is an open subset $U \subset S$ such that for all $n \in \mathbb{Z}$ and all closed points $v \in U$, the following condition holds*

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0.$$

Then there exist a positive integer k and an endomorphism $\varphi \in \operatorname{End}_K A \setminus \{0\}$ such that

$$\varphi(P) = kQ$$

Proof. There exist field L/K such that the isogeny $\varphi : A \to A_1^{e_1} \times \cdots \times A_t^{e_t}$ is defined. Let $c \in \mathbb{N}$ be such that the following condition holds

$$nr_w(\varphi(P)) = 0 \Rightarrow nr_w(cQ) = 0$$

for same $w \in U'$ over v where U' is preimage of U for the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ such that R' is integral closure of R in L. Let $B = \prod_{i=1}^{t} A_i^{e_i}$. Now from Theorem 8.1 there exists $C \in \mathbb{Z}$ and endomorphism $\beta \in \operatorname{End}_L(B)$ such that

$$C\varphi(cQ) = \beta\varphi(P).$$

Let $\widetilde{\varphi}$ be a dual isogeny such that

$$[deg\varphi]CcQ = \widetilde{\varphi}\beta\varphi(P).$$

Now using method from the proof of Theorem 8.1 we get

$$kQ = \alpha P$$

for same $k \in \mathbb{Z} \setminus \{0\}$ and $\alpha \in \operatorname{End}_K(A) \setminus \{0\}$. ■

Theorem 8.6. *Let A/K be an abelian variety defined over K. Let $P_0, P_1, \ldots, P_n$, $Q_0, Q_1, \ldots, Q_n \in A(K)$ be the points of infinite order. Assume that the following condition holds:*

There is an open set $U \subset S$ such that for every set of nonnegative integers $m_1, \ldots, m_n$ and for all closed points $v \in U$, the following condition holds.

$$r_v(P_0) = \sum_{i=1}^{n} m_i r_v(P_i) \qquad \textit{implies} \qquad r_v(Q_0) = \sum_{i=1}^{n} m_i r_v(Q_i)$$

Then there exist $\alpha_i \in \operatorname{End}_K(A) \setminus \{0\}$ and $k \in \mathbb{N} \setminus \{0\}$ such that $\alpha_i P_i = k_i Q_i$ for all $i = 0, 1, \ldots, n$.

Proof. Assume that $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$ where A_i is simple and not isogenous to A_j for all $j \neq i$. We use the same notation as in the proof of Theorem 8.1.

$$P_0 = \left[P_1^{j_1}, \ldots, P_t^{j_t}\right]_{1 \leqslant j_1 \leqslant e_1, \ldots, 1 \leqslant j_t \leqslant e_t}, \qquad Q_0 = \left[Q_1^{j_1}, \ldots, Q_t^{j_t}\right]_{1 \leqslant j_1 \leqslant e_1, \ldots, 1 \leqslant j_t \leqslant e_t},$$

and $\mathcal{R} := \operatorname{End}_K A$, $\mathcal{R}_i := \operatorname{End}_K A_i$. Because m_i is any nonnegative integer we can take $m_i = 0$ for all i. Then we have

$$r_v(P_0) = 0 \Rightarrow r_v(Q_0) = 0$$

Using the same method as in proof of Theorem 8.1 we get

$$k_0 Q_0 = \alpha_0 P_0, \qquad \text{for } k_0 \in \mathbb{N} \setminus \{0\},\ \alpha_0 \in \mathcal{R} \setminus \{0\}.$$

Now fix $m_i = 1$ and $m_j = 0$ for all $j \neq i$. We get

$$r_v(P_i) = r_v(P_0) \Rightarrow r_v(Q_i) = r_v(Q_0).$$

Let $l \nmid k_0$. We show that P_i and Q_i are linearly dependent in $A(K)$. Assume that P_i and Q_i are linearly independent in $A(K)$ over $\mathcal{R}$. By the Theorem 6.3 there exists $v \in U$ such that $r_v(P_i) = 0$ and $r_v(Q_i) \neq 0$ in $\mathcal{A}_v(k_v)_l$. But the point P_0 and Q_0 are linearly dependent, hence

$$0 = r_v(P_i) = r_v(P_0) = r_v(Q_0) = r_v(Q_i) \neq 0$$

So the point P_i and Q_i are linearly dependent. Again we use methods from proof of Theorem 8.1 and Corollary 8.5. This finishes the proof. ■

References

[B] G. Banaszak, *On a Hasse principle for Mordel–Weil groups*, Comptes Rendus Mathematique **347** (2009), 709–714.

