

ACADEMIC
PRESSAvailable at
WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT®

Journal of Number Theory 100 (2003) 133–168

**JOURNAL OF
Number
Theory**

<http://www.elsevier.com/locate/jnt>

Support problem for the intermediate Jacobians of l -adic representations

G. Banaszak,^{a,*} W. Gajda,^{a,1} and P. Krasoń^b^aDepartment of Mathematics, Adam Mickiewicz University, Poznań, Poland^bDepartment of Mathematics, Szczecin University, Szczecin, Poland

Received 25 March 2002; revised 29 August 2002

Communicated by D. Goss

Abstract

We consider the support problem of Erdős in the context of l -adic representations of the absolute Galois group of a number field. Main applications of the results of the paper concern Galois cohomology of the Tate module of abelian varieties with real and complex multiplications, the algebraic K -theory groups of number fields and the integral homology of the general linear group of rings of integers. We answer the question of Corrales-Rodríguez and Schoof concerning the support problem for higher dimensional abelian varieties.

© 2003 Elsevier Science (USA). All rights reserved.

MSC: 11R34; 11G10; 19D99

Keywords: l -Adic representations; Intermediate Jacobians; Abelian variety; K -theory

1. Introduction

The support problem for \mathbb{G}_m was first stated by Pál Erdős who in 1988 raised the following question:

*Corresponding author.

E-mail addresses: banaszak@math.amu.edu.pl (G. Banaszak), gajda@mpim-bonn.mpg.de, gajda@math.amu.edu.pl (W. Gajda), krason@uoo.univ.szczecin.pl (P. Krasoń).

¹Current address: Max Planck Institut für Mathematik in Bonn, Germany.

Let $\text{Supp}(m)$ denote the set of prime divisors of the integer m . Let x and y be two natural numbers. Are the following two statements equivalent?

- (1) $\text{Supp}(x^n - 1) = \text{Supp}(y^n - 1)$ for every $n \in \mathbb{N}$,
- (2) $x = y$.

This question, along with its extension to all number fields, and also its analogue for elliptic curves, were solved by Corrales-Rodrigáñez and Schoof in the paper [C-RS]. Other related support problems can be found in [Ba,S]. In the present paper we investigate the support problem in the context of l -adic representations

$$\rho_l : G_F \rightarrow GL(T_l).$$

The precise description of the class of representations which are considered is rather technical. It is given by Assumptions I and II in Sections 2 and 3, respectively. This class of representations contains powers of the cyclotomic character, Tate modules of abelian varieties of nondegenerate CM type, and also Tate modules of some abelian varieties with real multiplications (cf. Examples 3.3–3.7).

Consider the reduction map

$$r_v : H_{f,S_l}^1(G_F; T_l) \rightarrow H^1(g_v; T_l),$$

for all $v \notin S_l$, which is defined on the subgroup $H_{f,S_l}^1(G_F; T_l)$ of the Galois cohomology group $H^1(G_F; T_l)$ (see Definition 2.2). S_l denotes here a finite set of primes which contains primes over l in F . Let $B(F)$ be a finitely generated abelian group such that for every l there is an injective homomorphism

$$\psi_{F,l} : B(F) \otimes \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_F; T_l).$$

Let P and Q be two nontorsion elements of $B(F)$. Put $\hat{P} = \psi_{F,l}(P \otimes 1)$ and $\hat{Q} = \psi_{F,l}(Q \otimes 1)$. Our main point of interest is the following support problem.

Support problem. Let \mathcal{P}^* be an infinite set of prime numbers. Assume that for every $l \in \mathcal{P}^*$ the following condition holds in the group $H^1(g_v; T_l)$:
for every integer m and for almost every $v \notin S_l$

$$mr_v(\hat{P}) = 0 \text{ implies } mr_v(\hat{Q}) = 0.$$

How are the elements P and Q related in the group $B(F)$?

Main results. Let \mathcal{P}^* be the infinite set of prime numbers which we define precisely in Section 4 of the paper. We prove the following theorem.

Theorem A (Theorem 5.1). *Assume that for every $l \in \mathcal{P}^*$, for every integer m and for almost every $v \notin S_l$, the following condition holds in the group $H^1(g_v; T_l)$:*

$$mr_v(\hat{P}) = 0 \text{ implies } mr_v(\hat{Q}) = 0.$$

Then there exist $a \in \mathbb{Z} - \{0\}$ and $f \in \mathcal{O}_E - \{0\}$ such that $aP + fQ = 0$ in $B(F)$. Here \mathcal{O}_E denotes the ring of integers of the number field E associated with the representation ρ_l (see Definition 3.2).

In order to prove Theorem A we investigate representations with special properties formulated in Assumptions I and II. We introduce the notion of the Mordell-Weil \mathcal{O}_E -module for such representations. Proof of Theorem A is based on a careful study of reduction maps in Galois cohomology associated with the given l -adic representation satisfying Assumptions I and II. We managed to extend the method of [C-RS] to the context of such l -adic representations. The main point in the proof is to control the relation between arithmetical properties of the images of l -adic representations and reduction maps. Key theorems on the image of the representations are proved in the separate work, cf. Theorems A and B of [BGK1]. In Section 6 of the paper we derive the following corollaries of Theorem A.

Theorem B (Corollary 6.4). *Let P, Q be two nontorsion elements of the algebraic K -theory group $K_{2n+1}(F)$, where n is an even, positive integer. Assume that for almost every prime v of \mathcal{O}_F and every integer m the following condition holds in the group $K_{2n+1}(k_v)$:*

$$mr_v(P) = 0 \text{ implies } mr_v(Q) = 0,$$

where in this case, r_v is the map induced on the Quillen K -group by the reduction at v . Then the elements P and Q of $K_{2n+1}(F)$ are linearly dependent over \mathbb{Z} .

Note that Theorem B has already been proven by a different method in [BGK].

Theorem A has the following corollary concerning the class of abelian varieties mentioned in the beginning of this Introduction.

Theorem C (Corollary 6.11). *Let A be an abelian variety of dimension $g \geq 1$, defined over the number field F and such that A satisfies one of the following conditions:*

- (1) *A has the nondegenerate CM type with $\text{End}_F(A) \otimes \mathbb{Q}$ equal to a CM field E such that $E^H \subset F$ (cf. example 3.5).*
- (2) *A is simple, principally polarised with real multiplication by a totally real field $E = \text{End}_F(A) \otimes \mathbb{Q}$ such that $E^H \subset F$ and the field F is sufficiently large. We also assume that $\dim A = he$, where $e = [E : \mathbb{Q}]$ and h is odd (cf. example 3.6) or A is simple, principally polarised such that $\text{End}_F(A) = \mathbb{Z}$ and $\dim A$ is equal to 2 or 6 (cf. example 3.7 (b)).*

Let P, Q be two nontorsion elements of the group $A(F)$. Assume that for almost every prime v of \mathcal{O}_F and for every integer m the following condition holds in $A_v(k_v)$:

$$mr_v(P) = 0 \text{ implies } mr_v(Q) = 0.$$

Then there exist $a \in \mathbb{Z} - \{0\}$ and $f \in \mathcal{O}_E - \{0\}$ such that $aP + fQ = 0$ in $A(F)$.

There are two important special cases of abelian varieties satisfying conditions of (2) of Theorem C: abelian varieties A with $\text{End}_F(A) = \mathbb{Z}$ such that $\dim A$ is an odd integer [Se1] (cf. example 3.7 (b)) and abelian varieties with real multiplication by a totally real number field $E = \text{End}_F(A) \otimes \mathbb{Q}$, such that $e = g$ [R1] (cf. example 3.7 (a)). Note that for these abelian varieties the analogues of the open image theorem of Serre have been proven [R1, Se1]. The proof of Theorem C relies on the analysis of the image of the corresponding Galois representation. The necessary information on the image of Galois representations on l -torsion points of abelian varieties from (1) and (2) of Theorem C is provided by Theorems 2.1 and 3.5 of [BGK1]. It is worth mentioning that Theorem C given above provides an answer to the question of Corrales-Rodríguez and Schoof about the support problem for higher dimensional abelian varieties [C-RS, p. 277].

Notation

l	is an odd 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
$\mathcal{O}_{F,S}$	is the ring of S -integers in F , for a finite set S of prime ideals in \mathcal{O}_F
$G_{F,S}$	is the Galois group of the maximal extension of F unramified outside S
F_v	is the completion of F at v and k_v denotes the residue field \mathcal{O}_F/v
G_v	$= G(\bar{F}_v/F_v)$
I_v	is the inertia subgroup of G_v
g_v	$= G(\bar{k}_v/k_v)$
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	$G_F \rightarrow GL(T_l)$ is a representation unramified outside a fixed finite set S_l of primes of \mathcal{O}_F , containing all primes over l
$\bar{\rho}_l$	denotes the residual representation $G_F \rightarrow GL(T_l/l)$ induced by ρ_l
F_l	$= F(A_l[l])$ denotes the number field $\bar{F}^{ker \bar{\rho}_l}$
G_l	$= G(F_l/F)$; observe that $G_l \cong \bar{\rho}_l(G_F)$ is isomorphic to a subgroup of $GL(T/l) \cong GL_d(\mathbb{Z}/l)$. 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

$[H, H]$ denotes the commutator subgroup of an abstract group H
 $H^i(G, M)$ denotes Galois cohomology group of the G -module M

2. l -adic intermediate Jacobians

Definition 2.1. Define

$$H_f^1(G_F; T_l), \quad (\text{resp. } H_f^1(G_F; V_l))$$

to be the kernel of the natural map:

$$H^1(G_F; T_l) \rightarrow \prod_v H^1(G_v; T_l)/H_f^1(G_v; T_l)$$

$$(\text{resp. } H^1(G_F; V_l) \rightarrow \prod_v H^1(G_v; V_l)/H_f^1(G_v; V_l)),$$

where $H_f^1(G_v; T_l) = i_v^{-1}H_f^1(G_v; V_l)$ via the natural map

$$i_v : H^1(G_v; T_l) \rightarrow H^1(G_v; V_l).$$

The group $H_f^1(G_v; V_l)$ is defined in [BK, p. 353] (see also [F, p. 115]) as follows:

$$H_f^1(G_v; V_l) = \begin{cases} \text{Ker}(H^1(G_v; V_l) \rightarrow H^1(I_v; V_l)) & \text{if } v \nmid l, \\ \text{Ker}(H^1(G_v; V_l) \rightarrow H^1(G_v; V_l \otimes_{\mathbb{Q}_l} B_{\text{cris}})) & \text{if } v|l, \end{cases}$$

where B_{cris} is the ring defined by Fontaine (cf. [BK, p. 339]).

