DETECTING LINEAR DEPENDENCE BY REDUCTION MAPS

G. Banaszak, W. Gajda, P. Krasoń

Abstract. We consider the local to global principle for detecting linear dependence of points in groups of the Mordell-Weil type. As applications of our general setting we obtain corresponding statements for Mordell-Weil groups of non-CM elliptic curves and some higher dimensional abelian varieties defined over number fields, and also for odd dimensional K-groups of number fields.

1. Introduction.

Let E be an elliptic curve defined over a number field F. By the classical theorems of Mordell and Weil the group $E(F)$ of F-rational points is finitely generated. The torsion part of $E(F)$ can be computed quite efficiently in many cases: for $F{=}\mathbb{Q}$ due to results of Lutz, Nagell and Mazur (see, for example [G-SOT]) and for some larger F due to results of Kamienny, Merel and others. One of the basic facts which are useful in calculations of the torsion is the reduction theorem [Si, Prop. 3.1, p.176] which says that the reduction map:

$$r_v : E(F) \longrightarrow E_v(\kappa_v)$$

(where $\kappa_v{=}\mathcal{O}_F/v$) is an injection, when restricted to the torsion subgroup, for all primes v of good reduction. On the other hand, it is well-known that the rank of $E(F)$ is much more difficult to compute (cf. [RS] for an up-to-date survey on the ranks of $E(F)$, when $F{=}\mathbb{Q}$).

One of our goals in this paper is to show that the reduction maps can be used to investigate the nontorsion part of the Mordell-Weil group. Given a finite set of nontorsion points of $E(F)$, one can ask whether it is possible to detect linear dependence among elements of this set by reductions. Similar questions are of interest for the Mordell-Weil group of any higher dimensional abelian variety over F, and also more generally - if we are given a finitely generated abelian group $B(F)$ together with maps $r_v : B(F) \longrightarrow B_v(\kappa_v)$ to finite groups - one map for every finite prime of F. A good example of this situation is provided by Quillen's K-groups $K_{2n+1}(F)$, where $n \geq 0$, and the homomorphisms

$$r_v : K_{2n+1}(F) \longrightarrow K_{2n+1}(\kappa_v).$$

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

induced by projections $\mathcal{O}_F \longrightarrow \kappa_v$. Note that $K_{2n+1}(F)=K_{2n+1}(\mathcal{O}_F)$, for $n > 0$ and the K-group is finitely generated cf. [Q1]. Its rank equals the order of vanishing of the Dedekind zeta function of F at $s = -n$ cf. [B]. In this case the target of the reduction map r_v is the cyclic group $\mathbb{Z}/(q_v^{n+1}-1)$, where q_v denotes the number of elements of the residue field cf. [Q2]. According to the conjecture of Quillen and Lichtenbaum the map to the continuous Galois cohomology

$$K_{2n+1}(F) \otimes \mathbb{Z}_l \longrightarrow H^1(G_{F,S_0}, \mathbb{Z}_l(n+1))$$

constructed by Dwyer and Friedlander in [DF], should be an isomorphism, for all odd l. Here we have denoted by $G_{F,S_0}=G(F_{S_0}/F)$ the Galois group of the maximal extension F_{S_0}/F contained in $\bar{F}$, which is unramified outside of l.

In this paper we apply an axiomatic setup (see Section 2 for the details) which embraces simultaneously the Mordell-Weil groups of elliptic curves (or rather, of all abelian varieties with commutative endomorphism algebras) and K-groups of number fields. Let $\mathcal{O}$ be a ring with unity. We use the general framework of the Mordell-Weil systems $\{B(L)\}_L$ of finitely generated left $\mathcal{O}$-modules, indexed by finite extensions L/F, which was developed in [BGK2] for the solution of the support problem for l-adic representations. One part of the structure of the Mordell-Weil system is a collection of well-behaved maps taking values in the Selmer groups defined by Bloch and Kato [BK] in the Galois cohomology of $G(\bar{F}/F)$. In the case of $E(F)$ these maps are induced by the classical Kummer homomorphisms, whereas for K-groups they are given by the Dwyer-Friedlander maps.

Our main results concern linear dependence of nontorsion points in $B(F)$. We assume that the system $\{B(L)\}_L$ and the Galois representation in question meet the assumptions formulated in Section 2.

Theorem A. *[Theorem 3.12]*
Let P and $P_1, \ldots, P_r$ be nontorsion elements of $B(F)$ such that $P_1, P_2, \ldots, P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the submodule of $B(F)$ generated by $P_1, P_2, \ldots, P_r$. The following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

In addition to the methods of [BGK2], in the proof of Theorem A we used the Kummer theory over division fields which was developed by Ribet in [Ri]. The main technical result of the paper is Theorem 3.1. In the first part of its proof (Step 1) we applied an argument due to Khare and Prasad (cf. [KP], Lemma 5) extended to the context of the Mordell-Weil systems.

In the case of the K-group $K_{2n+1}(F)$, where $n \geq 0$ and F is a number field, we put $B(F)=K_{2n+1}(F)/C_F$, where C_F is the subgroup of $K_{2n+1}(F)$ generated by l-parts, of kernels of the Dwyer-Friedlander maps, for all primes l. Note that C_F is

a finite group by [DF], and if the Quillen-Lichtenbaum conjecture holds true, then $B(F)$=$K_{2n+1}(F)$. Theorem A applied to this case implies Theorem 4.1, which for two points, i.e., if r=1, was proven already in [BGK1].

Theorem B. *[Theorem 4.1]*
Let P and P_1, P_2, ..., P_r be nontorsion elements of $K_{2n+1}(F)/C_F$, such that P_1, P_2, ..., P_r are linearly independent over $\mathbb{Z}$. Let $\Lambda \subset K_{2n+1}(F)/C_F$ denote the subgroup generated by $P_1, P_2, \ldots, P_r$. The following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

If $n = 0$, then Theorem B gives the statement about the multiplicative group of the field F, which was previously proven by Khare, [K], Proposition 3, p.10.

The problem which we consider in this paper is motivated by the support problem of Erdös and also by our papers [BGK1] and [BGK2] on the generalization of the Erdös problem to l-adic Galois representations. The support problem for an abelian variety A cf. [C-SR, p.277] is the following question: *are the points $P, P_1 \in A(F)$ related over the endomorphism algebra of A, if the order of $r_v(P) \in A_v(\kappa_v)$ divides the order of $r_v(P_1)$, for almost all v ?* Note that the groups $A_v(\kappa_v)$ are not necessarly cyclic, and therefore our problem for A and r=1, is essentially different from the support problem for A. We would like to mention that Michael Larsen has recently given a solution of the support problem for all abelian varieties cf. [L].

In the case of abelian varieties Theorem A provides the complete solution of the problem of detecting linear dependence of nontorsion points by reductions for the class of abelian varieties for which Serre proved in [Se1] the analog of the open image theorem.

