ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 119 (2006) 1–17
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On reduction maps and support problem in K-theory and abelian varieties

Stefan Barańczuk

Department of Mathematics, Adam Mickiewicz University, Poznań, Poland

Received 1 March 2005; revised 19 July 2005

Available online 13 December 2005

Communicated by David Goss

Abstract

In this paper we consider orders of images of nontorsion points by reduction maps for abelian varieties defined over number fields and for odd dimensional K-groups of number fields. As an application we obtain the generalization of the support problem for abelian varieties and K-groups.

1. Introduction

By Supp(m) we will denote the set of prime numbers dividing a positive number m. Pál Erdös asked the following question:

Suppose that for some integers x, y, the following condition holds

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

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

Corrales-Rodrigáñez and Schoof answered the question and proved its analogue for number fields and for elliptic curves in [C-RS].

Schinzel proved the support problem for the pair of sets of natural numbers in [S].

E-mail address: stefbar@amu.edu.pl.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2005.10.011

Banaszak, Gajda and Krasoń examined the support problem for abelian varieties for which the images of the l-adic representation is well controlled and for K-theory of number fields in [BGK1,BGK2].

The support problem for abelian varieties over number fields was considered independently by Khare and Prasad in [KP].

Larsen in [Lar] gave a solution of the support problem for all abelian varieties over number fields.

Weston gave in [We] a solution to a question of Gajda which is related to the support problem for abelian varieties. In [BGK3] Banaszak, Gajda and Krasoń considered similar question as in Weston's paper in the framework of Mordell–Weil systems. In the present work I apply this framework.

In this paper we consider the generalization of the support problem for K-theory and abelian varieties; namely, we deal with the pair of sets of points instead of pair of points. Let us state, for example, Theorem 8.2.

Theorem 8.2. *Let A be an abelian variety defined over number field F such that* $\mathrm{End}(A)$ *is an integral domain. Let $P_1, \dots, P_n, Q_1, \dots, Q_n \in A(F)$ be the points of infinite order. Assume that for almost every prime l the following condition holds*:

For every set of positive integers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

Then there exist $k_i \in \mathbb{Z} \setminus \{0\}$, $\beta_i \in \mathrm{End}(A) \setminus \{0\}$ such that $k_i P_i + \beta_i Q_i = 0$ for every $i \in \{1, \dots, n\}$.

Intuitively, the condition from the generalized support problem means that for almost every v each linear dependence satisfied by the points $r_v(P_1), \dots, r_v(P_n)$ is also satisfied by the points $r_v(Q_1), \dots, r_v(Q_n)$.

The main technical result of the paper is Theorem 5.1 which lets us control the images of linearly independent points of K-groups and abelian varieties over number fields via reduction maps. These theorems are the refinement of Theorem 3.1 of [BGK3] and are proven using similar methods. I have recently found out that Pink has proven by a different method a result similar to Theorem 5.1 in the abelian variety case, cf. [Pink, Corollary 4.3].

2. Groups of the Mordell–Weil type

The following axiomatic setup of Mordell–Weil systems was developed in [BGK3].

Notation.

$\mathbb{N}$	the set of positive integers
l	a prime number
F	a number field, $\mathcal{O}_F$ its ring of integers
$\bar{F}$	fixed algebraic closure of F
G_F	$= G(\bar{F}/F)$
v	a finite prime of $\mathcal{O}_F$, $\kappa_v = \mathcal{O}_F/v$ the residue field at v
g_v	$= G(\bar{\kappa_v}/\kappa_v)$
T_l	a free $\mathbb{Z}_l$ -module of finite rank d

V_l	$= T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$
A_l	$= V_l / T_l$
S_l	a fixed finite set of primes of $\mathcal{O}_F$ containing all primes above l
$\rho_l : G_F \to GL(T_l)$	a Galois representation unramified outside the set S_l
$\bar{\rho_{l^k}} : G_F \to GL(T_l / l^k)$	the residual representation induced by ρ_l
F_{l^k}	the number field $\bar{F}^{\operatorname{Ker} \bar{\rho_{l^k}}}$
F_{l^∞}	$= \bigcup_k F_{l^k}$
G_l	$= G(F_l / F)$
G_{l^k}	$= G(F_{l^k} / F)$
G_{l^∞}	$= G(F_{l^\infty} / F)$
$C[l^k]$	the subgroup of l^k-torsion elements of an abelian group C
C_l	$= \bigcup_k C[l^k]$, the l-torsion subgroup of C.

Let L/F be a finite extension contained in $\bar{F}$ and w a finite prime in L. We write $w \notin S_l$ to indicate that w is not over any prime in S_l.

Let $\mathcal{O}$ be a ring with unity, free as $\mathbb{Z}$-module, which acts on T_l in such a way that the action commutes with the G_F action. All modules over the ring $\mathcal{O}$ considered 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. We assume that for every embedding $L \hookrightarrow L'$ of extensions of F the induced 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 suppose that the system $\{B_v(\kappa_w)\}_{\kappa_w}$ is compatible with G_F action. Namely, if $\kappa_{w'}$ is a residue field for a prime w' over w in a finite extension L'/L then a natural map $B_v(\kappa_w) \to B_v(\kappa_{w'})$ assumes G_F action in the following way: if $\sigma \in G_F$ then the map $B_v(\kappa_{\sigma(w)}) \to B_v(\kappa_{\sigma(w')})$ is the image of the map $B_v(\kappa_w) \to B_v(\kappa_{w'})$ under σ.

We make the following assumptions on the action of the G_F and $\mathcal{O}$:

(A1) 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;

(A2) 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:

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

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

(A3) either for every L the map $\psi_{l,L}$ is an isomorphism for almost all l or $B(\bar{F})$ is a discrete G_F-module divisible by l for almost l;

(A4) for every L we have: $B(\bar{F})^{G_L} \cong B(L)$ and there is a Galois equivariant and $\mathcal{O}$-equivariant map $j_{L,l}$ such that the following diagram commutes:

$$\begin{array}{ccc} & & B(L) \\ & \overset{j_{L,l}}{\nearrow} & \downarrow \\ & & B(L) \otimes \mathbb{Z}_l \\ & & \big\downarrow \\ H^0(G_L, A_l) & \hookrightarrow & H^1_{f,S_l}(G_L, T_l) \end{array}$$

and by abuse of notation we will consider $H^0(G_L, A_l)$ as a subgroup of $B(L)$.