We have the natural maps

$$H_f^1(G_F; T_l) \rightarrow \prod_v H_f^1(G_v; T_l),$$

$$H_f^1(G_F; V_l) \rightarrow \prod_v H_f^1(G_v; V_l).$$

Definition 2.2. We also define

$$H_{f,S_l}^1(G_F; T_l) \quad (\text{resp. } H_{f,S_l}^1(G_F; V_l))$$

as the kernel of the natural map:

$$H^1(G_F; T_l) \rightarrow \prod_{v \notin S_l} H^1(G_v; T_l)/H_f^1(G_v; T_l)$$

$$(\text{resp. } H^1(G_F; V_l) \rightarrow \prod_{v \notin S_l} H^1(G_v; V_l)/H_f^1(G_v; V_l)).$$

Here S_l denotes a fixed finite set of primes of \mathcal{O}_F containing primes over l and such that the representation ρ_l is unramified outside of S_l .

Obviously,

$$H_f^1(G_F; T_l) \subset H_{f,S_l}^1(G_F; T_l) \quad \text{and} \quad H_f^1(G_F; V_l) \subset H_{f,S_l}^1(G_F; V_l).$$

Below we define various intermediate Jacobians associated with the representation ρ_l , (cf. [Sc, Chapter 2]).

Definition 2.3. We put

$$J(T_l) = \varinjlim_{L/F} H^1(G_L; T_l), \quad J(V_l) = \varinjlim_{L/F} H^1(G_L; V_l), \tag{1}$$

$$J_f(T_l) = \varinjlim_{L/F} H_f^1(G_L; T_l), \quad J_f(V_l) = \varinjlim_{L/F} H_f^1(G_L; V_l), \tag{2}$$

$$J_{f,S_l}(T_l) = \varinjlim_{L/F} H_{f,S_l}^1(G_L; T_l), \quad J_{f,S_l}(V_l) = \varinjlim_{L/F} H_{f,S_l}^1(G_L; V_l), \tag{3}$$

where the direct limits are taken over all finite extensions L/F of the number field F , which are contained in some fixed algebraic closure \bar{F} .

Remark 2.4. Observe that the groups $J(V_l)$, $J_f(V_l)$ and $J_{f,S_l}(V_l)$ are vector spaces over \mathbb{Q}_l .

Remark 2.5. Note that we also could have defined the intermediate Jacobians of the module T_l for the cohomology groups of $G_{F,\Sigma}$ for any Σ containing S_l . However, if $H^0(g_v; A_l(-1))$ is finite for all $v \notin S_l$, (as it often happens for interesting examples of T_l), then,

$$H^1(G_{F,\Sigma}; T_l) = H^1(G_F; T_l).$$

In the sequel we will only consider l -adic representations which satisfy the following condition.

Assumption I. Assume that for each l , each finite extension L/F and any prime w of \mathcal{O}_L , such that $w \notin S_l$, we have

$$T_l^{Fr_w} = 0,$$

(or equivalently $V_l^{Fr_w} = 0$), where $Fr_w \in g_w$ denotes the arithmetic Frobenius at w .

Example 2.6. Let X be a smooth projective variety defined over a number field F with good reduction at primes $v \notin S_l$. Let \mathcal{X} be the regular, proper model of X over \mathcal{O}_{F,S_l} and let \mathcal{X}_v be its reduction at the prime v of \mathcal{O}_{F,S_l} . Put $\bar{X} = X \otimes_F \bar{F}$ and $\bar{\mathcal{X}}_v = \mathcal{X}_v \otimes_{k_v} \bar{k}_v$. In the case when $H_{\text{et}}^i(\bar{X}; \mathbb{Z}_l(j))$ is torsion free for some i, j such that $i \neq 2j$ we put

$$T_l = H_{\text{et}}^i(\bar{X}; \mathbb{Z}_l(j)).$$

By the theorem of proper and smooth base change (cf. [Mil, VI, Corollary 4.2]) there is a natural isomorphism of G_v -modules

$$H_{\text{et}}^i(\bar{X}; \mathbb{Z}_l(j)) \cong H_{\text{et}}^i(\bar{\mathcal{X}}_v; \mathbb{Z}_l(j)) \tag{2.7}$$

(cf. [Ja, p. 322]). Since the inertia subgroup $I_v \subset G_v$ acts trivially on $H_{\text{et}}^i(\bar{\mathcal{X}}_v; \mathbb{Z}_l(j))$, we observe by (2.7) that the representation $\rho_l : G_F \rightarrow GL(T_l)$ is unramified outside S_l . It follows by the theorem of Deligne [Dl] (proof of the Weil conjectures, see also [Har, Appendix C, Theorem 4.5]) that for an ideal w of \mathcal{O}_L such that $w \notin S_l$, the eigenvalues of Fr_w on the vector space

$$V_l = H_{\text{et}}^i(\bar{X}; \mathbb{Q}_l(j))$$

are algebraic integers of the absolute value $N(w)^{-i/2+j}$, where $N(w)$ denotes the absolute norm of w . It follows that $T_l^{Fr_w} = 0$. In the special case when $X = A$ is an abelian variety defined over F , we have

$$T_l = H_{\text{et}}^i(\bar{A}; \mathbb{Z}_l(j)) \cong \bigwedge^i H_{\text{et}}^1(\bar{A}; \mathbb{Z}_l)(j) \cong \bigwedge^i \text{Hom}_{\mathbb{Z}_l}(T_l(A); \mathbb{Z}_l)(j),$$

which is a free \mathbb{Z}_l module of rank $\binom{2g}{i}$ by [Mi2, Theorem 15.1]. In this paper, most of the time we will consider the representation

$$\rho_l : G_F \rightarrow GL(T_l(A))$$

of the Galois group G_F on the Tate module $T_l(A) = H_{\text{et}}^1(\bar{A}; \mathbb{Z}_l)^*$ of the abelian variety A defined over F , where for a \mathbb{Z}_l -module M , we put $M^* = \text{Hom}_{\mathbb{Z}_l}(M; \mathbb{Z}_l)$. By the above discussion we see that ρ_l satisfies Assumption I.

Lemma 2.8. *For every prime w of \mathcal{O}_L which is not over primes in S_l , we have:*

- (1) *the natural map $H^1(G_w; T_l)/H_f^1 \rightarrow H^1(G_w; V_l)/H_f^1$ is an imbedding,*
- (2) $H_f^1(G_w; T_l)_{\text{tor}} = H^1(G_w; T_l)_{\text{tor}} = H^0(G_w; A_l) = H^0(g_w; A_l)$
- (3) $H_f^1(G_w; T_l) = H^1(g_w; T_l)$.

Proof. First part of the lemma is obvious from the definition of $H_f^1(G_w; T_l)$. The second part follows immediately from the first part and diagram (2.9) below. Note

that $H^1(G_w; V_l)/H_f^1(G_w; V_l)$ is a \mathbb{Q}_l -vector space. To prove the third part consider again diagram (2.9).

$$\begin{array}{ccccc}
 H^0(g_w; A_l) & \longrightarrow & H^1(g_w; T_l) & \longrightarrow & H_f^1(G_w; V_l) \\
 \downarrow = & & \downarrow & & \downarrow \\
 H^0(G_w; A_l) & \longrightarrow & H^1(G_w; T_l) & \longrightarrow & H^1(G_w; V_l) \\
 \downarrow & & \downarrow & & \downarrow \\
 H^0(I_w; A_l) & \xrightarrow{0} & H^1(I_w; T_l) & \longrightarrow & H^1(I_w; V_l)
 \end{array} \tag{2.9}$$

The horizontal rows are exact. The middle and the right vertical columns are also exact. The left bottom horizontal arrow is zero because I_w acts on T_l , V_l and A_l trivially by assumption. This gives the exactness of the following short exact sequence.

$$0 \rightarrow H^0(I_w; T_l) \rightarrow H^0(I_w; V_l) \rightarrow H^0(I_w; A_l) \rightarrow 0$$

In addition because of Assumption I we have

$$H^0(g_w; V_l) = H^0(G_w; V_l) = 0.$$

Therefore the left upper and middle horizontal arrows are imbeddings. The right, upper horizontal arrow is defined because of the commutativity of the lower, right square in the diagram. The middle vertical column is the inflation–restriction sequence. It is actually inverse limit on coefficients of the inflation–restriction sequence but it remains exact with infinite coefficients because we deal with H^1 . Now the claim follows by diagram chasing. \square

Remark 2.10. Observe that the Assumption I implies, that $H^0(g_w; A_l)$ and $H^1(g_w; T_l)$ are finite for all $w \notin S_l$.