Theorem C. *[Theorem 4.2]*
Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1, \ldots, P_r$ be nontorsion elements of $A(F)$ such that $P_1, P_2, \ldots, P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1, P_2, \ldots, P_r$. Then the following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F, where $r_v : A(F) \longrightarrow A_v(\kappa_v)$ are the reduction maps.*

In particular, the Mordell-Weil group $E(F)$ of any non-CM elliptic curve E defined over the number field F has the property stated in Theorem C, i.e., our initial question has a positive answer for such curves (cf. Corollary 4.3). We hope that in the case of elliptic curves defined over $\mathbb{Q}$, Theorem C will find some practical implementations.

While this paper was being prepared we have learned that Tom Weston has proven by a different method a result similar to our Theorem 2.9, for all abelian varieties with commutative algebras cf. [We], Corollary. 2.8.

2. Kummer theory for l-adic representations.

Notation.

l	is a prime number
F	is a number field, $\mathcal{O}_F$ its ring of integers
G_F	$= G(\bar{F}/F)$
v	denotes a finite prime of $\mathcal{O}_F$, κ_v=$\mathcal{O}_F/v$ denotes the residue field at v
g_v	$= G(\overline{\kappa}_v/\kappa_v)$
T_l	denotes a free $\mathbb{Z}_l$-module of finite rank d
V_l	$= T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$
A_l	$= V_l/T_l$
ρ_l :	$G_F \to GL(T_l)$ is a Galois representation unramified outside a fixed finite set S_l of primes of $\mathcal{O}_F$ containing all primes above l
$\overline{\rho_{l^k}}$	denotes the residual representation $G_F \to GL(T_l/l^k)$ induced by ρ_l
F_{l^k}	$= F(A_l[l^k])$, for any $k > 0$, denotes the number field $\bar{F}^{ker\overline{\rho_{l^k}}}$
F_{l^∞}	$= \bigcup_k F_{l^k}$
G_l	$= G(F_l/F)$
G_{l^k}	$= G(F_{l^k}/F)$
G_{l^∞}	$= G(F_{l^\infty}/F)$
H_{l^k}	$= G(\overline{F}/F_{l^k})$
H_{l^∞}	$= G(\overline{F}/F_{l^\infty})$
$C[l^k]$	denotes the subgroup of l^k-torsion elements of an abelian group C
C_l	$= \bigcup_{k\geq 1} C[l^k]$, is the l-torsion subgroup of C.

Let L/F be a finite extension and w a finite prime in L. To indicate that w is not over any prime in S_l we will write $w \notin S_l$, slightly abusing notation. Let $\mathcal{O}$ be a ring with unity which acts on T_l in such a way that the action commutes with the G_F-action. Unless specified otherwise (see paragraph after Lemma 3.11), all modules over the ring $\mathcal{O}$, which we consider in this paper, are left $\mathcal{O}$-modules. Let $\{B(L)\}_L$ be a direct system of finitely generated $\mathcal{O}$-modules indexed by all finite field extensions L/F. The structure maps of the system are induced by inclusions of fields. We assume that for every embedding $L \to L'$ of extensions of F, the structure map $B(L) \to B(L')$ is a homomorphism of $\mathcal{O}$-modules. Similarly, for every prime v of F we define a direct system $\{B_v(\kappa_w)\}_{\kappa_w}$ of $\mathcal{O}$-modules where κ_w is a residue field for a prime w over v in a finite extension L/F. We require that G_F acts on both systems: $\{B(L)\}_L$ and $\{B_v(\kappa_w)\}_{\kappa_w}$ functorially. Let us put $B(\overline{F}) = \varinjlim_{L/F} B(L)$. We assume that the actions of G_F and $\mathcal{O}$ have the following properties:

- (A_1) for each l, each finite extension L/F and any prime w of L, such that $w \notin S_l$, we have $T_l^{Fr_w} = 0$, where $Fr_w \in g_w$ denotes the arithmetic Frobenius at w.

(A_2) for every L and $w \notin S_l$ there are natural maps $\psi_{l,L}$, $\psi_{l,w}$ and r_w respecting G_F and $\mathcal{O}$ actions such that the diagram commutes:

$$\begin{array}{ccc} B(L)\otimes\mathbb{Z}_l & \xrightarrow{r_w} & B_v(\kappa_w)_l \\ {\scriptstyle\psi_{l,L}}\downarrow & & \cong\downarrow{\scriptstyle\psi_{l,w}} \\ H^1_{f,S_l}(G_L,T_l) & \xrightarrow{r_w} & H^1(g_w,T_l) \end{array} \tag{2.1}$$

where $H^1_{f,S_l}(G_L,T_l)$ is the group defined by Bloch and Kato (cf.[BK], see also [BGK2]). The left (resp., the right) vertical arrow in the diagram (2.1) is an embedding (resp., an isomorphism) for every L (resp., for every $w \notin S_l$)

(A_3) for every L the map $\psi_{l,L}$ is an isomorphism for almost all l or $B(\overline{F})$ is a discrete G_F-module divisible by l, for almost all l, and for every L we have: $B(\overline{F})^{G_L} \cong B(L)$ and $H^0(G_L;A_l) \subset B(L)$.

For a point $R \in B(L)$ (resp., a subgroup $\Gamma \subset B(L)$) we denote $\hat{R} = \psi_{l,L}(R)$ (resp. $\hat{\Gamma}$=$\psi_{l,L}(\Gamma)$). As in [Ri] we impose the following four axioms on the representations which we consider:

(B_1) $End_{G_l}(A_l[l]) \cong \mathcal{O}/l\mathcal{O}$, for almost all l and
$End_{G_{l^\infty}}(T_l) \cong \mathcal{O}\otimes\mathbb{Z}_l$, for all l

(B_2) $A_l[l]$ is a semisimple $\mathbb{F}_l[G_l]$-module, for almost all l and
V_l is a semisimple $\mathbb{Q}_l[G_{l^\infty}]$-module, for all l

(B_3) $H^1(G_l;A_l[l])=0$, for almost all l and
$H^i(G_{l^\infty};T_l)$ are finite groups, for all l and all $i \geq 0$

(B_4) for each finitely generated subgroup $\Gamma \subset B(F)$ the group

$$\Gamma' = \{P \in B(F) : mP \in \Gamma \quad \text{for some} \quad m \in \mathbb{N}\}$$

is such that Γ'/Γ has a finite exponent.

Note that in the case of the Tate module of an abelian variety, the conditions (A_1)-(A_3) were checked in [BGK2], Section 3. The conditions (B_1)-(B_4) are fulfiled in this case due to theorems of Faltings, Zarhin and Serre (cf. the proof of Theorem 4.2). In the sequel we assume that $\mathcal{O}$ is a finitely generated free $\mathbb{Z}$-module.