[BGK1] G. Banaszak, W. Gajda, P. Krasoń, *Detecting linear dependence by reduction maps*, Journal of Number Theory **115**(2) (2005), 322–342.

[BGK2] G. Banaszak, W. Gajda, P. Krasoń, *On reduction map for étale K–theory of curves*, Homology, Homotopy and Applications, Proceedings of Victor's Snaith 60th Birthday Conference **7**(3) (2005), 1–10.

[BGK3] G. Banaszak, W. Gajda, P. Krasoń, *Support problem for the intermediate jacobians of l–adic representations*, Journal of Number Theory **100** (2000), 133–168.

[BK] G. Banaszak, P. Krasoń, *On arithmetic in Mordell–Weil groups*, Acta Arithmetica **150** (2011), no. 4, 315–337.

[Bar] S. Barańczuk, *On reduction maps and support problem in K–theory and abelian varieties*, Journal of Number Theory **119** (2006), 1–17.

[Co] Edited by Gary Cornell Joseph H. Silverman *Arithmetic Geometry* Springer–Verlag, New York Berlin Heidelberg London Paris Tokyo, 1986.

[C-RS] C. Corralez–Rodrigáñez, R. Schoof, *Support problem and its elliptic analogue*, Journal of Number Theory **64** (1997), 276–290.

[F1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. Math. **73** (1983), 349–366.

[F2] G. Faltings, *Complements to Mordell*, Rational points. Seminar Bonn/Wuppertal 1983/1984 A publication of the Max-Planck-Instutute für Mathematik, Bonn, Aspects of Mathematics, Vieweg (1992), 203–227.

[FC] G. Faltings, C.-L. Chai, *Degeneration of abelian varieties* Springer-Verlag.

[FW] G. Faltings, G. Wüstholz, *Rational Points* A publication of the Max-Planck-Instutute für Mathematik, Bonn, Seminar Bonn/Wuppertal 1983/84, 1992.

[GG] W. Gajda, K. Górnisiewicz, *Linear dependence in Mordell–Weil groups*, Journal für die Reine und Angew. Math. **630** (2009), 219–233.

[J] P. Jossen, *Detecting linear dependence on a simple abelian variety*, to appear in the Comment. Math. Helv.

[JP] P. Jossen, A. Perucca, *A counterexample to the local–global principle of linear dependence for abelian varieties*, arXiv:0905.0409v1 [math.NT] 4 May 2009.

[K] N.M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502.

[Kh] C. Khare, *Compatible systems of mod p Galois rpresentations and Hecke characters.*, Math. Res. Letters **10** (2003), 71–83.

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

[L] S. Lang, *Number theory III, diophantine geometry* Springer–Verlag (1991).

[Lar] M. Larsen, *The support problem for abelian varieties*, J. Numbers **101** (2003) 398–403.

[Mi1] J.S. Milne, *Abelian varieties*, Arithmetic Geometry, G. Cornell, J.H. Silverman eds. 103–150, Springer-Verlag (1986).

[Mi2] J.S. Milne, *Étale cohomology*, Princeton Univ. Press 1980.

[Pe1] A. Perucca, *Two variants of the support problem for products of abelian varieties and tori*, J. Number Theory **129** (2009), 1883–1892.

[Pe2] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. of Number Theory **129** (2009), 469–476.

[Ri] K.A. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Mathematical Journal **46**(4) (1979), 745–761.

[Sch] A. Schinzel, *On power residues and exponential congruences*, Acta Arithmetica **27** (1975), 397–420.

[Se1] J.-P. Serre, Lettre á Ken Ribet du 7/3/1986 *Lettre á Ken Ribet du 7/3/1986.*

[Se2] J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes. II*, Izviestia Akademii Nauk CCCP, Seria mat. **35** (1971), 731–737.

[Se3] J.-P. Serre, *Zeta and L function*, Arithmetical Algebraic Geometry, Harper and Row, New York (1965), 82–92.

[S-Z] A. Skorobogatov, Yu.G. Zarhin, *A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces*, J. Algebraic Geometry **17** (2008) 481–502.

[Sil] J. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.

[ST] *Stacks Project*, last version 2013.

[T] J. Tate, *Relation between K_2 and Galois cohomology* Invent. Math. **36** (1976), 257–274.

[We] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell–Weil groups*, Acta Arithmetica **110** (2003), 77–88.

[Za] J.G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. math. **79** (1985), 309–321.

Address: Piotr Rzonsowski: Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland.

E-mail: rzonsol@amu.edu.pl

Received: 3 September 2013; **revised:** 16 September 2013