As in [Ri] we impose the following four axioms on the representations which we consider:

(B1) $\mathrm{End}_{G_l}(A_l[l]) \cong \mathcal{O}/l\mathcal{O}$, for almost all l and $\mathrm{End}_{G_{l^\infty}}(T_l) \cong \mathcal{O} \otimes \mathbb{Z}_l$, for all l;
(B2) $A_l[l]$ 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;
(B3) $H^1(G_l, A_l[l]) = 0$ for almost all l and $H^1(G_{l^\infty}, T_l)$ is a finite group for all l;
(B4) for each finitely generated subgroup $\Gamma \subset B(F)$ the group

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

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

For a point $R \in B(L)$ (respectively a subgroup $\Gamma \subset B(F)$) we denote $\hat{R} = \psi_{l,L}(R)$ (respectively $\hat{\Gamma} = \psi_{l,L}(\Gamma)$).

Definition 2.1. The system of modules $\{B(L)\}_L$ fulfilling the above axioms is called a *Mordell–Weil system.*

3. Examples of Mordell–Weil systems

In all cases below the axioms (A_1)–(A_4) and (B_1)–(B_4) are satisfied by [BGK3], proofs of Theorems 4.1 and 4.2 loc. cit. In particular, in the case of abelian varieties, the assumptions are fulfilled due to results of Faltings [Fa], Zarhin [Za], Serre [Serre], and Mordell and Weil.

The cyclotomic character. Let $T_l = \mathbb{Z}_l(1)$, $V_l = \mathbb{Q}_l(1)$, $A_l = \mathbb{Q}_l/\mathbb{Z}_l(1)$. Let S be an arbitrary finite set of primes in $\mathcal{O}_F$. We put

$$B(L) = \mathcal{O}_{L,S}^{\times}$$

for any finite extension L/F and we have $\mathcal{O} = \mathbb{Z}$.

Algebraic K-theory of number fields. Let n be a natural number. For every finite extension L/F consider the Dwyer–Friedlander maps [DF]:

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

where the action of G_L on $\mathbb{Z}_l(n+1)$ is given by the $(n+1)$th tensor power of the cyclotomic character.

Let C_L be the subgroup of $K_{2n+1}(L)$ generated by the l-parts of kernels of the maps $K_{2n+1}(L) \to H^1(G_L; \mathbb{Z}_l(n+1))$ for all primes l. By [DF] C_L is finite and according to Quillen–Lichtenbaum conjecture should be trivial. We put

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

and we have $\mathcal{O} = \mathbb{Z}$. The map $\psi_{L,l}$ is induced by the Dwyer–Friedlander map.

Abelian varieties over number fields. Let A be an abelian variety over number field F and let

$$\rho_l : G_F \to GL\big(T_l(A)\big)$$

be the l-adic representation given by the action of absolute Galois group on the Tate module $T_l(A)$ of A. In this case we put $B(L) = A(L)$ for every finite field extension L/F and $\mathcal{O} = \mathrm{End}(A)$.

4. Kummer theory for l-adic representations

We introduce the Kummer theory for l-adic representations, following [Ri,BGK3]. Let Λ be a finitely generated free $\mathcal{O}$-submodule of $B(F)$ with basis $P_1, \ldots, P_r$.

For natural numbers k we have the Kummer maps:

$$\phi^k_{P_i} : G(\bar{F}/F_{l^k}) \to A_l\big[l^k\big],$$
$$\phi^k_{P_i}(\sigma) = \sigma\left(\frac{1}{l^k}\hat{P}_i\right) - \frac{1}{l^k}\hat{P}_i.$$

These maps are well defined by the definition of maps $j_{L,l}$ in axiom (A4).

We define

$$\Phi^k : G(\bar{F}/F_{l^k}) \to \bigoplus_{i=1}^{r} A_l\big[l^k\big], \quad \Phi^k = \big(\phi^k_{P_1}, \ldots, \phi^k_{P_r}\big).$$

We define the field:

$$F_{l^k}\left(\frac{1}{l^k}\hat{\Lambda}\right) := \bar{F}^{\,\mathrm{Ker}\,\Phi^k}.$$

Taking the inverse limit in the following commutative diagram

$$\begin{array}{ccc} G(\bar{F}/F_{l^k}) & \xrightarrow{\phi_{P_i}^k} & A_l[l^k], \\ \downarrow & & \downarrow \times l \\ G(\bar{F}/F_{l^{k-1}}) & \xrightarrow{\phi_{P_i}^{k-1}} & A_l[l^{k-1}] \end{array}$$

we obtain a map:

$$\phi_{P_i}^{\infty}: G(\bar{F}/F_{l^\infty}) \to T_l.$$

We define:

$$\Phi^{\infty}: G(\bar{F}/F_{l^\infty}) \to \bigoplus_{i=1}^{r} T_l, \quad \Phi = (\phi_{P_1}^{\infty}, \dots, \phi_{P_r}^{\infty}).$$

Lemma 4.1. *For k big enough*

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

Proof. The proof follows the lines of step 1 of the proof of Proposition 2.2 in [BGK4] that partly repeats the argument in the proof of Lemma 5 in [KP].