The next lemma describes the relation between conditions in the assumption (B_1).

Lemma 2.2. *If $End_{G_l}(A_l[l]) \cong \mathcal{O}/l\mathcal{O}$, then $End_{G_{l^\infty}}(T_l) \cong \mathcal{O}\otimes\mathbb{Z}_l$.*

Proof. We prove by induction that for every $k > 0$ we have $End_{G_{l^k}}(A_l[l^k]) \cong \mathcal{O}/l^k\mathcal{O}$. Assume that the claim is true for k=$1,2,\ldots,i-1$. Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & End_{G_{l^{i-1}}}(A_l[l^{i-1}]) & \longrightarrow & End_{G_{l^i}}(A_l[l^i]) & \xrightarrow{p} & End_{G_l}(A_l[l]) & \longrightarrow & 0 \\ & & \cong\uparrow & & {\scriptstyle s}\uparrow & & \cong\uparrow & & \\ 0 & \longrightarrow & \mathcal{O}/l^{i-1}\mathcal{O} & \longrightarrow & \mathcal{O}/l^i\mathcal{O} & \xrightarrow{p'} & \mathcal{O}/l\mathcal{O} & \longrightarrow & 0. \end{array}$$

The map p in the diagram is a surjection, since p' is a surjection. Hence, s is an isomorphism. The lemma follows by taking inverse limit over k. $\square$

Let Λ be a finitely generated $\mathcal{O}$-submodule of $B(F)$. Throughout the paper we assume that the points $P_1, \ldots, P_r$ constitute a basis of Λ over $\mathcal{O}$ i.e., they give an $\mathcal{O}$-isomorphism $\Lambda \cong \mathcal{O}^r$. Let $\overline{P}_i$ denote the image of P_i in $\Lambda/l\Lambda$. It is clear that $\overline{P}_1, \ldots, \overline{P}_r$ form a basis of the module $\Lambda/l\Lambda$ over $\mathcal{O}/l\mathcal{O}$.

In the remainder of this section, following [Ri] we introduce the Kummer theory for the l-adic representations which meet our assumptions. For $P \in B(F)$ and $k > 0$ we have the Kummer maps:

$$\phi_P^{(k)} : H_{l^k} \longrightarrow A_l[l^k] \tag{2.3}$$
$$\phi_P^{(k)}(\sigma) = \sigma(\frac{1}{l^k}\hat{P}) - \frac{1}{l^k}\hat{P}.$$

We define:

$$\Phi^{(k)} : H_{l^k} \longrightarrow \bigoplus_{i=1}^{r} A_l[l^k]$$
$$\Phi^{(k)} = (\phi_{P_1}^{(k)}, ..., \phi_{P_r}^{(k)}).$$

One checks easily that, for every $k > 1$, the following diagram commutes:

$$\begin{array}{ccc} H_{l^k} & \xrightarrow{\phi_P^{(k)}} & A_l[l^k] \\ \downarrow & & \downarrow \times l \\ H_{l^{k-1}} & \xrightarrow{\phi_P^{(k-1)}} & A_l[l^{k-1}]. \end{array} \tag{2.4}$$

Taking the inverse limits over k in (2.4) we obtain a map:

$$\phi_P^{(\infty)} : H_{l^\infty} \longrightarrow T_l(A),$$

which we denote briefly $\phi_i := \phi_{P_i}^{(\infty)}$. We define:

$$\Phi : H_{l^\infty} \longrightarrow \bigoplus_{i=1}^{r} T_l$$
$$\Phi = (\phi_1, \ldots, \phi_r).$$

Consider the field $F_l(\frac{1}{l}\hat{\Lambda}) := \overline{F}^{ker\ \Phi^{(1)}}$ and the map induced by $\Phi^{(1)}$:

$$G(F_l(\frac{1}{l}\hat{\Lambda})/F_l) \longrightarrow \bigoplus_{i=1}^{r} A_l[l] \tag{2.5}$$

cf. [BGK2], (4.13). Since $\overline{P}_1, \ldots, \overline{P}_r$ is a basis of $\Lambda/l\Lambda$ over $\mathcal{O}/l\mathcal{O}$, the same argument as in [Ri], Theorem 1.2, shows that, for every l, the map (2.5) is an isomorphism of G_l-modules.

Lemma 2.6. *For almost all l, there exists an isomorphism of $\mathcal{O}/l\mathcal{O}$-modules:*

$$\Lambda/l\Lambda \longrightarrow Hom_{G_l}(G(F_l(\frac{1}{l}\hat{\Lambda})/F_l); A_l[l]). \tag{2.7}$$

Proof. By Kummer theory the map $P \mapsto \phi_P$ induces a homomorphism:

$$B(F)/lB(F) \longrightarrow Hom_{G_l}(H_l;\, A_l[l]) = H^1(H_l;\, A_l[l])^{G_l}$$

which fits into the commutative diagram:

$$\begin{array}{ccc} \Lambda/l\Lambda & \longrightarrow & Hom_{G_l}(G(F_l(\frac{1}{l}\hat{\Lambda})/F_l); A_l[l]) \\ \downarrow & & \downarrow \\ B(F)/lB(F) & \longrightarrow & Hom_{G_l}(H_l;\, A_l[l]) \\ \downarrow & & = \downarrow \\ H^1(G_F;\, A_l[l]) & \xrightarrow{res} & H^1(H_l;\, A_l[l])^{G_l} \end{array} \tag{2.8}$$

as the middle horizontal map. The map (2.7) is the upper horizontal map in the diagram (2.8). The lower horizontal map is the restriction. By the inflation-restriction sequence in Galois cohomology, the kernel of res is contained in $H^1(G_l;\, A_l[l])$ which vanishes, for almost all l, by the axiom (B_3). The left-lower vertical map in (2.8) is injective by (A_3). The left-upper vertical arrow is an injection for almost all l by (B_4). This shows that the map (2.7) is an imbedding for almost all l. Comparing the dimensions over $\mathbb{Z}/l\mathbb{Z}$, we conclude by the axiom (B_1) and the isomorphism (2.5), that the map (2.7) is an isomorphism of $\mathcal{O}/l\mathcal{O}$-modules, for almost all l. □

Theorem 2.9.
Let $P \in B(F)$ be such that for almost all primes v of F, we have $r_v(P) \in r_v(\Lambda)$. Then there is a natural number a such that $aP \in \Lambda$.