Lemma 2.11. *For any finite extension L/F the following equalities hold:*

$$H_{f,S_l}^1(G_L; T_l)_{\text{tor}} = H^1(G_L; T_l)_{\text{tor}} = H^0(G_L; A_l)$$

Proof. The first equality follows from Lemma 2.8 and the exact sequence.

$$0 \rightarrow H_{f,S_l}^1(G_L; T_l) \rightarrow H^1(G_L; T_l) \rightarrow \prod_{w \notin S_l} H^1(G_w; T_l)/H_f^1(G_w; T_l).$$

Consider the exact sequence (see [T, p. 261])

$$H^0(G_L; V_l) \rightarrow H^0(G_L; A_l) \xrightarrow{\partial_l} H^1(G_L; T_l).$$

By Assumption I we get $H^0(G_L; V_l) = 0$. Hence by [T, Proposition 2.3, p. 261]

$$H^0(G_L; A_l) = H^1(G_L; T_l)_{\text{tor}}.$$

Thus, the second equality in the statement of Lemma 2.11 also holds. \square

For $w \notin S_l$ consider the following commutative diagram:

$$\begin{array}{ccc} H^1_{f,S_l}(G_L; T_l) & \longrightarrow & H^1(g_w; T_l) \\ \uparrow & & \uparrow \\ H^0(G_L; A_l) & \longrightarrow & H^0(g_w; A_l). \end{array} \tag{2.12}$$

The bottom horizontal arrow is obviously an injection. Hence, by Lemmas 2.8 and 2.11, we obtain the following:

Lemma 2.13. *For any finite extension L/F and any prime $w \notin S_l$ in \mathcal{O}_L the natural map*

$$r_w : H^1_{f,S_l}(G_L; T_l)_{\text{tor}} \rightarrow H^1(g_w; T_l)$$

is an imbedding.

Proposition 2.14. *We have the following exact sequences:*

$$\begin{aligned} 0 \rightarrow A_l \rightarrow J(T_l) \rightarrow J(V_l) \rightarrow 0, \\ 0 \rightarrow A_l \rightarrow J_{f,S_l}(T_l) \rightarrow J_{f,S_l}(V_l) \rightarrow 0. \end{aligned}$$

In particular

$$J(T_l)_{\text{tor}} = J_{f,S_l}(T_l)_{\text{tor}} = A_l$$

and the groups

$$J(T_l) \quad \text{and} \quad J_{f,S_l}(T_l)$$

are divisible.

Proof. Consider the following long exact sequence (see [T, p. 261])

$$H^0(G_L; A_l) \rightarrow H^1(G_L; T_l) \rightarrow H^1(G_L; V_l) \rightarrow H^1(G_L; A_l).$$

Taking direct limits with respect to finite extensions L/F gives the following short exact sequence:

$$0 \rightarrow A_l \rightarrow J(T_l) \rightarrow J(V_l) \rightarrow 0$$

This short exact sequence fits into the following commutative diagram:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & 0 & \longrightarrow & \varinjlim_{L/F} \prod_{w \notin S_l} H^1(G_w; T_l)/H_f^1 & \longrightarrow & \varinjlim_{L/F} \prod_{w \notin S_l} H^1(G_w; V_l)/H_f^1 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & A_l & \longrightarrow & J(T_l) & \longrightarrow & J(V_l) \longrightarrow 0 \\
 & & = \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & A_l & \longrightarrow & J_{f,S_l}(T_l) & \longrightarrow & J_{f,S_l}(V_l) \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
 \end{array} \tag{2.15}$$

The rows and columns of the diagram are exact. The exactness on the right of the bottom horizontal sequence follows from the injectivity of the top, nontrivial, horizontal arrow by Lemma 2.8. \square

Proposition 2.16. *Let L be a finite extension of F . Then we have isomorphisms:*

- (1) $H^1(G_L; T_l) \cong J(T_l)^{G_L}$,
- (2) $H_{f,S_l}^1(G_L; T_l) \cong J_{f,S_l}(T_l)^{G_L}$.

Proof. Under condition of Assumption I the proof of claim (1) is done in the same way as the proof of (4.1.1) of [BE]. To prove (2) take an arbitrary finite Galois extension L'/L and consider the following commutative diagram:

$$\begin{array}{ccc}
 0 & & 0 \\
 \downarrow & & \downarrow \\
 H_{f,S_l}^1(G_L; T_l) & \longrightarrow & H_{f,S_l}^1(G_{L'}; T_l)^{G(L'/L)} \\
 \downarrow & & \downarrow \\
 H^1(G_L; T_l) & \xrightarrow{\cong} & H^1(G_{L'}; T_l)^{G(L'/L)} \\
 \downarrow & & \downarrow \\
 \prod_{w \notin S_l} H^1(I_w; T_l) & \longrightarrow & \prod_{w \notin S_l} (\prod_{w'|w} H^1(I_{w'}; T_l))^{G(L'/L)}
 \end{array} \tag{2.17}$$

The columns of this diagram are exact. The upper horizontal arrow is trivially an imbedding. The middle horizontal arrow is an isomorphism. This follows directly from claim (1). Since the representation ρ_l is unramified outside S_l then using Theorem 8.1 and Corollary 8.3, Chapter I of [CF] and Kummer pairing we get the

following commutative diagram:

$$\begin{array}{ccc}
 H^1(I_w; T_l) & \longrightarrow & H^1(I_{w'}; T_l) \\
 \downarrow = & & \downarrow = \\
 \text{Hom}_{cts}(I_w; T_l) & \longrightarrow & \text{Hom}_{cts}(I_{w'}; T_l) \\
 \downarrow \cong & & \downarrow \cong \\
 \text{Hom}_{cts}(\mathbb{Z}_l(1); T_l) & \longrightarrow & \text{Hom}_{cts}(\mathbb{Z}_l(1); T_l)
 \end{array} \tag{2.18}$$

Since $L_{w'}/L_w$ is a finite extension, the bottom horizontal arrow is induced by a nontrivial (hence injective) homomorphism of \mathbb{Z}_l -modules $\mathbb{Z}_l(1) \rightarrow \mathbb{Z}_l(1)$. Because T_l is a free \mathbb{Z}_l -module, every nontrivial homomorphism of \mathbb{Z}_l -modules $\mathbb{Z}_l(1) \rightarrow T_l$ is injective. Hence the bottom horizontal arrow in diagram (2.18) is injective. So the bottom horizontal arrow in diagram (2.17) is also an imbedding. Now claim (2) follows by taking direct limits over L' in diagram (2.17) and chasing the resulting diagram. \square

At the end of this section we give some additional information about the reduction map

$$r_v : H_{f,S_l}^1(G_F; T_l) \rightarrow H^1(g_v; T_l).$$

Proposition 2.19. *Let $\hat{P} \in H_{f,S_l}^1(G_F; T_l)$ be a nontorsion element. Given $M_1 = l^{m_1}$ a fixed power of l , there exist infinitely many primes $v \notin S_l$ such that $r_v(\hat{P}) \in H^1(g_v; T_l)$ is an element of order at least M_1 .*

Proof. Let M be a power of l which we will specify below. Let F_M denote the extension $F(A_l[M])$. Consider the following commutative diagram:

$$\begin{array}{ccc}
 H_{f,S_l}^1(G_F; T_l)/M & \xrightarrow{r_v} & H^1(g_v; T_l)/M \\
 h_1 \downarrow & & \downarrow \\
 H_{f,S_l}^1(G_F; A_l[M]) & \xrightarrow{r_v} & H^1(g_v; A_l[M]) \\
 h_2 \downarrow & & \downarrow \\
 H_{f,S_l}^1(G_{F_M}; A_l[M]) & \xrightarrow{r_w} & H^1(g_w; A_l[M]) \\
 h_3 \downarrow & & \downarrow \\
 \text{Hom}(G_{F_M}; A_l[M]) & \xrightarrow{r_w} & \text{Hom}(G_w; A_l[M]) \\
 h_4 \downarrow \cong & & \downarrow = \\
 \text{Hom}(G_{F_M}^{ab}; A_l[M]) & \xrightarrow{r_w} & \text{Hom}(g_w; A_l[M])
 \end{array} \tag{2.20}$$

The horizontal arrows in diagram (2.20) are induced by the reduction maps. We describe the vertical map. The map h_2 is an injection (cf. Proposition 4.3 (1)). The map h_3 is the injection which comes from the long exact sequence in cohomology associated to the following exact sequence of G_{F_M} -modules:

$$0 \rightarrow A_l[M] \rightarrow J_{f,S_l}(T_l) \xrightarrow{\times M} J_{f,S_l}(T_l) \rightarrow 0. \tag{2.21}$$

The vertical maps on the right-hand side of diagram (2.20) are defined in the similar way. Consider the nontorsion element $\hat{P} \in H_{f,S_l}^1(G_F; T_l)$. Let l^s be the largest power of l such that $\hat{P} = l^s \hat{R}$ for an $\hat{R} \in H_{f,S_l}^1(G_F; T_l)$. Such an l^s exists since $H_{f,S_l}^1(G_F; T_l)$ is a finitely generated \mathbb{Z}_l -module. We put $M = M_1 l^s$. Let P' be the image of \hat{P} in $Hom(G_{F_M}^{ab}; A_l[M])$ under the composition of the maps h_1, h_2, h_3 and h_4 . Since the maps h_1, h_2, h_3 and h_4 are injective, the element P' is of order M_1 . By the Chebotarev density theorem there exist infinitely many primes $w \notin S_l$ such that the map r_w preserves the order of P' . Hence, for those w the element \hat{P} is mapped by the composition of left vertical and lower horizontal arrows onto an element whose order is M_1 . The commutativity of (2.20) implies that $r_v(\hat{P}) \in H^1(g_v; T_l)$ is of order at least M_1 for the primes $v = w \cap \mathcal{O}_{F,S_l}$. \square