Consider the following commutative diagram:

$$\begin{array}{ccc} G\big(F_{l^\infty}\big(\frac{1}{l^\infty}\hat{\Lambda}\big)/F_{l^\infty}\big) & \longrightarrow & T_l^r/l^m T_l^r \\ \downarrow & & \downarrow \cong \\ G\big(F_{l^{k+1}}\big(\frac{1}{l^{k+1}}\hat{\Lambda}\big)/F_{l^{k+1}}\big) & \longrightarrow & \big(A_l[l^{k+1}]\big)^r/l^m\big(A_l[l^{k+1}]\big)^r \\ \downarrow & & \downarrow \cong \\ G\big(F_{l^k}\big(\frac{1}{l^k}\hat{\Lambda}\big)/F_{l^k}\big) & \longrightarrow & \big(A_l[l^k]\big)^r/l^m\big(A_l[l^k]\big)^r \end{array}$$

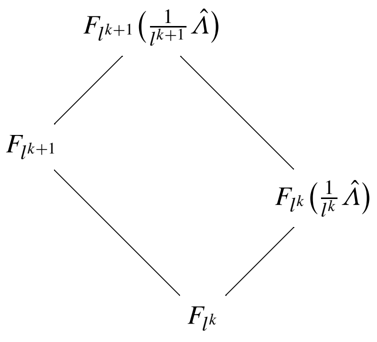
where the horizontal arrows are the Kummer maps and $m \in \mathbb{N}$ is big enough so that $l^m T_l^r \subset \operatorname{Im}(G(F_{l^\infty}(\frac{1}{l^\infty}\hat{\Lambda})/F_{l^\infty}) \to T_l^r)$. Such m exists by [BGK3] Lemma 2.13.

Now we see that for k big enough the images of the maps

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

must be all isomorphic. Hence the maps $G(F_{l^{k+1}}(\frac{1}{l^{k+1}}\hat{\Lambda})/F_{l^{k+1}}) \to G(F_{l^k}(\frac{1}{l^k}\hat{\Lambda})/F_{l^k})$ are surjective.

Now the diagram



shows that

$$F_{l^k}\left(\frac{1}{l^k}\hat{\Lambda}\right) \cap F_{l^{k+1}} = F_{l^k}. \qquad \square$$

5. Main technical result

Theorem 5.1. *Assume that $\rho(G_F)$ contains an open subgroup of the group of homotheties. Let*

$$P_1, \ldots, P_s \in B(F)$$

be points of infinite order, which are linearly independent over $\mathcal{O}$.

Then for any prime l, and for any set $\{k_1, \ldots, k_s\} \subset \mathbb{N} \cup \{0\}$, there are infinitely many primes v, such that the image of the point P_t via the map

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

has order equal to l^{k_t} for every $t \in \{1, \ldots, s\}$.

Proof. Let us rename the points $P_1, \ldots, P_s \in B(F)$ in the following way:

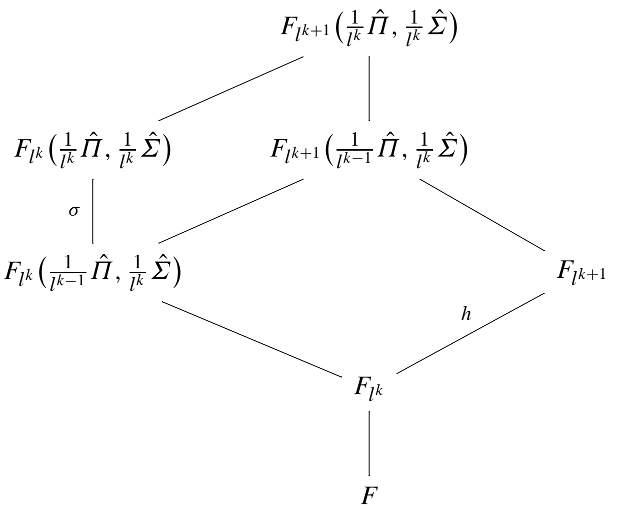
$$P_1, \ldots, P_i, Q_1, \ldots, Q_j \in B(F),$$

and we are going to show that for any prime l, and for any set $\{k_1, \ldots, k_i\} \subset \mathbb{N}$, there are infinitely many primes v, such that the image of the point P_t via the map

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

has order equal to l^{k_t} for every $t \in \{1, \ldots, i\}$ and the images of the points $Q_1, \ldots, Q_j$ are trivial. It is enough to prove the theorem in a case when $k_t = 1$ for every $t \in \{1, \ldots, i\}$, since if $r_v(l^{k_t-1}P_t)$ has order equal to l then $r_v(P_t)$ has order equal to l^{k_t}.

We will make use of the following diagram:



where Π (respectively Σ) is the $\mathcal{O}$-submodule of $B(F)$ generated by $P_1, \dots, P_i$ (respectively by $Q_1, \dots, Q_j$).

It follows by Lemma 4.1 applied to the $\mathcal{O}$-submodule of $B(F)$ generated by $lP_1, \dots, lP_i, Q_1, \dots, Q_j$ that for k big enough

$$F_{l^k}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right) \cap F_{l^{k+1}} = F_{l^k}.$$

Step 1. Consider the following commutative diagram:

$$\begin{array}{ccc}
G\left(F_{l^\infty}\left(\frac{1}{l^\infty}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right)/F_{l^\infty}\left(\frac{1}{l^\infty}\hat{\Sigma}\right)\right) & \longrightarrow & T_l^i \\
\downarrow & & \downarrow \\
G\left(F_{l^\infty}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right)/F_{l^\infty}\left(\frac{1}{l^\infty}\hat{\Sigma}\right)\right) & \hookrightarrow & \left(A_l\left[l^k\right]\right)^i \\
\downarrow & & \downarrow l \\
G\left(F_{l^\infty}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right)/F_{l^\infty}\left(\frac{1}{l^\infty}\hat{\Sigma}\right)\right) & \hookrightarrow & \left(A_l\left[l^{k-1}\right]\right)^i
\end{array} \tag{2}$$