Proof. Let Λ_1 be the $\mathcal{O}$-submodule of $B(F)$ generated by P. We consider the Galois extensions $F_l(\frac{1}{l}\hat{\Lambda})/F$ and $F_l(\frac{1}{l}\hat{\Lambda}_1)/F$, where $F_l(\frac{1}{l}\hat{\Lambda}_1) := \overline{F}^{ker\, \phi_P^{(1)}}$. Assume that v splits completely in $F_l(\frac{1}{l}\hat{\Lambda})/F$. Let w' be any prime over v in $F_l(\frac{1}{l}\hat{\Lambda})/F$. We have $\kappa_{w'} = \kappa_v$, hence $g_{w'} = g_v$. Therefore $r_{w'}(\frac{1}{l}\hat{\Lambda}) \in H^1(g_v, T_l)$. Let w be any prime of $F_l(\frac{1}{l}\hat{\Lambda}_1)$ over v. Hence, by the assumption $r_w(\frac{1}{l}\hat{\Lambda}_1) \in H^1(g_v, T_l)$. Let $\hat{R}$ be any point in $\frac{1}{l}\hat{\Lambda}_1$. Since $Fr_w(\hat{R}) = \hat{R} + \hat{P}_0$, for some $\hat{P}_0 \in A_l[l]$, we have:

$$r_w(\hat{R}) = Fr_w r_w(\hat{R}) = r_w Fr_w(\hat{R}) = r_w(\hat{R}) + r_w(\hat{P}_0).$$

By [BGK2], Lemma 2.13 and the axiom (A_1) we obtain $\hat{P}_0 = 0$. This means that v splits completely in the field $F_l(\frac{1}{l}\hat{\Lambda}_1)$. By the Frobenius density theorem [J], Corollary 5.5, p.136, we get:

$$F_l(\frac{1}{l}\hat{\Lambda}_1) \subset F_l(\frac{1}{l}\hat{\Lambda}). \tag{2.10}$$

Hence, by the isomorphism (2.7) applied to Λ and Λ_1, and the inclusion (2.10) we obtain the diagram:

$$\begin{array}{ccc} \Lambda_1/l\Lambda_1 & \longrightarrow & Hom_{G_l}(G(F_l(\frac{1}{l}\hat{\Lambda}_1)/F_l); A_l[l]) \\ \downarrow & & \downarrow \alpha \\ \Lambda/l\Lambda & \longrightarrow & Hom_{G_l}(G(F_l(\frac{1}{l}\hat{\Lambda})/F_l); A_l[l]), \end{array} \tag{2.11}$$

where the left vertical arrow is defined to make the diagram (2.11) commute. Since α is injective by (2.10), we obtain an inclusion:

$$\Lambda_1/l\Lambda_1 \subset \Lambda/l\Lambda.$$

Put $B_0 = B(F)/\Lambda$. By (2.11) we see that P maps to zero in B_0/lB_0. Hence, by the axiom (B_4) we get that $P - Q \in (B_0)_{tor}$, for some $Q \in \Lambda$. This proves the theorem, if we take for a the exponent of the finite group $(B_0)_{tor}$. $\square$

Lemma 2.12. *If $\alpha_1, \ldots, \alpha_r \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ are such that $\alpha_1\phi_1 + \cdots + \alpha_r\phi_r = 0$, then $\alpha_1 = \cdots = \alpha_r = 0$.*

Proof. Let Ψ be the composition of maps:

$$B(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow H^1(G_F : T_l) \longrightarrow H^1(H_{l^\infty}; T_l).$$

Note that $H^1(H_{l^\infty}; T_l) = Hom(H_{l^\infty}; T_l)$ and $\Psi(P_i \otimes 1) = \phi_i$. By (B_3) we have $ker\,\Psi \subset (B(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l)_{tor}$. Let $t := \#B(F)_{tor}$. Since Ψ is an $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$-homomorphism, we have:

$$0 \quad = \quad \alpha_1\phi_1 + \cdots + \alpha_r\phi_r \quad = \quad \Psi(\alpha_1(P_1 \otimes 1) + \cdots + \alpha_r(P_r \otimes 1)).$$

Hence, $\Sigma_{j=1}^r \alpha_j(P_j \otimes 1) \in (B(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l)_{tor}$, so:

$$t\alpha_1(P_1 \otimes 1) + \cdots + t\alpha_r(P_r \otimes 1) = 0$$

in $B(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l$. Observe that the points $P_1 \otimes 1, \ldots, P_r \otimes 1$ are linearly independent over $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ in $B(F) \otimes_{\mathbb{Z}} \mathbb{Z}_l$. This implies that $t\alpha_j = 0$ for $j = 1, \ldots, r$. Hence,

$$\alpha_1 = \cdots = \alpha_r = 0,$$

because $\mathcal{O}$ is a free $\mathbb{Z}$-module, by assumption. $\square$

Lemma 2.13. *The image of the map Φ is open in $\bigoplus_{i=1}^r T_l$ in the topology induced from the natural topology on $\mathbb{Z}_l$.*

Proof. It is enough to show that $Im\,\Phi$ has a finite index in $\bigoplus_{i=1}^r T_l$. The proof follows the lines of the proof of [Ri, Th. 1.2]. Let $W = \bigoplus_{i=1}^r V_l$ and $M = Im(\Phi \otimes 1) \subset W$, where $V_l = T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Both M and W are $\mathbb{Q}_l[G_{l^\infty}]$-modules. First we will show that $\Phi \otimes 1$ is onto. Suppose it is not. By (B_2) we have a nontrivial decomposition $W = M \oplus M_1$ of $\mathbb{Q}_l[G_{l^\infty}]$-modules. Let $\pi_i : W \to V_l$ be a projection that maps M_1 nontrivially. By the axiom (B_1) we have:

$$\pi_i(v_1, \ldots, v_r) = \sum_{j=1}^r \beta_j v_j,$$

for some $\beta_j \in \mathcal{O} \otimes \mathbb{Q}_l$. Since π_i is nontrivial, we see that some β_j is nonzero. On the other hand

$$\pi_i(\Phi \otimes 1)(h) = \sum_{j=1}^r \beta_j(\phi_j(h) \otimes 1) = 0,$$

for all $h \in H_{l^\infty}$. Since $\beta_j \in \mathcal{O} \otimes \mathbb{Q}_l$, we can multiply the last equality by a suitable power l^k to get:

$$0 = \sum_{j=1}^r \alpha_j(\phi_j(h) \otimes 1),$$

where $\alpha_j = l^k \beta_j \in \mathcal{O} \otimes \mathbb{Z}_l$. Since the maps:

$$\mathcal{O} \otimes \mathbb{Z}_l \hookrightarrow \mathcal{O} \otimes \mathbb{Q}_l$$

$$Hom(G_{l^\infty}, T_l) \hookrightarrow Hom(G_{l^\infty}, V_l)$$

are imbeddings of $\mathcal{O} \otimes \mathbb{Z}_l$-modules, we obtain: $\sum_{j=1}^r \alpha_j \phi_j = 0$. By Lemma 2.12 this shows:

$$\alpha_1 = \cdots = \alpha_r = 0,$$

a contradiction. Therefore we have $M_1 = 0$. Since both $\bigoplus_{i=1}^r T_l$ and $Im\,\Phi$ are $\mathbb{Z}_l$-lattices in $\bigoplus_{i=1}^r V_l$, we see that $Im\,\Phi$ has a finite index in $\bigoplus_{i=1}^r T_l$, as required. □

3. Main Results.

In this section we show that for some $\{B(L)\}_L$, one can choose a=1 in Theorem 2.9. Let $\mathcal{G}_l^{alg}$ be the Zariski closure of the image of ρ_l in the algebraic group $GL_d/\mathbb{Z}_l$, endowed with the unique structure of the reduced, closed group subscheme. The next proposition is the main technical result of the paper.