Corollary 2.22. *Let $\hat{P} \in H_{f,S_l}^1(G_F; T_l)$ be an element which maps onto a generator of the free \mathbb{Z}_l -module $H_{f,S_l}^1(G_F; T_l)/tor$. There exist infinitely many primes $v \notin S_l$ such that $r_v(\hat{P})$ is a generator of a cyclic summand in the l -primary decomposition of the group $H^1(g_v; T_l)$.*

3. Specification of l -adic representations

In addition to Assumption I the representations which we consider are supposed to satisfy Assumption II stated below. In order to formulate the assumption we introduce more notation. We fix a finite extension E/\mathbb{Q} of degree $e = [E : \mathbb{Q}]$ such that the Hilbert class field E^H of E is contained in F . We assume that each prime l we consider splits completely in F . Let

$$(l) = \lambda_1 \dots \lambda_e$$

be the decomposition of the ideal (l) in \mathcal{O}_E . We also assume that \mathcal{O}_E acts on T_l in such a way that T_l is a free $\mathcal{O}_{E,l} = \mathcal{O}_E \otimes \mathbb{Z}_l$ module of rank h and that the action of $\mathcal{O}_{E,l}$ commutes with the action of G_F given by the representation ρ_l . It is clear that e divides $d = \dim \rho_l$ and $h = \frac{d}{e}$. Put $E_l = \mathcal{O}_{E,l} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. In addition, we denote by E_{λ_i} the completion of E at λ_i and by \mathcal{O}_{λ_i} the ring of integers in E_{λ_i} . Now,

it is obvious that

$$\mathcal{O}_{E,l} = \prod_{i=1}^e \mathcal{O}_{\lambda_i} \quad \text{and} \quad E_l = \prod_{i=1}^e E_{\lambda_i}.$$

Since T_l has the $\mathcal{O}_{E,l}$ -module structure, we can represent V_l and A_l as follows:

$$V_l = T_l \otimes_{\mathcal{O}_{E,l}} E_l,$$

$$A_l = T_l \otimes_{\mathcal{O}_{E,l}} E_l / \mathcal{O}_{E,l} = \bigoplus_{i=1}^e T_l \otimes_{\mathcal{O}_{E,l}} E_{\lambda_i} / \mathcal{O}_{\lambda_i} = \bigoplus_{i=1}^e A_{\lambda_i},$$

where we put $A_{\lambda_i} = T_l \otimes_{\mathcal{O}_{E,l}} E_{\lambda_i} / \mathcal{O}_{\lambda_i}$.

Note that every prime ideal λ_i is principal, because by assumption $E^H \subset F$. Hence, $\lambda_i = (\pi_i)$ for some $\pi_i \in \mathcal{O}_E$. In this case $E_{\lambda_i} / \mathcal{O}_{\lambda_i} \cong \mathbb{Q}_l / \mathbb{Z}_l$ for each i , hence all A_{λ_i} are divisible groups of the same corank h . Observe that $A_l[\lambda_i^k] = A_{\lambda_i}[\lambda_i^k]$ and

$$A_l[l] \cong \bigoplus_{i=1}^e A_l[\lambda_i], \tag{3.1}$$

where $\dim_{\mathbb{Z}/l} A_l[\lambda_i] = h$, for all $1 \leq i \leq e$. By assumptions and decomposition (3.1) it is clear that the image $\overline{\rho}_l(G_F)$ of the representation $\overline{\rho}_l$ is contained in the subgroup of $GL_d(\mathbb{Z}/l)$ which consists of matrices of the form

$$\begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & C_e \end{pmatrix},$$

where $C_i \in GL_h(\mathbb{Z}/l)$, for all $1 \leq i \leq e$. Hence, we can consider the image of $\overline{\rho}_l$ as a subgroup of the product $\prod_{i=1}^e GL_h(\mathbb{Z}/l)$.

Assumption II. Let $\mathcal{P} = \mathcal{P}(\rho)$ be an infinite set of prime numbers $l > 3$, which split completely in F and such that the l -adic representation ρ_l satisfies the following conditions.

- (1) If $h > 1$, then for each $1 \leq i \leq e$, there is a subgroup $H_i \trianglelefteq G(F(A[\lambda_i])/F) \subset GL_h(\mathbb{Z}/l) \cong GL(A_l[\lambda_i])$ such that:
 - (i) the subgroup $H_1 \times \cdots \times H_i \times \cdots \times H_e$ of the group $\prod_{i=1}^e GL_h(\mathbb{Z}/l)$ is contained in $\text{Im } \overline{\rho}_l = G_l$ and $H_1 \times \cdots \times H_i \times \cdots \times H_e$ has index prime to l in G_l ,
 - (ii) H_i acts irreducibly on $A_l[\lambda_i] \cong (\mathbb{Z}/l)^h$,
 - (iii) $H_i/[H_i, H_i]$ has order prime to l ,
 - (iv) there exist matrices $\sigma_i, \beta_i \in H_i$ such that 1 is an eigenvalue of σ_i with eigenspace of dimension 1 and 1 is not an eigenvalue of β_i ,

- (v) the centraliser of H_i in $GL_h(\mathbb{Z}/l)$ is $(\mathbb{Z}/l)^\times I_h$, i.e. if $\sigma \in GL_h(\mathbb{Z}/l)$ and $\sigma\gamma = \gamma\sigma$ for all $\gamma \in H_i$, then σ is a scalar matrix,
 - (vi) for each $1 \leq i \leq e$ the group H_i contains a nontrivial subgroup D_i^0 of the group $\{aI_h; a \in (\mathbb{Z}/l)^\times\} \subset GL_h(\mathbb{Z}/l)$ of scalar matrices.
- (2) If $h = 1$, we require that $G_l = G(F_l/F)$ satisfies two conditions:
- (i) for every $1 \leq i \leq d$, there is a diagonal matrix $\sigma_i = \text{diag}(\mu_1, \dots, \mu_d)$ in the group G_l with $\mu_i = 1$ and $\mu_j \neq 1$, for all $j \neq i$,
 - (ii) there is an isomorphism of rings $\mathbb{Z}/l[G_l] \cong \mathcal{O}_E/l$, where $\mathbb{Z}/l[G_l]$ denotes a subring of \mathcal{O}_E/l generated by \mathbb{Z}/l and the image of G_l in \mathcal{O}_E/l via the natural imbedding $G_l \rightarrow (\mathcal{O}_E/l)^\times$.

Definition 3.2. Let $\{B(L)\}_L$ be a direct system of \mathcal{O}_E -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 of fields $L \rightarrow L'$ the structure map $B(L) \rightarrow B(L')$ is a homomorphism of \mathcal{O}_E -modules. Let us put $B(\bar{F}) = \varinjlim_{L/F} B(L)$. Let ρ

and \mathcal{P} be as in Assumption II. The system $\{B(L)\}_L$ is called the Mordell-Weil \mathcal{O}_E -module of the pair (ρ, \mathcal{P}) if the following conditions are satisfied:

- (1) $B(L)$ is a finitely generated \mathcal{O}_E -module for all L .
- (2) There are functorial homomorphisms of \mathcal{O}_E -modules

$$\psi_{L,l} : B(L) \rightarrow H_{f,S_l}^1(G_L; T_l),$$

where L is as above and $l \in \mathcal{P}$, such that:

- (i) for every $l \in \mathcal{P}$, the induced map

$$\psi_{L,l} \otimes \mathbb{Z}_l : B(L) \otimes \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_L; T_l)$$

is an isomorphism or

- (ii) for every $l \in \mathcal{P}$, the map $\psi_{L,l} \otimes \mathbb{Z}_l$ is an imbedding, the group $B(\bar{F})$ is a discrete G_F -module which is divisible by l , and for every L we have: $B(\bar{F})^{G_L} \cong B(L)$ and $H^0(G_L; A_l) \subset B(L)$.

We end this section with the examples of Mordell-Weil \mathcal{O}_E -modules related to l -adic representations which satisfy Assumptions I and II.

Example 3.3. Consider the l -adic representation

$$\rho_l : G(\bar{F}/F) \rightarrow GL(\mathbb{Z}_l(1)) \cong GL_1(\mathbb{Z}_l) \cong \mathbb{Z}_l^\times$$

given by the cyclotomic character. In this case $T_l = \mathbb{Z}_l(1)$, $V_l = \mathbb{Q}_l(1)$ and $A_l = \mathbb{Q}_l/\mathbb{Z}_l(1)$. This representation is given by the action of G_F on the Tate module of the multiplicative group scheme \mathbb{G}_m/F . Let S be any finite set of primes in \mathcal{O}_F . Denote by S_l the set of primes consisting of primes in S and primes in F over l . Put $B(L) = \mathbb{G}_m(\mathcal{O}_{L,S}) = \mathcal{O}_{L,S}^\times$ for any finite extension L/F . The Kummer map (which is obviously injective)

$$B(L) \otimes \mathbb{Z}_l \rightarrow H^1(G_{L,S_l}; \mathbb{Z}_l(1)) \rightarrow H^1(G_L; \mathbb{Z}_l(1))$$

factors naturally through

$$\psi_{L,l} \otimes \mathbb{Z}_l : B(L) \otimes \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_F; \mathbb{Z}_l(1)).$$

In this case we take $E = \mathbb{Q}$ hence $\mathcal{O}_E = \mathbb{Z}$. We take \mathcal{P} to be the set of all prime numbers l such that $G(F(\mu_l)/F)$ is nontrivial.