The horizontal arrows in the diagram (2) are the Kummer maps. The upper horizontal arrow has finite cokernel by [BGK3, Lemma 2.13], so for k big enough the horizontal arrows have cokernels bounded independently of k. Hence for k big enough there exists $\sigma \in G(F_{l^\infty}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma})/F_{l^\infty}(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}))$ such that σ maps via the Kummer map

$$G\left(F_{l^\infty}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right)\Big/ F_{l^\infty}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right)\right) \to \left(A_l[l]\right)^i \tag{3}$$

to an element whose all i projections on the direct summands $(A_l[l])^i$ are nontrivial. Then the following tower of fields

$$\begin{array}{ccc} & F_{l^\infty}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right) & \\ \diagup & & \diagdown \\ F_{l^\infty}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^\infty}\hat{\Sigma}\right) & & F_{l^k}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right) \\ \diagdown & & \diagup \\ & F_{l^k}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right) & \end{array} \tag{4}$$

shows that there exist $\sigma \in G(F_{l^k}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})/F_{l^k}(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}))$ such that σ maps via the Kummer map

$$G\left(F_{l^k}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right) \Big/ F_{l^k}\left(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right)\right) \to \left(A_l[l]\right)^i \tag{5}$$

to an element whose all i projections on the direct summands $(A_l[l])^i$ are nontrivial.

Step 2. Let k be big enough that there is an element σ constructed in a previous step and such that there exists a nontrivial homothety $h \in G(F_{l^{k+1}}/F_{l^k})$ acting on the module T_l as a multiplication by $1 + l^k u_0$, for some $u_0 \in \mathbb{Z}_l^\times$.

We choose an automorphism

$$\gamma \in G\left(F_{l^{k+1}}\left(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}\right)/F\right)$$

such that

$$\gamma|_{F_{l^k}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})} = \sigma,$$
$$\gamma\,|_{F_{l^{k+1}}} = h.$$

By the Tchebotarev Density Theorem there exist 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 $F_{l^{k+1}}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})/F$. In the remainder of the proof we work with prime ideals v we have just selected.

Step 3. Using the same argument as in [BGK3], step 4, we show that $lr_v(P_1), \ldots, lr_v(P_i)$, $r_v(Q_1), \ldots, r_v(Q_j)$ are trivial in $B_v(\kappa_v)_l$:

Let P denote any of the points $lP_1, \ldots, lP_i, Q_1, \ldots, Q_j$. Let l^c be an order of the point $r_v(P)$ in the group $B_v(\kappa_v)_l$ (see the axiom (A2)). Let w_1 be a prime ideal of $F_{l^{k+1}}(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})$ below w. A point $\frac{1}{l^k}P \in B(F_{l^{k+1}}(\frac{1}{l^{k-1}}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma}))$ and its image $r_{w_1}(\frac{1}{l^k}P) \in B_v(\kappa_{w_1})_l$ has order equal l^{k+c}. By the choice v the point $r_{w_1}(\frac{1}{l^k}P)$ comes from an element of $B_v(\kappa_v)_l$. The right vertical arrow in the diagram (1) is an isomorphism, hence by the choice of v,

$$h\left(r_{w_1}\left(\frac{1}{l^k}P\right)\right) = \left(1 + l^k u_0\right) r_{w_1}\left(\frac{1}{l^k}P\right).$$

But $r_{w_1}(\frac{1}{l^k}P) \in B_v(\kappa_v)_l$, hence $h(r_{w_1}(\frac{1}{l^k}P)) = r_{w_1}(\frac{1}{l^k}P)$, again by the choice of v. Thus $l^k r_{w_1}(\frac{1}{l^k}P) = 0$ and $c = 0$.

Step 4. Using similar argument, as in [BGK3] step 5, we show that $r_v(P_1), \dots, r_v(P_i)$ have order divisible by l in $B_v(\kappa_v)_l$:

Let w_2 denote the prime ideal in $F_{l^k}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})$ below w and let u_2 denote the prime in F_{l^k} below w_2. Consider the following commutative diagram:

$$\begin{array}{ccc} B(F)/l^k B(F) & \longrightarrow & B_v(\kappa_v)/l^k B_v(\kappa_v) \\ \downarrow & & \downarrow \\ B(F_{l^k})/l^k B(F_{l^k}) & \longrightarrow & B_v(\kappa_{u_2})/l^k B_v(\kappa_{u_2}) \\ \downarrow & & \downarrow \\ \mathrm{Hom}\big(G(\bar{F}/F_{l^k})^{ab}; A_l\big[l^k\big]\big) & \longrightarrow & \mathrm{Hom}\,\big(g_{u_2}; A_l[l^k]\big). \end{array} \qquad (6)$$

Every point P_j maps via the left vertical arrow in the diagram (6) to the Kummer map $\phi^k_{P_j}$. The homomorphism $\phi^k_{P_j}$ factors through the group $G(F_{l^k}(\frac{1}{l^k}\hat{\Pi}, \frac{1}{l^k}\hat{\Sigma})/F_{l^k})$. We denote this factorization with the same symbol $\phi^k_{P_j}$. By the choice of the automorphism γ the element $\phi^k_{P_j}(\gamma|_{F_{l^k}((1/l^k)\hat{\Pi},(1/l^k)\hat{\Sigma})}) \in A_l[l^k]$ is nontrivial. Hence the element $\phi^k_{P_j} \in \mathrm{Hom}(G(\bar{F}/F_{l^k})^{ab}; A_l[l^k])$ is nontrivial. Thus by the choice of v image of the element $\phi^k_{P_j}$ via map $\mathrm{Hom}(H^{ab}_{l^k}; A_l[l^k]) \to \mathrm{Hom}(g_{u_2}; A_l[l^k])$ from diagram (6) is nontrivial. Hence the image of P_j via the bottom horizontal arrow in the diagram (6) is nontrivial.

Thus every point $r_v(P_1), \dots, r_v(P_i)$ has the order divisible by l in $B_v(\kappa_v)_l$. But step 3 shows that every point $lr_v(P_1), \dots, lr_v(P_i)$ is trivial. Hence elements $r_v(P_1), \dots, r_v(P_i)$ have orders equal l. □

6. Support problem for *K*-theory and abelian varieties

Let $\mathcal{O}$ be an integral domain.