Theorem 3.1.
Assume that $\rho_l(G_F)$ is open in $\mathcal{G}_l^{alg}(\mathbb{Z}_l)$ in the topology induced from $\mathbb{Z}_l$. In addition, assume that $\rho_l(G_F)$ contains an open subgroup of the group of homotheties and that the reduction map $\mathcal{G}_l^{alg}(\mathbb{Z}_l) \to \mathcal{G}_l^{alg}(\mathbb{Z}/l^k)$ is onto, for every $k > 0$. Let $P_1, \ldots, P_r \in B(F)$ be points of infinite order, which are linearly independent over $\mathcal{O}$. Let

$$I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, r\}$$

be any subset of indeces and let

$$J = \{j_1, \ldots, j_{r-s}\} \subset \{1, \ldots, r\}$$

be such that $I \cap J = \emptyset$ and $I \cup J = \{1, \ldots, r\}$. Then for any natural M, and for any prime l, there are infinitely many primes v, such that the images of the points $P_{i_1}, \ldots, P_{i_s}$ via the map:

$$r_v \,:\, B(F) \to B_v(\kappa_v)_l$$

are trivial and the images of the points $P_{j_1}, \ldots, P_{j_{r-s}}$ have orders divisible by l^M.

Proof. **Step 1.** This part of the proof is analogous to the proof of Lemma 5 of [KP]. Let Λ_I (resp., Λ_J) be the $\mathcal{O}$-submodule of Λ generated by $P_{i_1}, \ldots, P_{i_r}$ (resp., by $P_{j_1}, \ldots, P_{j_{r-s}}$). Let $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_I)$ (resp., $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_J)$) be the composite of the fields $F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I)$ (resp., $F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_J)$), for $k > 0$. We will use the notation similar to [KP]:

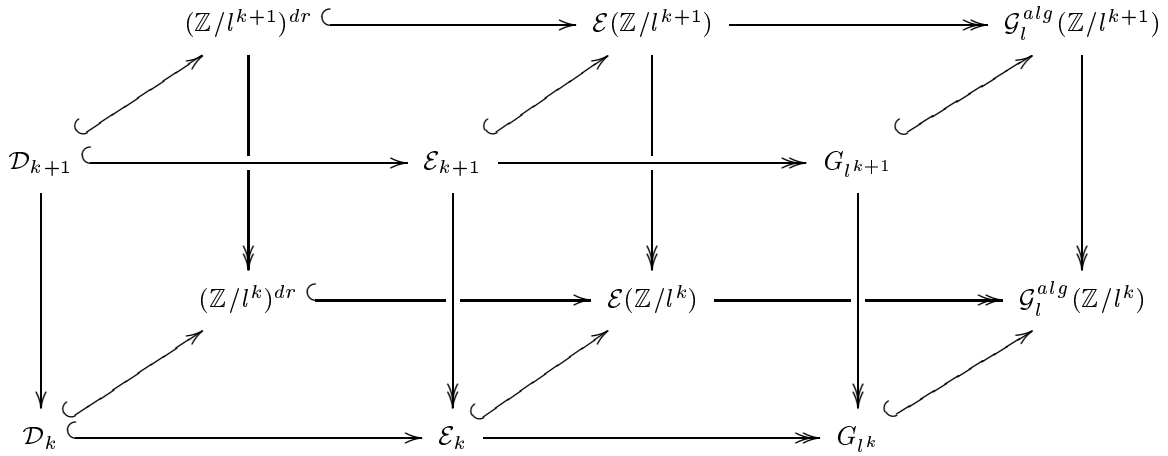
$$\begin{aligned}
\mathcal{D}_k &= G(F_{l^k}(\tfrac{1}{l^k}\hat{\Lambda}_I)/F_{l^k}) \\
\mathcal{E}_k &= G(F_{l^k}(\tfrac{1}{l^k}\hat{\Lambda}_I)/F) \\
\mathcal{D}_\infty &= G(F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I)/F_{l^\infty}) \\
\mathcal{E}_\infty &= G(F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I)/F).
\end{aligned}$$

Consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{D}_\infty & \longrightarrow & \mathcal{E}_\infty & \longrightarrow & G_{l^\infty} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathbb{G}_a^d)^r(\mathbb{Z}_l) & \longrightarrow & \mathcal{E}(\mathbb{Z}_l) & \longrightarrow & \mathcal{G}_l^{alg}(\mathbb{Z}_l) & \longrightarrow & 0.
\end{array} \tag{3.2}$$

The group scheme $\mathcal{E} = \mathcal{G}_l^{alg} \ltimes (\mathbb{G}_a^d)^r$ is a semi-direct product and $(\mathbb{G}_a^d)^r(\mathbb{Z}_l) \cong T_l^r := \bigoplus_{i=1}^r T_l$. The left vertical arrow in the diagram (3.2) is induced by the map Φ. The image of Φ is open by Lemma 2.13. Since by the assumption G_{l^∞} is open in $\mathcal{G}_l^{alg}(\mathbb{Z}_l)$, it follows by (3.2) that $\mathcal{E}_\infty$ is open in $\mathcal{E}(\mathbb{Z}_l)$. Because the map $\mathcal{G}_l^{alg}(\mathbb{Z}_l) \to \mathcal{G}_l^{alg}(\mathbb{Z}/l^k)$ is onto, the map $\mathcal{E}(\mathbb{Z}_l) \to \mathcal{E}(\mathbb{Z}/l^k)$ is also onto, for $k > 0$. Consider the following commutative diagram.