Example 3.4. Let n be a positive integer. Let $T_l = \mathbb{Z}_l(n+1)$, hence $V_l = \mathbb{Q}_l(n+1)$ and $A_l = \mathbb{Q}_l/\mathbb{Z}_l(n+1)$. Consider the one-dimensional representation

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

which is given by the $(n+1)$ th tensor power of the cyclotomic character. For each odd prime number l and for a finite extension L/F consider the Dwyer–Friedlander map [DF]

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

Let C_L be the subgroup of $K_{2n+1}(L)$ which is generated by the l -parts of kernels of Dwyer–Friedlander maps for all odd primes l . We define the group $B(L)$ by putting

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

Note that the group C_L is finite by [DF] and it should vanish if the Quillen–Lichtenbaum conjecture holds. Note that in this case

$$H^1(G_L; \mathbb{Z}_l(n+1)) \cong H^1(G_{L,S_l}; \mathbb{Z}_l(n+1)) \cong H_{f,S_l}^1(G_L; \mathbb{Z}_l(n+1)).$$

It follows by the definition of $B(L)$ and surjectivity of the Dwyer–Friedlander map that

$$\psi_{L,l} \otimes \mathbb{Z}_l : B(L) \otimes \mathbb{Z}_l \cong H^1(G_L; \mathbb{Z}_l(n+1)).$$

In the following three examples we discuss representations which come from Tate modules of abelian varieties. Let A/F be a simple abelian variety of dimension d over a number field F . As usual, we denote by $T_l = T_l(A)$ the Tate module of A . Consider

the l -adic representation

$$\rho_l : G_F \rightarrow GL(T_l(A)).$$

Assumption I holds due to the Weil conjectures (cf. [Sil, pp. 132-134]). Let S be the set of prime ideals of F at which A has bad reduction. By the Kummer pairing and Serre–Tate theorem ([ST, Theorem 1, p. 493] and Corollaries 1 and 2 of Manin’s Appendix II to the book [M]) we have a natural imbedding

$$\psi_{L,l} \otimes \mathbb{Z}_l : A(L) \otimes \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_L; T_l(A)).$$

Put $B(L) = A(L)$ for any finite extension L/F .

Example 3.5. Let A/F be a simple abelian variety with complex multiplication by a CM field E (cf. [La]) such that $E^H \subset F$, where E^H is the Hilbert class field of E . We assume that CM type of A is nondegenerate (cf. [BGK1, Definition 2.1]) and defined over F . Condition (i) of Assumption II (2) holds by Theorem 2.1 of [BGK1] (for CM elliptic curves it also follows by an alternative argument cf. [C-RS, Lemma 5.1, p. 286]). Condition (ii) of Assumption II (2) follows by Proposition, p. 72 of [R2]. We take \mathcal{P} to be the set of prime numbers l which split completely in F and such that A has good reduction at l .

Example 3.6. Consider a simple, principally polarised abelian variety A/F such that $E = \text{End}_F(A) \otimes \mathbb{Q} = \text{End}_{\bar{F}}(A) \otimes \mathbb{Q}$ (cf. [R1,C]) where $e = [E : \mathbb{Q}]$ and $2he = 2g$ with h and odd integer. In addition, we choose F to be a number field satisfying conditions indicated in the discussion which follows Theorem 3.1 of [BGK1] and such that $E^H \subset F$. We take \mathcal{P} to be the set of prime numbers $l \geq 0$ which split completely in F , and such that A has good reduction at l . Hence by Theorem 3.5 of [BGK1] we get

$$\prod_{i=1}^e Sp_{2h}(\mathbb{F}_l) = [G_l, G_l].$$

Taking $H_i = Sp_{2h}(\mathbb{F}_l)$, for all $1 \leq i \leq e$, we observe that conditions of Assumption II (1) are fulfilled since

- (i) $\prod_{i=1}^e Sp_{2h}(\mathbb{F}_l) \subset G_l$, and the quotient group $GS_{p_{2h}}(\mathbb{F}_l)/Sp_{2h}(\mathbb{F}_l)$ has order prime to l ,
- (ii) $Sp_{2h}(\mathbb{F}_l)$ acts on $A_l[\lambda_i] \cong (\mathbb{Z}/l)^{2h}$, in an irreducible way.
- (iii) $Sp_{2h}(\mathbb{F}_l)$ modulo its centre is a simple group.

(iv) matrix $\sigma_i \in Sp_{2h}(\mathbb{F}_l)$

$$\sigma_i = \begin{pmatrix} J_h(1) & J_h(1) \\ O & (J_h(1)')^{-1} \end{pmatrix}$$

has eigenvalue 1 with the eigenspace of dimension 1 where $J_h(1)$ is the $h \times h$ Jordan block matrix with 1 as the eigenvalue and $\beta_i = -I_{2h} \in Sp_{2h}(\mathbb{F}_l)$ does not have 1 as an eigenvalue.

(v) The centraliser of $Sp_{2h}(\mathbb{F}_l)$ in $GL_{2h}(\mathbb{F}_l)$ is $(\mathbb{F}_l)^\times I_{2h}$.

Observe that condition (1) (vi) of Assumption II is satisfied since obviously $-I_{2h} \in Sp_{2h}(\mathbb{F}_l)$.

There are two special cases of Example 3.6 that have been considered extensively in the past.

Example 3.7. (a) Let A/F be a simple, principally polarised abelian variety with real multiplication by a totally real field $E = End_F(A) \otimes \mathbb{Q} = End_{\bar{F}}(A) \otimes \mathbb{Q}$ such that $e = g$ and $h = 1$ (cf. [R1]). We choose F to be such a number field that $E^H \subset F$. We take \mathcal{P} to be the set of prime numbers l which split completely in F and such that A has a good reduction at l . Theorem 5.5.2, p. 801 of [R1] or Theorem 3.5 of [BGK1] implies that the image of the representation $\bar{\rho}_l$ contains the subgroup

$$\prod_{i=1}^g SL_2(\mathbb{F}_l) = \prod_{i=1}^g Sp_2(\mathbb{F}_l),$$

therefore the representation $\bar{\rho}_l$ satisfies Assumption II (1).

(b) Let A/F be a simple, principally polarised abelian variety with the property that $End_{\bar{F}}(A) = \mathbb{Z}$ and $g = \dim A$ is odd or equal to 2 or 6. In this case $E = \mathbb{Q}$ hence $e = 1$ and $h = g$. By the theorem of Serre [Se1, Theorem 3] the image of the representation $\bar{\rho}_l$ equals $GSp_{2g}(\mathbb{F}_l)$ (hence contains $Sp_{2g}(\mathbb{F}_l)$) for almost all l . We take \mathcal{P} to be the set of prime numbers such that the image of $\bar{\rho}_l$ equals $GSp_{2g}(\mathbb{F}_l)$ and A has good reduction at l . Hence the image of the representation $\bar{\rho}_l$ satisfies condition (1) of Assumption II.

It is rather hard to find further examples of Mordell-Weil \mathcal{O}_E -modules satisfying condition (2)(i) of Definition 3.2. Indeed, if we concentrate on finding a Mordell-Weil \mathcal{O}_E -module associated to T_l coming from étale cohomology of a smooth proper scheme X over F , then we should first prove Conjecture 5.3 (ii) p. 370 of [BK], for such an X .

4. Key propositions

Definition 4.1. Let

$$\phi_P : G_{F_l} \rightarrow A_l[l]$$

be the map:

$$\phi_P(\sigma) = \sigma\left(\frac{1}{l}\hat{P}\right) - \frac{1}{l}\hat{P},$$

where $P \in B(F)$ and \hat{P} is the image of P via the natural map

$$B(F) \rightarrow B(F) \otimes \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_F; T_l) \subset J_{f,S_l}(T_l).$$

Remark 4.2. Note that $\frac{1}{l}\hat{P}$ makes sense in $J_{f,S_l}(T_l)$ since the last group is divisible due to Proposition 2.14. The element $\frac{1}{l}\hat{P}$ is defined up to an element of the group $A_l[l]$.

Proposition 4.3. *Suppose that the Assumptions I and II are fulfilled. Then the following properties hold.*

- (1) $H^r(G(F_l/F); A_l[l]) = 0$ for $r \geq 0$ and all $l \in \mathcal{P}$, except the case of trivial G_l -module $A_l[l]$ when $r = 0$ and $d = 1$.
- (2) The map $H_{f,S_l}^1(G_F; T_l)/l \rightarrow H_{f,S_l}^1(G_{F_l}; T_l)/l$ is injective for all $l \in \mathcal{P}$.
- (3) The map $B(F)/lB(F) \rightarrow B(F_l)/lB(F_l)$ is injective for all $l \in \mathcal{P}$.
- (4) Let $P \in B(F)$. If $l \in \mathcal{P}$ does not divide $\#B(F)_{\text{tor}}$ and $P \notin \lambda_i B(F)$ for all $1 \leq i \leq e$, then the map ϕ_P is surjective.