Theorem 6.1. *Let $P_1, \dots, P_n, P_0, Q_1, \dots, Q_n, Q_0 \in B(F)$ be the points nontorsion over $\mathcal{O}$. Assume that for almost every prime l the following condition holds in the group $B_v(\kappa_v)_l$:*

For every set of nonnegative integers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = r_v(P_0) \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = r_v(Q_0).$$

Then there exist $\alpha_i, \beta_i \in \mathcal{O} \setminus \{0\}$ such that $\alpha_i P_i + \beta_i Q_i = 0$ in $B(F)$ for every $i \in \{0, \dots, n\}$.

Proof. Set $m_i = 0$ for every $i \in \{1, \dots, n\}$. We get

$$r_v(P_0) = 0 \quad \text{implies} \quad r_v(Q_0) = 0 \qquad (7)$$

for almost every prime v. Assume that P_0 and Q_0 are linearly independent in $B(F)$ over $\mathcal{O}$. By Theorem 5.1 there are infinitely many primes v such that $r_v(P_0)=0$ and $r_v(Q_0)$ has order l. This contradicts (7). Hence there exist $\alpha_0, \beta_0 \in \mathcal{O}\setminus\{0\}$ such that $\alpha_0 P_0 + \beta_0 Q_0 = 0$ in $B(F)$.

Now fix $m_1 = \cdots = m_{j-1} = m_{j+1} = \cdots = m_n = 0$. Let m_j be a natural number such that $m_j P_j + P_0$, $(m_j+1)P_j + P_0$, $(m_j+2)P_j + P_0$, $m_j Q_j + Q_0$, $(m_j+1)Q_j + Q_0$, $(m_j+2)Q_j + Q_0$ be nontorsion points.

As above we show that there exist $x_0, y_0, x_1, y_1, x_2, y_2 \in \mathcal{O}\setminus\{0\}$ such that

$$\begin{cases} x_0(m_j P_j + P_0) + y_0(m_j Q_j + Q_0) = 0, \\ x_1((m_j+1)P_j + P_0) + y_1((m_j+1)Q_j + Q_0) = 0, \\ x_2((m_j+2)P_j + P_0) + y_2((m_j+2)Q_j + Q_0) = 0. \end{cases}$$

Hence

$$\begin{cases} x_1 y_0 P_j + y_1 y_0 Q_j = (x_0 y_1 - x_1 y_0)(m_j P_j + P_0), \\ 2(x_2 y_0 P_j + y_2 y_0 Q_j) = (x_0 y_2 - x_2 y_0)(m_j P_j + P_0). \end{cases} \tag{8}$$

If $(x_0 y_1 - x_1 y_0) = 0$ or $(x_0 y_2 - x_2 y_0) = 0$ we are done. So assume that

$$(x_0 y_1 - x_1 y_0)(x_0 y_2 - x_2 y_0) \neq 0. \tag{9}$$

Hence from (8) we get

$$y_0\big(x_0(x_2 y_1 - x_1 y_2) + x_2(x_0 y_1 - x_1 y_0)\big)P_j = y_0\big(y_0(x_1 y_2 - x_2 y_1) + y_2(x_1 y_0 - x_0 y_1)\big)Q_j.$$

If $y_0(x_0(x_2 y_1 - x_1 y_2) + x_2(x_0 y_1 - x_1 y_0)) \neq 0$ or $y_0(y_0(x_1 y_2 - x_2 y_1) + y_2(x_1 y_0 - x_0 y_1)) \neq 0$ we are done. So assume that

$$\begin{cases} y_0(x_0(x_2 y_1 - x_1 y_2) + x_2(x_0 y_1 - x_1 y_0)) = 0, \\ y_0(y_0(x_1 y_2 - x_2 y_1) + y_2(x_1 y_0 - x_0 y_1)) = 0. \end{cases}$$

Then

$$\begin{cases} x_0(x_2 y_1 - x_1 y_2) + x_2(x_0 y_1 - x_1 y_0) = 0, \\ y_0(x_1 y_2 - x_2 y_1) + y_2(x_1 y_0 - x_0 y_1) = 0. \end{cases}$$

Hence we get

$$(x_0 y_1 - x_1 y_0)(x_0 y_2 - x_2 y_0) = 0$$

that contradicts (9). □

Theorem 6.2. *Let $P_1, \ldots, P_n, Q_1, \ldots, Q_n \in B(F)$ be the points nontorsion over $\mathcal{O}$. Assume that for almost every prime l the following condition holds in the group $B_v(\kappa_v)_l$:*

For every set of natural numbers $m_1, \ldots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

Then there exist $\alpha_i, \beta_i \in \mathcal{O}\setminus\{0\}$ such that $\alpha_i P_i + \beta_i Q_i = 0$ in $B(F)$ for every $i \in \{1, \ldots, n\}$.

Proof. The proof of the theorem is analogous to the proof of Theorem 6.1:

Let m_j be a natural number such that

$$m_1P_1+\cdots+m_{j-1}P_{j-1}+m_jP_j+m_{j+1}P_{j+1}+\cdots+m_nP_n,$$
$$m_1P_1+\cdots+m_{j-1}P_{j-1}+(m_j+1)P_j+m_{j+1}P_{j+1}+\cdots+m_nP_n,$$
$$m_1P_1+\cdots+m_{j-1}P_{j-1}+(m_j+2)P_j+m_{j+1}P_{j+1}+\cdots+m_nP_n,$$
$$m_1Q_1+\cdots+m_{j-1}Q_{j-1}+m_jQ_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n,$$
$$m_1Q_1+\cdots+m_{j-1}Q_{j-1}+(m_j+1)Q_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n,$$
$$m_1Q_1+\cdots+m_{j-1}Q_{j-1}+(m_j+2)Q_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n$$

be nontorsion points. There exist $x_0, y_0, x_1, y_1, x_2, y_2 \in \mathcal{O}\setminus\{0\}$ such that