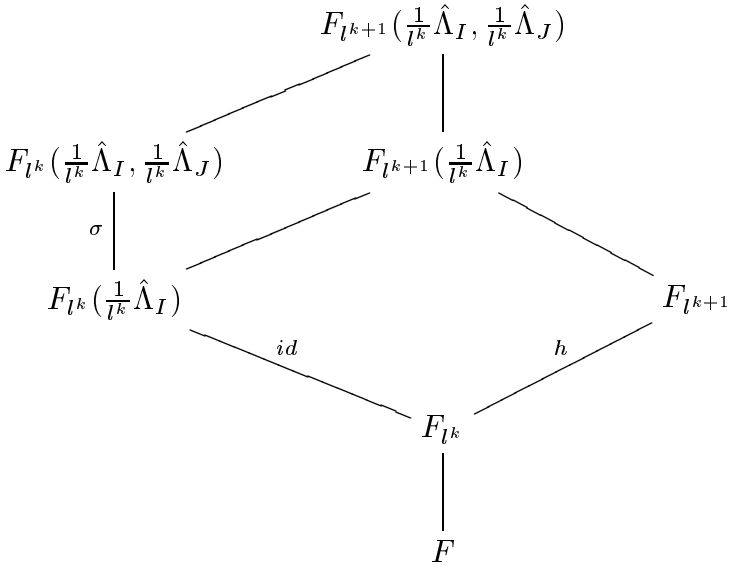
(3.3)



Using the argument on the natural congruence subgroup of $\mathcal{E}(\mathbb{Z}_l)$ of level l^k, as in the proof of Lemma 5, [KP], we note that, for k big enough, the preimage of $\mathcal{E}_k$ via the middle vertical arrow in the rear wall of diagram (3.3) is $\mathcal{E}_{k+1}$. It follows by the diagram chasing that the left vertical arrow $\mathcal{D}_{k+1} \to \mathcal{D}_k$ in the front wall of (3.3) is surjective. This immediately implies that, for k big enough:

$$F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I) \cap F_{l^{k+1}} = F_{l^k}. \tag{3.4}$$

Step 2. We will make use of the following tower of fields.
(3.5)



Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T_l^{r-s} & \longrightarrow & T_l^r & \longrightarrow & T_l^s & \longrightarrow & 0, \end{array} \tag{3.6}$$

where we have put:

$$\begin{aligned} G_1 &= G(F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I, \tfrac{1}{l^\infty}\hat{\Lambda}_J)/F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I)) \\ G_2 &= G(F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I, \tfrac{1}{l^\infty}\hat{\Lambda}_J)/F_{l^\infty}) \\ G_3 &= G(F_{l^\infty}(\tfrac{1}{l^\infty}\hat{\Lambda}_I)/F_{l^\infty}) \end{aligned}$$

and $F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_I, \frac{1}{l^\infty}\hat{\Lambda}_J) = F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_I)F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_J)$. All vertical arrows in the diagram (3.6) are the Kummer maps discussed in Section 2. The right and the middle vertical arrows have open images (equivalently, finite cokernels) by Lemma 2.13. Applying the snake Lemma to the diagram (3.6), we observe that the left vertical arrow has finite cokernel, hence it has an open image. Consider the following commutative diagram:

$$\begin{array}{ccc} G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_I, \frac{1}{l^\infty}\hat{\Lambda}_J)/F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda}_I)) & \hookrightarrow & T_l^{r-s} \\ \downarrow & & \downarrow \\ G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I)) & \hookrightarrow & \bigoplus_{i=1}^{r-s} A_l[l^k]. \end{array} \tag{3.7}$$

The horizontal arrows in the diagram (3.7) are the Kummer maps. The upper horizontal arrow is the left vertical arrow in the diagram (3.6), so it has an open image. Hence, the lower horizontal arrow in the diagram (3.7) has the cokernel bounded independently of k. Let M be a natural number. It follows that, for k big enough, there is an element $\sigma \in G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I))$, such that σ maps via the horizontal arrow in (3.7) to an element of $\bigoplus_{i=1}^{r-s} A_l[l^k]$, whose all $r-s$ projections onto the direct summands $A_l[l^k]$ have orders divisible by l^M.

Step 3. Pick k big enough such that (3.4) holds and there is the element σ, constructed in Step 2. Consider the diagram (3.5). We choose an element

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

in the following manner: $\gamma|_{F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)} = (\sigma, Id)$ in the semidirect product

$$G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}) = G((F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I)) \rtimes G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I)/F_{l^k})$$

and $\gamma|_{F_{l^{k+1}}} = h$ is such that, the action of h on the module T_l is given by a nontrivial homothety $1 + l^k u_0$, for some $u_0 \in \mathbb{Z}_l^\times$. Such a homothety h exists by the assumption on the image $\rho_l(G_F)$. By the Chebotarev density theorem there are infinitely many prime ideals v in $\mathcal{O}_F$ such that γ is equal to the Frobenius element for the prime v in the extension $F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F$. In the remainder of the proof we work with prime ideals v which we have just selected. For each such v we fix a prime w in $F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)$ above v.

Step 4. Let $i \in I$ and let l^{c_i} be the order of $r_v(P_i)$ in $B_v(\kappa_v)_l$, for some $c_i \geq 0$. Hence, $l^{k+c_i}\frac{1}{l^k}\, r_v(P_i) = 0$. So $Q_i = \frac{1}{l^k}P_i \in B(F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}_I))$ maps via the map r_{w_1} (see the diagram (2.1)) to the point $r_{w_1}(Q_i) \in B_v(\kappa_{w_1})_l$ of order l^{k+c_i}. Here w_1 is a prime of $F_{l^{k+1}}(\frac{1}{l^k}\hat{\Lambda}_I)$ below w. By the axioms (A_2), (A_3) and by the choice of v, the point $r_{w_1}(Q_i)$ comes from an element of $B_v(\kappa_v)_l$. Using the assumption that the right vertical arrow in the diagram (2.1) is an isomorphism, by the choice of v, we see that the action of h on $r_{w_1}(Q_i)$ is as follows:

$$h(r_{w_1}(Q_i)) = (1 + l^k u_0) r_{w_1}(Q_i).$$

But $r_{w_1}(Q_i) \in B_v(\kappa_v)_l$, so $h(r_{w_1}(Q_i))=r_{w_1}(Q_i)$, again by the choice of v. Hence, $l^k r_{w_1}(Q_i)=0$. This can only happen, when $c_i = 0$.