Proof. (1) First let us consider the case $h > 1$. The group $D^0 = \prod_{i=1}^e D_i^0$ can be regarded as a subgroup of G_l once we identify G_l with its image via $\bar{\rho}_l$. D^0 is a normal subgroup of G_l . Assumption II (1) (vi) allows us to consider the Hochschild–Serre spectral sequence

$$E_2^{r,s} = H^r(G_l/D^0; H^s(D^0; A_l[l])) \Rightarrow H^{r+s}(G_l; A_l[l]). \tag{4.4}$$

Observe that $H^0(D^0; A_l[l]) = \bigoplus_{i=1}^e H^0(D_i^0; A_l[\lambda_i]) = 0$ because by definition D_i^0 is nontrivial and acts by matrix multiplication (actually scalar multiplication) on the \mathbb{Z}/l vector space $A_l[\lambda_i] \cong (\mathbb{Z}/l)^h$. The groups $H^s(D^0; A_l[l])$ vanish for $s > 0$, since l is odd by assumption and the order of D^0 is prime to l . Hence the claim (1) follows for $h > 1$. Now let $h = 1$. Note that G_l is isomorphic to a subgroup of diagonal matrices in $GL(A_l[l]) = GL_d(\mathbb{Z}/l)$. Since G_l has order relatively prime to l , $H^s(G_l; A_l[l]) = 0$ for $s > 0$. It follows easily by Assumption II (2) (i) that $H^0(G_l; A_l[l]) = 0$, for all $l \in \mathcal{P}$

and $d > 1$. This proves (1) in the case $h = 1$. If $d = 1$, then $H^0(G_l; A_l[l]) = 0$ ($= A_l[l]$ resp.) if $A_l[l]$ is nontrivial (trivial resp.) G_l -module.

(2) By Proposition 2.14, we have the following short exact sequence:

$$0 \rightarrow A_l[l] \rightarrow J_{f,S_l}(T_l) \xrightarrow{l} J_{f,S_l}(T_l) \rightarrow 0.$$

By the long exact sequence in cohomology associated to this exact sequence and Proposition 2.16, we obtain the commutative diagram in which the horizontal maps are injections.

$$\begin{array}{ccc}
 0 & & 0 \\
 \downarrow & & \downarrow \\
 \ker \alpha & \longrightarrow & H^1(G_l; A_l[l]) \\
 \downarrow & & \downarrow \\
 H^1_{f,S_l}(G_F; T_l)/l & \longrightarrow & H^1(G_F; A_l[l]) \\
 \downarrow \alpha & & \downarrow \gamma \\
 H^1_{f,S_l}(G_{F_l}; T_l)/l & \longrightarrow & H^1(G_{F_l}; A_l[l])
 \end{array} \tag{4.5}$$

However, $\ker \alpha = 0$, since it injects into the group $H^1(G_l; A_l[l])$ which vanishes by part (1) of the proposition.

(3) Let us first consider case (2) (i) of Definition 3.2. Because the map

$$B(L) \otimes \mathbb{Z}_l \rightarrow H^1_{f,S_l}(G_L; T_l),$$

is an isomorphism, the group $B(L)/l$ is isomorphic to $H^1_{f,S_l}(G_L; T_l)/l$. This shows that the horizontal maps in the commutative diagram

$$\begin{array}{ccc}
 B(F)/l & \longrightarrow & H^1_{f,S_l}(G_F; T_l)/l \\
 \downarrow & & \downarrow \alpha \\
 B(F_l)/l & \longrightarrow & H^1_{f,S_l}(G_{F_l}; T_l)/l
 \end{array} \tag{4.6}$$

are isomorphisms. Since we have proved in (2) that the map α is an injection, diagram (4.6) gives claim (3). Now consider case (2) (ii) of Definition 3.2. We get the exact sequence of G_F -modules:

$$0 \rightarrow A_l[l] \rightarrow B(\bar{F}) \xrightarrow{l} B(\bar{F}) \rightarrow 0.$$

This gives the following commutative diagram with injective horizontal arrows:

$$\begin{array}{ccc}
 0 & & 0 \\
 \downarrow & & \downarrow \\
 \ker \beta & \longrightarrow & H^1(G_l; A_l[l]) \\
 \downarrow & & \downarrow \\
 B(F)/l & \longrightarrow & H^1(G_F; A_l[l]) \\
 \downarrow \beta & & \downarrow \gamma \\
 B(F_l)/l & \longrightarrow & H^1(G_{F_l}; A_l[l])
 \end{array} \tag{4.7}$$

Since by (1) the map γ is injective for all $l \in \mathcal{P}$, the map β is also injective for all $l \in \mathcal{P}$.

(4) We easily check that the image of the map ϕ_P is G_F -invariant. If ϕ_P were not surjective, then $Im \phi_P$ would be a proper G_F submodule of $A_l[l]$. It is clear from the decomposition (3.1) of $A_l[l]$ and Assumption II (1) and (2) (ii) that every G_F submodule of $A_l[l]$ is of the form $A_l[\lambda_{i_1}] \oplus \dots \oplus A_l[\lambda_{i_r}]$ for some $i_1, \dots, i_r \in \{1, \dots, e\}$. Hence if $Im \phi_P$ were a proper G_F submodule, we could assume that

$$Im \phi_P \subset A_l[\lambda_1] \oplus \dots \oplus A_l[\lambda_{i-1}] \oplus A_l[\lambda_{i+1}] \oplus \dots \oplus A_l[\lambda_e]$$

for some $1 \leq i \leq e$. This implies that

$$\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e \left(\sigma \left(\frac{1}{l} \hat{P} \right) - \frac{1}{l} \hat{P} \right) = 0 \tag{4.8}$$

for every $\sigma \in G(\bar{F}/F_l)$. Equality (4.8) takes place in $J_{f,S_l}(T_l)$ under the (2) (i) part of Definition 3.2 (resp. in $B(\bar{F})$ under case (2) (ii) of Definition 3.2) and it implies that

$$\sigma \left(\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e \frac{1}{l} \hat{P} \right) = \pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e \frac{1}{l} \hat{P} \tag{4.9}$$

for every $\sigma \in G(\bar{F}/F_l)$. Hence by Proposition 2.16 (2) (resp. by Definition 3.2, of the Mordell-Weil \mathcal{O}_E -module $\{B(L)\}$) we get

$$\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e \frac{1}{l} \hat{P} \in H_{f,S_l}^1(G_{F_l}; T_l) \quad (\in B(F_l) \text{ resp.}). \tag{4.10}$$

So $\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e \hat{P} = 0$ in the group $H_{f,S_l}^1(G_{F_l}; T_l)/l$ (in $B(F_l)/lB(F_l)$, resp.). By parts (2) and (3) of the Proposition (see also diagram (4.6)) this implies

$\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e P = 0$ in the group $B(F)/lB(F)$ in both cases. Hence there is $P_1 \in B(F)$ such that $\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e P = lP_1$. This gives the equality

$$\pi_1 \dots \pi_{i-1} \pi_{i+1} \dots \pi_e (P - \pi_i P_2) = 0, \tag{4.11}$$

where $P_2 = uP_1 \in B(F)$ for some $u \in \mathcal{O}_E^\times$. Multiplying equation (4.11) by π_i we obtain the equality $l(P - \pi_i P_2) = 0$ in the group $B(F)$. Since, by assumption, $\#B(F)_l = 0$ we get $P = \pi_i P_2$, hence $P \in \lambda_i B(F)$ which contradicts the assumptions. \square

For a given l let $\bar{\rho}_i$ denote the representation:

$$\bar{\rho}_i : G_F \rightarrow GL(A_l[\lambda_i]).$$

Similarly to the definition of F_l we put $F_i = \bar{F}^{ker \bar{\rho}_i}$. In analogy with the Definition 4.1 we introduce a homomorphism

$$\begin{aligned} \phi_i : G_{F_i} &\rightarrow A_l[\lambda_i], \\ \phi_i(\sigma) &= \sigma \left(\frac{1}{\pi_i} \hat{P} \right) - \frac{1}{\pi_i} \hat{P}. \end{aligned}$$

Proposition 4.12. *We have the following properties.*

- (1) $H^r(G(F_i/F); A_l[\lambda_i]) = 0$ for $r \geq 0$, all $l \in \mathcal{P}$, and $1 \leq i \leq e$ except the case of trivial $G(F_i/F)$ -module $A_l[\lambda_i]$ when $r = 0$.
- (2) The map $H_{f, S_l}^1(G_F; T_l)/\lambda_i \rightarrow H_{f, S_l}^1(G_F; T_l)/\lambda_i$ is injective for all $l \in \mathcal{P}$ and $1 \leq i \leq e$.
- (3) The map $B(F)/\lambda_i B(F) \rightarrow B(F_i)/\lambda_i B(F_i)$ is injective for all $l \in \mathcal{P}$ and $1 \leq i \leq e$.
- (4) Let $P \in B(F)$. If $l \in \mathcal{P}$ does not divide $\#B(F)_{\text{tor}}$ and $P \notin \lambda_i B(F)$, then the map ϕ_i is surjective.