$$\begin{cases} x_0(m_1P_1+\cdots+m_{j-1}P_{j-1}+m_jP_j+m_{j+1}P_{j+1}+\cdots+m_nP_n) \\ \quad + y_0(m_1Q_1+\cdots+m_{j-1}Q_{j-1}+m_jQ_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n)=0, \\ x_1(m_1P_1+\cdots+m_{j-1}P_{j-1}+(m_j+1)P_j+m_{j+1}P_{j+1}+\cdots+m_nP_n) \\ \quad + y_1(m_1Q_1+\cdots+m_{j-1}Q_{j-1}+(m_j+1)Q_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n)=0, \\ x_2(m_1P_1+\cdots+m_{j-1}P_{j-1}+(m_j+2)P_j+m_{j+1}P_{j+1}+\cdots+m_nP_n) \\ \quad + y_2(m_1Q_1+\cdots+m_{j-1}Q_{j-1}+(m_j+2)Q_j+m_{j+1}Q_{j+1}+\cdots+m_nQ_n)=0. \end{cases}$$

The rest of the proof follows the lines of the proof of Theorem 6.1. □

Remark 6.2.1. Assume that $\mathcal{O}=\mathcal{O}_E$ for some number field E. Assume that there exist $\alpha, \beta \in \mathcal{O}_E\setminus\{0\}$ such that $\alpha P+\beta Q=0$ in $B(F)$. Then there exist $z\in\mathbb{Z}\setminus\{0\}$ such that $z\frac{\beta}{\alpha}\in\mathcal{O}_E$ (see [Mol, p. 46]). Hence $zP+z\frac{\beta}{\alpha}Q=0$ in $B(F)$. We can then replace the expression "$\alpha_i, \beta_i \in \mathcal{O}\setminus\{0\}$" in Theorem 6.1 by "$\alpha_i\in\mathbb{Z}\setminus\{0\}$, $\beta_i\in\mathcal{O}\setminus\{0\}$."

7. The case $\mathcal{O}=\mathbb{Z}$

We consider the special case $\mathcal{O}=\mathbb{Z}$. The following lemma was proved in the abelian varieties case using different method by Larsen in [Lar]:

Lemma 7.1. *Let $P, Q\in B(F)$ be points of infinite order. Assume that for every prime number l the following condition holds in the group $B_v(\kappa_v)_l$:*

For every natural number n and for almost every prime v:

$$nr_v(P)=0 \quad \textit{implies} \quad nr_v(Q)=0. \tag{10}$$

Then there is an integer e such that $Q=eP$.

Proof. By Theorem 6.2 there are $\alpha, \beta\in\mathbb{Z}\setminus 0$ such that $\alpha P=\beta Q$. Let l^k be the largest power of prime number l that divides β, $\beta=bl^k$. By (10) we have

$$\alpha r_v(P)=0 \quad \text{implies} \quad \alpha r_v(Q)=0,$$

hence

$$\beta r_v(Q) = 0 \quad \text{implies} \quad \alpha r_v(Q) = 0$$

and

$$bl^k r_v(Q) = 0 \quad \text{implies} \quad \alpha r_v(Q) = 0.$$

But obviously $\alpha r_v(Q) = 0$ implies $b\alpha r_v(Q) = 0$. Hence we get

$$l^k r_v(bQ) = 0 \quad \text{implies} \quad \alpha r_v(bQ) = 0. \tag{11}$$

By Theorem 5.1 there are infinitely many primes v such that the order of $r_v(bQ)$ is l^k. So by (11) we get $\alpha r_v(bQ) = 0$ and l^k divides α.

Now repeating an argument from the proof of the Theorem 3.12 of [BGK3] we show that $Q = \frac{\alpha}{\beta} P$ with $\frac{\alpha}{\beta} \in \mathbb{Z}$:

We have $\frac{\alpha}{l^k} P = \frac{\beta}{l^k} Q + R$ where $R \in B(F)[l^k]$. By Theorem 5.1 and by Assumption 10 there are infinitely many primes v such that $r_v(P) = r_v(Q) = 0$. Hence we get $r_v(R) = 0$ for infinitely many primes v. But the map

$$r_v : B(F)_{\text{tor}} \to B_v(\kappa_v)$$

is an embedding for any prime $v \notin S_l$ by Lemma 3.11 of [BGK3]. Thus $R = 0$. □

Lemma 7.2. *Let $P_1, P_2, Q_1, Q_2 \in B(F)$ be points of infinite order. Assume that for every prime number l the following condition holds in the group $B_v(\kappa_v)_l$:*

For every set of natural numbers m_1, m_2 and for almost every prime v:

$$m_1 r_v(P_1) + m_2 r_v(P_2) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + m_2 r_v(Q_2) = 0. \tag{12}$$

Then there is an integer e such that $Q_1 = eP_1$ and $Q_2 = eP_2$.

Proof. By Theorem 6.2 there are integers $\alpha_1, \alpha_2, \beta_1, \beta_2$ such that $\alpha_1 P_1 = \beta_1 Q_1$, $\alpha_2 P_2 = \beta_2 Q_2$. We can assume that $\alpha_1, \alpha_2 > 0$.

Now we have to consider two cases.

First, assume that P_1 and P_2 are linearly independent over $\mathbb{Z}$. Hence P_1 and $|b|Q_2$ are also linearly independent, where $\beta_2 = bl^k$ and l^k is the largest power of prime number l that divides β_2.

By Theorem 5.1 there are infinitely many primes v such that $r_v(P_1) = 0$ and $r_v(|b|\,Q_2)$ has order l^k.

By (12), for $m_1 = |\beta_1|$ and $m_2 = \alpha_2$, and by the choice of v we have:

$$|\beta_2| r_v(Q_2) = 0 \quad \text{implies} \quad \alpha_2 r_v(Q_2) = 0,$$
$$l^k r_v\big(|b|Q_2\big) = 0 \quad \text{implies} \quad \alpha_2 r_v\big(|b|Q_2\big) = 0.$$

Again by the choice of v

$$\alpha_2 r_v\big(|b|Q_2\big) = 0.$$

Hence l^k divides α_2. Now we repeat again the argument from the proof of Theorem 3.12 of [BGK3] showing that $Q_2 = e_2 P_2$ for some nonzero integer e_2 and analogously $Q_1 = e_1 P_1$ for some nonzero integer e_1.