Step 5. In this part of the proof we use the argument similar to that in Proposition 2.19 of [BGK2]. Let w_2 denote the prime in $F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)$ below w and let u_2 denote the prime in F_{l^k} below w_2. Consider the following commutative diagram:

$$\begin{array}{ccc} B(F)/l^k B(F) & \longrightarrow & B_v(\kappa_v)/l^k B_v(\kappa_v) \\ \downarrow & & \downarrow \\ B(F_{l^k})/l^k B(F_{l^k}) & \longrightarrow & B_v(\kappa_{u_2})/l^k B_v(\kappa_{u_2}) \\ \downarrow & & \downarrow \\ Hom(H^{ab}_{l^k}; A_l[l^k]) & \longrightarrow & Hom(g_{u_2}; A_l[l^k]). \end{array} \tag{3.8}$$

The bottom vertical maps are discribed in the natural way (similarly to the map Ψ in the proof of Lemma 2.12). Every point P_j, where $j \in J$, maps via the left vertical arrow in the diagram (3.8) to an element $\phi^{(k)}_{P_j}$ defined by (2.3). The homomorphism $\phi^{(k)}_{P_j}$ factors through the group $G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k})$. We denote this factorization with the same symbol $\phi^{(k)}_{P_j}$. By the choice of the element γ in Step 3 (see also the comments following the diagram (3.7)) we see that the element $\phi^{(k)}_{P_j}(\gamma|_{F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)}) \in A_l[l^k]$ has the order divisible by l^M. Hence, the element $\phi^{(k)}_{P_j} \in Hom(H^{ab}_{l^k}; A_l[l^k])$ has the order divisible by l^M, and by the choice of v in Step 3, it maps via the bottom horizontal arrow in the diagram (3.8) to an element

of order divisible by l^M. So the point P_j maps to an element of order divisible by l^M via the top horizontal arrow in the diagram (3.8). $\square$

Corollary 3.9. *With the same assumptions as in the Theorem 3.1 the Galois group*

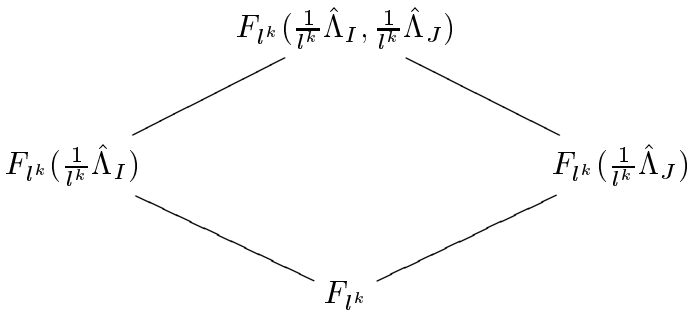
$$G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I) \cap F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_J) \,/\, F_{l^k})$$

has the order bounded independently of k.

Proof. In the same way as in Step 2 of the proof of Theorem 3.1 we show that the horizontal Kummer maps in the diagram (3.10) below have cokernels bounded independently of k (see diagram (3.7)).

$$\begin{array}{ccc} G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_J)) & \hookrightarrow & \bigoplus_{i=1}^{s} A_l[l^k] \\ \downarrow & & \downarrow \\ G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}) & \hookrightarrow & \bigoplus_{i=1}^{r} A_l[l^k] \\ \uparrow & & \uparrow \\ G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I)) & \hookrightarrow & \bigoplus_{i=1}^{r-s} A_l[l^k] \end{array} \tag{3.10}$$

The diagram (3.10) and the following diagram.



show that the subgroup

$$G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_J))\, G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I))$$

of $G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I, \frac{1}{l^k}\hat{\Lambda}_J)/F_{l^k})$ has a finite index bounded independently of k. Hence, the Galois group

$$G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_I) \cap F_{l^k}(\frac{1}{l^k}\hat{\Lambda}_J) \,/\, F_{l^k})$$

has the order bounded independently of k. $\square$

Lemma 3.11. *For any finite extension L/F and any prime $w \notin S_l$ in $\mathcal{O}_L$, the reduction map*

$$r_w \ : \ B(L)_{tor} \longrightarrow B_v(\kappa_w)$$

is an imbedding.

Proof. Since (A_1) and (A_2) are fulfilled by assumption, the lemma follows by the diagram (2.1) and [BGK2], Lemma 2.13. Note that Lemma 2.13 of [BGK2] holds also for l=2. □

Under the assumptions of Section 2, we can derive the following stronger version of Theorem 2.9 in the case when $\mathcal{O} = \mathbb{Z}$.

Theorem 3.12.
Let P and $P_1, \ldots, P_r$ be nontorsion elements of $B(F)$ such that $P_1, P_2, \ldots, P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the submodule of $B(F)$ generated by the $P_1, P_2, \ldots, P_r$. The following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

Proof. We prove that (2) implies (1). The opposite implication is obvious. By Theorem 2.9 there exists $a \in \mathbb{Z}$ such that

$$aP = \alpha_1 P_1 + \cdots + \alpha_r P_r, \tag{3.13}$$

for some $\alpha_i \in \mathcal{O}$. Let l^M be the largest power of l that divides a. Fix $1 \leq i \leq r$. By Theorem 3.1 there are infinitely many primes v such that

$$r_v(P_1) = \cdots = r_v(P_{i-1}) = r_v(P_{i+1}) = \cdots = r_v(P_r) = 0$$

in $B_v(\kappa_v)_l$ and $r_v(P_i)$ has order at least l^M in $B(k_v)_l$. Applying r_v to the equality (3.13) we get:

$$ar_v(P) = \alpha_i r_v(P_i). \tag{3.14}$$

By the assumption of the theorem and the choice of v,

$$r_v(P) = \beta_i r_v(P_i) \tag{3.15}$$

in $B_v(\kappa_v)_l$, for some $\beta_i \in \mathbb{Z}$. Multipying both sides of (3.15) by a and comparing qith (3.14) we get:

$$(\alpha_i - a\beta_i) r_v(P_i) = 0$$

in $B_v(\kappa_v)_l$, which implies that l^M divides α_i. So the equality (3.13) gives:

$$\frac{a}{l^M} P = \frac{\alpha_1}{l^M} P_1 + \cdots + \frac{\alpha_r}{l^M} P_r + R, \tag{3.16}$$

where $R \in B(F)[l^M]$. By Theorem 3.1 we pick infinitely many primes v in F such that $r_v(P_1)=\ldots=r_v(P_r)=0$ in $B_v(\kappa_v)_l$, and apply the assumption that $r_v(P) \in r_v(\Lambda)$, for almost all v. Hence, by applying r_v to the equality (3.16), we get $r_v(R)=0$, for infinitely many primes v. This contradicts Lemma 3.11, unless $R=0$. Hence, we obtain the equality:

$$\frac{a}{l^M}P = \frac{\alpha_1}{l^M}P_1 + \cdots + \frac{\alpha_r}{l^M}P_r.$$

Repeating the above argument for primes dividing $\frac{a}{l^M}$ we finish the proof by induction. $\square$

4. Corollaries of Theorem 3.12.

In the case of K-groups, we put $B(F)=K_{2n+1}(F)/C_F$, for $n\geq 0$, where C_F is the subgroup of $K_{2n+1}(F)$ generated by l-parts (for all primes l) of kernels of the Dwyer-Friedlander map. Observe that if the Quillen-Lichtenbaum conjecture holds true, then $B(F)=K_{2n+1}(F)$. We obtain the following specialization of Theorem 3.12 which strengthens the Theorem of [BGK1].