Proof. Proofs of (1), (2), and (3) are done in the same way as the corresponding proofs in Proposition 4.3. Statement (4) holds because ϕ_i is obviously G_F equivariant, ϕ_i is nontrivial since $P \notin \lambda_i B(F)$, and $A_l[\lambda_i]$ is an irreducible $\mathbb{Z}/l[G_F]$ module due to Assumption II. \square

Let P, Q be two nontorsion elements of the group $B(F)$. Let S_l be the finite set of primes which contains primes for which ρ_l is ramified and primes over l . For $v \notin S_l$ let

$$r_v : H_{f, S_l}^1(G_F; T_l) \rightarrow H^1(g_v; T_l)$$

denote the reduction map at a prime ideal v of \mathcal{O}_F . We will investigate the linear dependence of P and Q over \mathcal{O}_E in $B(F)$ under some local conditions for the maps r_v ,

(see statement of Theorem 5.1 below). We need some additional notation. Let \mathcal{P}^* be the set of rational primes $l \in \mathcal{P}$ such that $P \notin \lambda_i B(F)$ and $Q \notin \lambda_i B(F)$ for all $1 \leq i \leq e$. The set $\mathcal{P} \setminus \mathcal{P}^*$ is finite, since $B(F)$ is finitely generated \mathcal{O}_E -module. Let $\hat{R} \in J_{f,S_l}(T_l)$ be such that $l\hat{R} = \hat{P}$. The element \hat{R} exists by Proposition 2.14. The Galois group G_{F_l} acts on the set

$$\{\hat{R} + t : t \in A_l[l]\}$$

which is contained in $J_{f,S_l}(T_l)$. Let $N_P \subset G_{F_l}$ be the kernel of this action. Note that N_P is a normal subgroup of G_{F_l} of finite index. Define the field

$$F_l\left(\frac{1}{l}\hat{P}\right) = \bar{F}^{N_P}.$$

Let $F_l(\frac{1}{l}\hat{Q})$ denote the corresponding field defined for Q . Observe that $F_l(\frac{1}{l}\hat{P})/F$ and $F_l(\frac{1}{l}\hat{Q})/F$ are Galois extensions and we have isomorphisms

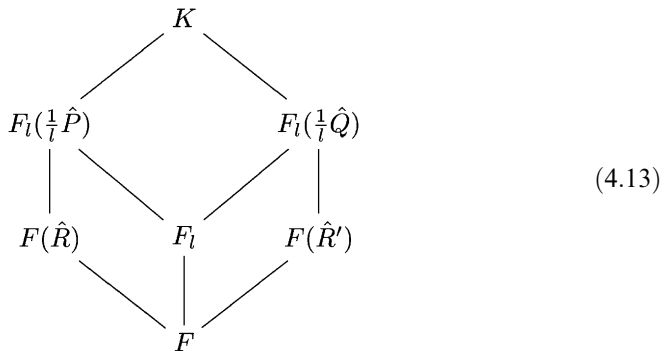
$$\text{Gal}\left(F_l\left(\frac{1}{l}\hat{P}\right)/F\right) \cong H_2 \rtimes G_l, \quad \text{Gal}\left(F_l\left(\frac{1}{l}\hat{Q}\right)/F\right) \cong H_1 \rtimes G_l,$$

where

$$H_1 = \text{Gal}\left(F_l\left(\frac{1}{l}\hat{Q}\right)/F_l\right), \quad H_2 = \text{Gal}\left(F_l\left(\frac{1}{l}\hat{P}\right)/F_l\right).$$

By Proposition 4.3 (4) the group H_1 (H_2 , respectively) can be identified with $A_l[l]$ via the map ϕ_Q (ϕ_P , resp.). Put $K = F_l(\frac{1}{l}\hat{P})F_l(\frac{1}{l}\hat{Q})$.

All fields introduced above are displayed in the diagram below.



Similarly, let $\hat{R}_i \in J_{f,S_l}(T_l)$ be such that $\pi_i \hat{R}_i = \hat{P}$. The element \hat{R}_i exists by Proposition 2.14. The Galois group G_{F_i} acts on the set

$$\{\hat{R}_i + t : t \in A_l[\lambda_i]\}$$

which is contained in $J_{f,S_i}(T_i)$. Let $N_i \subset G_{F_i}$ be the kernel of this action. Note that N_i is a normal subgroup of G_{F_i} of finite index. Define the field

$$F_i\left(\frac{1}{\pi_i}\hat{P}\right) = \bar{F}^{N_i}.$$

Let $F_i(\frac{1}{\pi_i}\hat{Q})$ denote the corresponding field defined in the same way for Q . Observe that $F_i(\frac{1}{\pi_i}\hat{P})/F$ and $F_i(\frac{1}{\pi_i}\hat{Q})/F$ are Galois extensions and there are isomorphisms

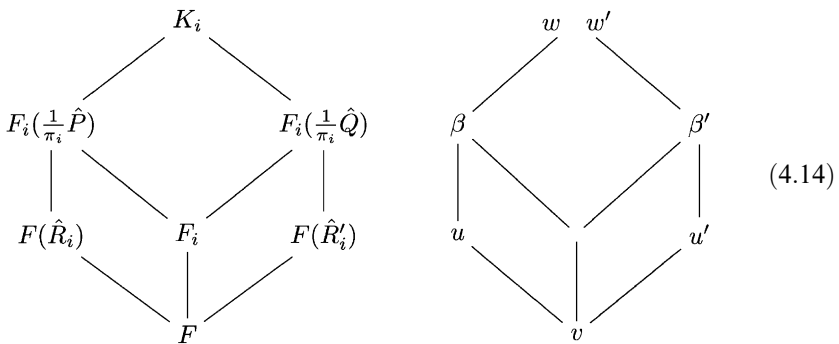
$$\text{Gal}\left(F_i\left(\frac{1}{\pi_i}\hat{P}\right)/F\right) \cong H_{2,i} \rtimes G(F_i/F), \quad \text{Gal}\left(F_i\left(\frac{1}{\pi_i}\hat{Q}\right)/F\right) \cong H_{1,i} \rtimes G(F_i/F),$$

where

$$H_{1,i} = \text{Gal}\left(F_i\left(\frac{1}{\pi_i}\hat{Q}\right)/F_i\right), \quad H_{2,i} = \text{Gal}\left(F_i\left(\frac{1}{\pi_i}\hat{P}\right)/F_i\right).$$

By Proposition 4.12 (4) the group $H_{1,i}$ ($H_{2,i}$, resp.) can be identified with $A_l[\lambda_i]$ via the map ϕ_i for Q (for P resp.) Put $K_i = F_i(\frac{1}{\pi_i}\hat{P})F_i(\frac{1}{\pi_i}\hat{Q})$.

Fields introduced above are displayed in the left diagram below. In the right diagram we depicted the relevant prime ideals that will be used in the proof of Theorem 5.1 below.



Remark 4.15. Observe that

$$F_l\left(\frac{1}{l}\hat{P}\right) = F_1\left(\frac{1}{\pi_1}\hat{P}\right) \cdots F_i\left(\frac{1}{\pi_i}\hat{P}\right) \cdots F_e\left(\frac{1}{\pi_e}\hat{P}\right),$$

$$F_l\left(\frac{1}{l}\hat{Q}\right) = F_1\left(\frac{1}{\pi_1}\hat{Q}\right) \cdots F_i\left(\frac{1}{\pi_i}\hat{Q}\right) \cdots F_e\left(\frac{1}{\pi_e}\hat{Q}\right).$$

In addition there is an equality

$$[F(\hat{R}_i) : F] = \left[F_i \left(\frac{1}{\pi_i} \hat{P} \right) : F_i \right],$$

since by Proposition 4.12 (4) there are $[F_i(\frac{1}{\pi_i}\hat{P}) : F_i]$ different imbeddings of $F(\hat{R}_i)$ into \tilde{F} that fix F . Hence from diagram (4.14) we find out that $F(\hat{R}_i) \cap F_i = F$.

5. The support problem for l -adic representations

Theorem 5.1. *Let \mathcal{P}^* be the infinite set of prime numbers introduced after the proof of Proposition 4.12. Assume that for every $l \in \mathcal{P}^*$ the following condition holds in the group $H^1(g_v; T_l)$.*

For every integer m and for almost every $v \notin S_l$

$$mr_v(\hat{P}) = 0 \text{ implies } mr_v(\hat{Q}) = 0.$$

Then there exist $a \in \mathbb{Z} - \{0\}$ and $f \in \mathcal{O}_E - \{0\}$ such that $aP + fQ = 0$ in $B(F)$.

Lemma 5.2. *Let $H_{1,i}$ and $H_{2,i}$ be two h -dimensional \mathbb{F}_l -vector spaces equipped with the natural action of the group $G_i = \text{Im } \bar{\rho}_i \subset GL_h(\mathbb{F}_l)$. Let us denote by Ω_i the semidirect product $(H_{1,i} \oplus H_{2,i}) \rtimes G_i$. Assume that we are given $\sigma_i \in G_i$ such that for every $h_1 \in H_{1,i}$ $(h_1, 0, \sigma_i) \in (H_{1,i} \oplus \{0\}) \rtimes G_i$ is conjugate to an element $(0, h_2, \tau_i) \in (\{0\} \oplus H_{2,i}) \rtimes G_i$. Then 1 is not an eigenvalue of the matrix σ_i .*

Proof. cf. [C-RS, Lemma 4.2]. □

Remark 5.3. Observe, that by Assumption II, for every $1 \leq i \leq e$ and every $l \in \mathcal{P}$ there exists a matrix $\sigma_i \in G_i$, such that 1 is an eigenvalue of σ_i with an eigenspace of dimension 1.

Proof of Theorem 5.1. We want to prove that

$$F_l \left(\frac{1}{l} \hat{P} \right) = F_l \left(\frac{1}{l} \hat{Q} \right). \tag{5.4}$$

Hence it is enough to prove that for each $1 \leq i \leq e$ we have

$$F_i \left(\frac{1}{\pi_i} \hat{P} \right) = F_i \left(\frac{1}{\pi_i} \hat{Q} \right). \tag{5.5}$$

Suppose this is false for some i . Then we observe that

$$F_i \left(\frac{1}{\pi_i} \hat{P} \right) \cap F_i \left(\frac{1}{\pi_i} \hat{Q} \right) = F_i,$$

since both groups $H_{1,i} = G(F_i(\frac{1}{\pi_i}\hat{Q})/F_i)$ and $H_{2,i} = G(F_i(\frac{1}{\pi_i}\hat{P})/F_i)$ are irreducible $G_i = G(F_i/F)$ modules by Assumption II (1) (ii). Hence

$$\text{Gal}(K_i/F_i) \cong H_{1,i} \oplus H_{2,i} \cong A_l[\lambda_i] \oplus A_l[\lambda_i]. \tag{5.6}$$

We need the following result.