Now by (12)

$$r_v(P_1) + r_v(P_2) = 0 \quad \text{implies} \quad r_v(Q_1) + r_v(Q_2) = 0.$$

Hence

$$r_v(P_1) + r_v(P_2) = 0 \quad \text{implies} \quad (e_1 - e_2) r_v(P_2) = 0. \tag{13}$$

Let now k be arbitrary natural number and l be arbitrary prime number. By Theorem 5.1 there are infinitely many primes v such that $r_v(P_1 + P_2) = 0$ and $r_v(P_2)$ has order l^k. Hence by (13), l^k divides $e_1 - e_2$. So $e_1 - e_2 = 0$.

Now we assume that P_1 and P_2 are linearly dependent over $\mathbb{Z}$, i.e. there are numbers $x \in \mathbb{N}$ and $y \in \mathbb{Z} \setminus \{0\}$ such that $xP_1 = yP_2$. Hence $\alpha_2\beta_1 x Q_1 = \alpha_1\beta_2 y Q_2$. Put $m_2 = m_1\alpha_1\beta_2 y \operatorname{sgn}(\beta_2 y)$ in (12):

$$\begin{aligned} &m_1 r_v(P_1) + m_1\alpha_1\beta_2 y \operatorname{sgn}(\beta_2 y) r_v(P_2) = 0 \quad \text{implies} \\ &m_1 r_v(Q_1) + m_1\alpha_1\beta_2 y \operatorname{sgn}(\beta_2 y) r_v(Q_2) = 0, \end{aligned}$$

hence

$$m_1\big[1 + \alpha_1\beta_2 x \operatorname{sgn}(\beta_2 y)\big] r_v(P_1) = 0 \quad \text{implies} \quad m_1\big[1 + \alpha_2\beta_1 x \operatorname{sgn}(\beta_2 y)\big] r_v(Q_1) = 0.$$

Putting $P := [1 + \alpha_1\beta_2 x \operatorname{sgn}(\beta_2 y)]P_1$, $Q := [1 + \alpha_2\beta_1 x \operatorname{sgn}(\beta_2 y)]Q_1$ we get

$$m_1 r_v(P) = 0 \quad \text{implies} \quad m_1 r_v(Q) = 0.$$

By Lemma 7.1 there is an integer s such that $Q = sP$. So

$$\big[1 + \alpha_2\beta_1 x \operatorname{sgn}(\beta_2 y)\big] Q_1 = s\big[1 + \alpha_1\beta_2 x \operatorname{sgn}(\beta_2 y)\big] P_1.$$

Hence

$$Q_1 = \big[s\big(1 + \alpha_1\beta_2 x \operatorname{sgn}(\beta_2 y)\big) - \alpha_1\alpha_2 x \operatorname{sgn}(\beta_2 y)\big] P_1,$$

i.e. there is an integer e_1 such that $Q_1 = e_1 P_1$. Analogously there is an integer e_2 such that $Q_2 = e_2 P_2$.

Now, by (12), for $m_1 = x$, $m_2 = l^k - y$ where k is an arbitrary natural number and l is an arbitrary prime number such that $l^k - y > 0$, we get

$$l^k r_v(P_2) = 0 \quad \text{implies} \quad y(e_1 - e_2) r_v(P_2) = 0.$$

By Theorem 5.1 there are infinitely many primes v such that $r_v(P_2)$ has order l^k, so l^k divides $y(e_1 - e_2)$. But k was arbitrary, so $e_1 - e_2 = 0$. □

Theorem 7.3. *Let $P_1, \dots, P_n, Q_1, \dots, Q_n \in B(F)$ be the points of infinite order. Assume that for every prime number l the following condition holds in the group $B_v(\kappa_v)_l$:*

For every set of natural numbers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \dots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \dots + m_n r_v(Q_n) = 0.$$

Then there exists an integer e such that $Q_i = eP_i$ in $B(F)$ for every $i \in \{1, \dots, n\}$.

Proof. There is $s \in \mathbb{N}$ such that $P := sP_2 + P_3 + \dots + P_n$, $\bar{P} := (s+1)P_2 + P_3 + \dots + P_n$, $Q := sP_2 + P_3 + \dots + P_n$, $\bar{Q} := (s+1)Q_2 + Q_3 + \dots + Q_n$ are nontorsion points.

By the assumption of the theorem the following condition holds for every set of natural numbers m_1, m_2 and for almost every prime v:

$$m_1 r_v(P_1) + m_2 r_v(P) = 0 \quad \text{implies} \quad m_1 r_v(Q_1) + m_2 r_v(Q) = 0,$$
$$m_1 r_v(P_1) + m_2 r_v(\bar{P}) = 0 \quad \text{implies} \quad m_1 r_v(Q_1) + m_2 r_v(\bar{Q}) = 0.$$

By Lemma 7.2 there is an integer e such that $Q_1 = eP_1$, $Q = eP$, $\bar{Q} = e\bar{P}$, i.e.

$$\begin{cases} e[sP_2 + P_3 + \dots + P_n] = sQ_2 + Q_3 + \dots + Q_n, \\ e[(s+1)P_2 + P_3 + \dots + P_n] = (s+1)Q_2 + Q_3 + \dots + Q_n, \end{cases}$$

hence $Q_2 = eP_2$. Analogously $Q_i = eP_i$ for every $i \in \{3, \dots, n\}$. □

8. Corollaries of Theorems 6.1 and 6.2

We obtain the specializations of Theorems 6.1 and 6.2 for cyclotomic character, K-theory and abelian varieties (see Section 3). Let us state these results in abelian variety case.