Theorem 4.1.
Let P and P_1, P_2, ..., P_r be nontorsion elements of $K_{2n+1}(F)/C_F$, such that P_1, P_2, ..., P_r are linearly independent over $\mathbb{Z}$. Let $\Lambda \subset K_{2n+1}(F)/C_F$ denote the subgroup generated by $P_1, P_2, \ldots, P_r$. The following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

Proof. Similarly to [BGK2], Example 3.4, let:

$$\rho_l \ : \ G_F \to GL(T_l) \cong \mathbb{Z}_l^{\times}$$

be the one dimensional representation given by the $(n+1)$th tensor power of the cyclotomic character. For every finite extension L/F, let C_L be the subgroup of $K_{2n+1}(L)$ generated by the l-parts (for all odd primes l) of the kernels of the Dwyer-Friedlander maps cf. [DF]:

$$K_{2n+1}(L) \longrightarrow K_{2n+1}(L) \otimes \mathbb{Z}_l \longrightarrow H^1(G_L; \mathbb{Z}_l(n+1)).$$

Let us put:

$$B(L) = K_{2n+1}(L)/C_L$$

and $c := \#C_F$. If the Quillen-Lichtenbaum conjecture holds true, then $c=1$. Because $T_l=\mathbb{Z}_l(n+1)$ is one-dimensional over $\mathbb{Z}_l$ and $B(F)$ is finitely generated, the axioms $(A_1)-(A_3)$ and $(B_1)-(B_4)$ are clearly satisfied (cf. [BGK2], Section 6). In this case, we have $\mathcal{O} = \mathbb{Z}$, $\mathcal{G}_l^{alg} = \mathbb{G}_m$ and the map $\mathcal{G}_l^{alg}(\mathbb{Z}_l) \to \mathcal{G}_l^{alg}(\mathbb{Z}/l^k)$ is the natural projection $\mathbb{Z}_l^{\times} \to (\mathbb{Z}/l^k)^{\times}$. The image of ρ_l is open in ${\mathbb{Z}_l}^{\times}$, for each l, which is clear from the definition of ρ_l. $\square$

Theorem 4.2.
Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1, \ldots, P_r$ be nontorsion elements of $A(F)$ such that $P_1, P_2, \ldots, P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1, P_2, \ldots, P_r$. Then the following two statements are equivalent:

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

Proof. Let $\rho_l : G_F \longrightarrow GL(T_l(A))$ be the l-adic representation associated to A. For a finite extension L/F let $B(L)$=$A(L)$. The axioms $(A_1)-(A_3)$ are satisfied by [BGK2], Examples 3.6, 3.7. The axioms (B_1) and (B_2) are satisfied by the results of Faltings [F], Satz 4, and Zarhin [Z], Corollary 5.4.5. The condition (B_3) holds due to the result of Serre, [Se2], Corollary of Theorem 2, and the condition (B_4) holds, because $B(F)$=$A(F)$ is finitely generated. In this case, we have $\mathcal{O}$=$\mathbb{Z}$, $\mathcal{G}_l^{alg}$=GSp_{2g} and the map $\mathcal{G}_l^{alg}(\mathbb{Z}_l) \to \mathcal{G}_l^{alg}(\mathbb{Z}/l^k)$ is the natural map $GSp_{2g}(\mathbb{Z}_l) \to GSp_{2g}(\mathbb{Z}/l^k)$, which is surjective, for every $k > 0$, by [A], Lemma 3.3.2 (1), p.135. The image of ρ_l is open in $GSp_{2g}(\mathbb{Z}_l)$, for each l, by [Se1], Théorème 3, p. 97 and it contains an open subgroup of homotheties by the theorem of Bogomolov, cf. [Bo], Corollary 1, p.702. □

Corollary 4.3. *Let E be an elliptic curve without complex multiplication, which is defined over the number field F. Let P and $P_1, \ldots, P_r$ be non-torsion elements of the Mordell-Weil group $E(F)$ and such that $P_1, \ldots, P_r$ are linearly independent over $\mathbb{Z}$. Let Λ be the subgroup generated by $P_1, \ldots, P_r$. Then the following two statements are equivalent:*

(1) $P \in \Lambda$
(2) $r_v(P) \in r_v(\Lambda)$ *for almost all primes v of F.*

Acknowledgements: The authors thank the Isaac Newton Institute in Cambridge for the financial support during the visit in September 2002. The second author thanks the Max-Planck-Institut für Mathematik in Bonn for the hospitality and the financial support during the visit in 2002/2003. The research was partially financed by a KBN grant 2 PO3A 048 22.

References

[A] A.N. Andrianov, *Quadratic forms and Hecke operators*, vol. Grundlehren der math. Wissenschaften 286, Springer-Verlag, 1987.

[B] A. Borel, *Cohomologie de SL_n et values de fonctiones zeta*, Ann. Acad. Scuola Normale Superiore **7** (1974), 613-636.

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

[BGK1] G. Banaszak, W. Gajda, P. Krasoń, *A support problem for K-theory of number fields*, C. R. Acad. Sci. Paris Sér. 1 Math. **331 no. 3** (2000), 185-190.

[BGK2] G. Banaszak, W. Gajda, P. Krasoń, *Support problem for the intermediate jacobians of l-adic representations*, to appear in Journal of Number Theory.

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift,* **I** (1990), 333-400.

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

[DF] W. Dwyer, E. Friedlander, *Algebraic and étale K-theory*, Trans. Amer. Math. Soc. **292** (1985), 247-280.

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

[G-SOT] I. Garcia-Selfa, M.A. Olalla, J.M. Tornero, *Computing the rational torsion of an elliptic curve using Tate normal form*, Journal of Number Theory **96** (2002), 76-88.

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

[K] Ch. Khare, *Compatible systems of mod p Galois representations*, preprint.

[KP] Ch. Khare, D. Prasad, *Reduction of abstract homomorphisms of lattices mod p*, preprint (2002).

[L] M. Larsen, *The support problem for abelian varieties*, preprint (2002).

[Q1] D. Quillen, *Finite generation of the groups K_i of rings of algebraic integers.*, Lecture Notes in Mathematics **341** (1973), 179-198.

[Q2] D. Quillen, *On the cohomology and K-theory of the general linear group over finite field*, Ann. of Math. **96** (1972), 552-586.

[Ri] K.A. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Mathematical Journal **46, No. 4** (1979), 745-761.

[RS] K. Rubin, A. Silverberg, *Ranks of elliptic curves*, Bull. of the AMS **39** (2002), 455-474.

[Se1] J.-P. Serre, *Résumés des cours au Collège de France*, Annuaire du Collège de France (1985-1986), 95-99.

[Se2] J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes. II*, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 731-737.

[Si] J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

[We] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, preprint (2002).

[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.

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

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

current: Max Planck Intitute für Mathematik in Bonn, Bonn, Germany
E-mail address: GAJDA@mpim-bonn.mpg.de

Department of Mathematics, Szczecin University, Szczecin, Poland
E-mail address: KRASON@uoo.univ.szczecin.pl