Theorem 8.1. *Let A be an abelian variety defined over number field F such that* $\mathrm{End}(A)$ *is an integral domain. Let $P_1, \dots, P_n, P_0, Q_1, \dots, Q_n, Q_0 \in A(F)$ be the points of infinite order. Assume that for almost every prime l the following condition holds*:

For every set of nonnegative integers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \dots + m_n r_v(P_n) = r_v(P_0) \quad \textit{implies} \quad m_1 r_v(Q_1) + \dots + m_n r_v(Q_n) = r_v(Q_0).$$

Then there exist $k_i \in \mathbb{Z} \setminus \{0\}$, $\beta_i \in \mathrm{End}(A) \setminus \{0\}$ such that $k_i P_i + \beta_i Q_i = 0$ for every $i \in \{0, \dots, n\}$.

Proof. By Theorem 6.1 there exist $\alpha_i, \beta_i \in \mathrm{End}(A) \setminus \{0\}$ such that $\alpha_i P_i + \beta_i Q_i = 0$ for every $i \in \{0, \dots, n\}$. But $\mathrm{End}(A)$ is an integral domain, hence A is simple and $\mathrm{End}(A) \otimes \mathbb{Q}$ is division algebra. So there exists an endomorphism $\gamma_i \in \mathrm{End}(A)$ such that $\gamma_i \alpha_i = [k_i]$ for some $k_i \in \mathbb{Z} \setminus \{0\}$. Hence $k_i P_i + \gamma_i \beta_i Q_i = 0$. □

Theorem 8.2. *Let A be an abelian variety defined over number field F such that* $\mathrm{End}(A)$ *is an integral domain. Let $P_1, \dots, P_n, Q_1, \dots, Q_n \in A(F)$ be the points of infinite order. Assume that for almost every prime l the following condition holds*:

For every set of positive integers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

Then there exist $k_i \in \mathbb{Z} \setminus \{0\}$, $\beta_i \in \operatorname{End}(A) \setminus \{0\}$ such that $k_i P_i + \beta_i Q_i = 0$ for every $i \in \{1, \dots, n\}$.

9. Corollaries of Theorem 7.3

Theorem 9.1. *Let $p_1, \dots, p_s, q_1, \dots, q_s \in F^*$ and suppose that for almost every prime ideal $\wp$ in $\mathcal{O}_F$ and for every set of natural numbers $m_1, \dots, m_s$ the following condition holds*:

$$\prod_{i=1}^{s} p_i^{m_i} = 1 \ (\text{mod } \wp) \quad \textit{implies} \quad \prod_{i=1}^{s} q_i^{m_i} = 1 \ (\text{mod } \wp).$$

Then there exists $e \in \mathbb{Z} \setminus \{0\}$ such that $q_i = p_i^e$ for every $i \in \{1, \dots, s\}$.

Remark 9.1.2. Schinzel [S, Theorem 1] proved by a different method a similar result. Theorem 9.1 is a bit more general since it assumes only positive coefficients m_i.

Theorem 9.2. *Let $P_1, \dots, P_s, Q_1, \dots, Q_s \in K_{2n+1}(F)/C_F$ be the points of infinite order, where $n \geqslant 1$. Assume that for every prime l the following condition holds*:

For every set of natural numbers $m_1, \dots, m_s$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_s r_v(P_s) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_s r_v(Q_s) = 0.$$

Then there exists $e \in \mathbb{Z} \setminus \{0\}$ such that $Q_i = eP_i$ for every $i \in \{1, \dots, s\}$.

Theorem 9.3. *Let A be an abelian variety defined over number field F such that $\operatorname{End}(A) = \mathbb{Z}$. Let $P_1, \dots, P_n, Q_1, \dots, Q_n \in A(F)$ be the points of infinite order. Assume that for every prime l the following condition holds*:

For every set of natural numbers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

Then there exists $e \in \mathbb{Z} \setminus \{0\}$ such that $Q_i = eP_i$ for every $i \in \{1, \dots, n\}$.

Corollary 9.4. *Let E be an elliptic curve without complex multiplication defined over number field F. Let $P_1, \dots, P_n, Q_1, \dots, Q_n \in A(F)$ be the points of infinite order. Assume that for every prime l the following condition holds*:

For every set of natural numbers $m_1, \dots, m_n$ and for almost every prime v

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \quad \textit{implies} \quad m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

Then there exists $e \in \mathbb{Z} \setminus \{0\}$ such that $Q_i = eP_i$ for every $i \in \{1, \dots, n\}$.

Acknowledgments

This paper forms a part of my PhD thesis. I thank my thesis adviser Grzegorz Banaszak for suggesting the problem. I thank Wojciech Gajda for discussions and especially for pointing out an argument in the proof of Lemma 5 in [KP] and an argument in the proof of Theorem 8.1. I also thank the anonymous referee for many suggestions which let me improve the paper.

The research was partially financed by AAG EU grant MRTN-CT 2003-504917.

References

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

[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 (3) (2000) 185–190.

[BGK2] G. Banaszak, W. Gajda, P. Krasoń, Support problem for the unterediate jacobians of l-adic representations, J. Number Theory 100 (2003) 133–168.

[BGK3] G. Banaszak, W. Gajda, P. Krasoń, Detecting linear dependence by reduction maps, J. Number Theory 115 (2005) 322–342.

[BGK4] G. Banaszak, W. Gajda, P. Krasoń, On reduction map for étale K-theory of curves, Homology Homotopy Appl. 7 (2005) 1–10.

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

[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 Zahlkörpern, Invent. Math. 73 (1983) 349–366.

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

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

[Mol] R.A. Mollin, Algebraic Number Theory, CRC Press, Boca Raton, FL, 1999.

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

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

[S] A. Schinzel, O pokazatelnych sravneniach, Mat. Zapiski 2 (1996) 121–126.

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

[We] T. Weston, Kummer theory of abelian varieties and reductions of Mordell–Weil groups, Acta Arith. 110 (1) (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.