Lemma 5.7. *We have the following equality:*

$$K_i \cap F_l = F_i.$$

Proof. By (5.6) the group $G(K_i/F_i)$ is abelian of order l^{2h} . If $h = 1$, then $G(F_l/F_i) \subset \prod_{j=1, j \neq i}^d GL_1(\mathbb{Z}/l)$ has order relatively prime to l and it is clear that $K_i \cap F_l = F_i$.

Now assume that $h > 1$. We observe that

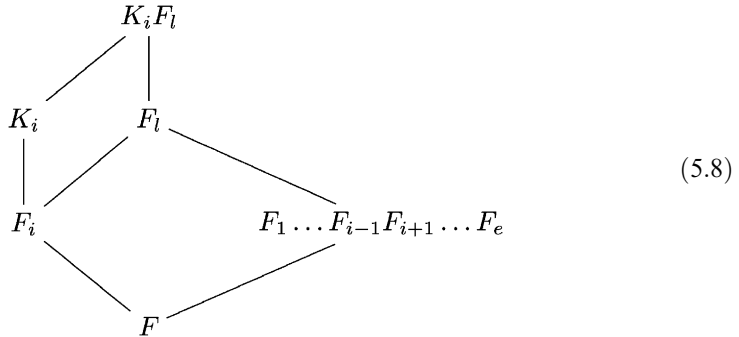
$$\prod_{j=1, j \neq i}^e [H_j, H_j] \subset \prod_{j=1, j \neq i}^e H_j \subset G(F_l/F_i)$$

hence by Assumption II (1) (i) and (iii) the subgroup $\prod_{j=1, j \neq i}^e [H_j, H_j]$ has index prime to l in $G(F_l/F_i)$. On the other hand

$$\prod_{j=1, j \neq i}^e [H_j, H_j] \subset [G(F_l/F_i), G(F_l/F_i)] \subset G(F_l/F_i),$$

hence the group $G(F_l/F_i)^{\text{ab}} = G(F_l/F_i)/[G(F_l/F_i), G(F_l/F_i)]$ has order prime to l . Let $K_0 = K_i \cap F_l$. Then K_0/F_i , as a subextension of K_i/F_i , is abelian with order equal to some power of l . On the other hand $G(K_0/F_i)$ is a quotient of the abelian group $G(F_l/F_i)^{\text{ab}}$, which has order prime to l . This implies that the group $G(K_0/F_i)$ is trivial. Hence $K_0 = F_i$. \square

Let us now return to the proof of Theorem 5.1. Consider the following tower of fields.



We can regard $G_l = G(F_l/F)$ as the subgroup of $\prod_{j=1}^e GL_h(\mathbb{F}_l)$. Let us pick $\sigma_l \in G_l$ such that $\sigma_l|_{F_i} = \sigma_i$ and $\sigma_l|_{F_j} = \beta_j$ for all $j \neq i$. Such a σ_l exists by Assumption II (1) (iv). Note that σ_l considered as a linear operator on the \mathbb{F}_l vector space $A_l[l]$ has an eigenvalue 1 with the eigenspace of dimension 1. Let $h_1 \in H_{1,i}$ be an arbitrary element. Let us pick an element of $G(K_i/F_i) \cong H_{1,i} \oplus H_{2,i}$ such that its projection onto $H_{1,i}$ is h_1 and its projection onto $H_{2,i}$ is a trivial element. We denote this element as $(h_1, 0)$. Taking into account Lemma 5.7, Remark 4.15 and the isomorphism of Galois groups $Gal(K_i/F) \cong (H_{1,i} \oplus H_{2,i}) \rtimes G(F_i/F)$, we can define an element $\gamma \in G(K_i F_l/F)$ such that $\gamma|_{K_i} = (h_1, 0, \sigma_i)$, $\gamma|_{F(\hat{R}_i)} = id_{F(\hat{R}_i)}$ and $\gamma|_{F_l} = \sigma_l$. By Chebotarev density theorem there exists a prime \tilde{w} of $K_i F_l$ such that:

- (i) $Fr_{\tilde{w}} = \gamma \in G(K_i F_l/F)$,
- (ii) the unique prime v in F below \tilde{w} is not in S_l and satisfies the assumptions of Theorem 5.1.

By the choice of prime v we see that

$$H^0(g_v; A_l)[l] = \bigoplus_{j=1}^e H^0(g_v; A_l)[\pi_j] = H^0(g_v; A_l)[\pi_i]$$

and also $H^0(g_v; A_l)[l] \cong \mathbb{Z}/l$. Hence for each $k \geq 1$ we have

$$H^0(g_v; A_l)[l^k] = H^0(g_v; A_l)[\pi_i^k]$$

which, together with finiteness of $H^0(g_v; A_l)$, shows that there is an m such that

$$H^0(g_v; A_l) = H^0(g_v; A_l)[l^m] = H^0(g_v; A_l)[\pi_i^m] \tag{5.9}$$

and $H^1(g_v; T_l) \cong H^0(g_v; A_l)$ is a finite, cyclic group.

Let w (u resp.) be the prime of K_i ($F(\hat{R}_i)$ resp.) which is over v and below \tilde{w} (cf. diagram (4.14)). Consider the following commutative diagram.

$$\begin{array}{ccc}
 H_{f,S_i}^1(G_{K_i}; T_l) & \xrightarrow{r_w} & H^1(g_w; T_l) \\
 \uparrow & & \uparrow \\
 H_{f,S_i}^1(G_{F_i(\frac{\hat{P}}{\pi_i})}; T_l) & \xrightarrow{r_\beta} & H^1(g_\beta; T_l) \\
 \uparrow & & \uparrow \\
 H_{f,S_i}^1(G_{F(\hat{R}_i)}; T_l) & \xrightarrow{r_u} & H^1(g_u; T_l) \\
 \uparrow & & \cong \uparrow \\
 H_{f,S_i}^1(G_F; T_l) & \xrightarrow{r_v} & H^1(g_v; T_l)
 \end{array} \tag{5.10}$$

The lowest right vertical arrow in diagram (5.10) is an isomorphism because, by the choices we have made the prime v splits in $F(\hat{R}_i)$ which means that $k_v \cong k_u$. Note that prime ideal v does not need to split completely in $F(\hat{R}_i)/F$ since this extension is usually not Galois. The left vertical arrows are embeddings by Proposition 2.16. Since v splits in $F(\hat{R}_i)$, we have the following equality in the group $H^1(g_v; T_l)$

$$r_v(\hat{P}) = \pi_i r_u(\hat{R}_i).$$

Let $t_v = l^m$ denote the order of the finite cyclic group $H^1(g_v; T_l) \cong H^0(g_v; A_l)$. For some $c \in \mathcal{O}_E^\times$ we have

$$\frac{t_v}{l} r_v(\hat{P}) = \frac{t_v}{l} \pi_i r_u(\hat{R}_i) = l^{m-1} \pi_i r_u(\hat{R}_i) = c \prod_{j \neq i} \pi_j^{m-1} (\pi_i^m r_u(\hat{R}_i)) = 0 \tag{5.11}$$

in the group $H^1(g_v; T_l)$, since $r_u(\hat{R}_i) \in H^0(g_v; A_l)[\pi_i^m]$ by (5.9).

By the assumption of Theorem 5.1, equality (5.11) implies that

$$\frac{t_v}{l} r_v(\hat{Q}) = 0. \tag{5.12}$$

Since $H^1(g_v; T_l)$ is cyclic, equality (5.12) implies that

$$r_v(\hat{Q}) \in lH^1(g_v; T_l).$$

This gives

$$r_v(\hat{Q}) = \pi_i \tilde{R}_i'' \tag{5.13}$$

for some $\hat{R}_i'' \in H^1(g_v; T_l)$. By Proposition 2.14 we can find an element $\hat{R}_i'' \in J_{f,S_l}(T_l)$ such that

$$\pi_i \hat{R}_i'' = \hat{Q}. \tag{5.14}$$

Choose a prime u'' in $F(\hat{R}_i'')$ over v . Let w' be a prime over u'' in K_i . Observe that, by the diagram similar to diagram 5.10 with \hat{P} and \hat{R}_i replaced by \hat{Q} and \hat{R}_i'' we obtain by (5.14) that

$$r_v(\hat{Q}) = \pi_i r_{u''}(\hat{R}_i'') \tag{5.15}$$

in the group $H^1(g_{u''}; T_l)$, hence also in $H^1(g_{w'}; T_l)$. By (5.13) and (5.15) we get

$$r_{w'}(\hat{R}_i'') - \hat{R}_i'' \in A_l[\pi_i] \cap H^1(g_{w'}; T_l).$$

Because $A_l[\pi_i] \subset H_{f,S_l}^1(G_{K_i}; T_l)$ (cf. proof of Lemma 2.11 and diagram (2.12)), by Lemma 2.13 there exists $\hat{P}_0 \in H_{f,S_l}^1(G_{K_i}; T_l)$ such that $r_{w'}(\hat{P}_0) = r_{u''}(\hat{R}_i'') - \hat{R}_i''$. We have the following equality:

$$r_{w'}(\hat{R}_i'' - \hat{P}_0) = \hat{R}_i''$$

in the group $H^1(g_{w'}; T_l)$.

Let $\hat{R}_i' = \hat{R}_i'' - \hat{P}_0$. Since $F(\hat{R}_i') \subset F_l(\frac{1}{l}\hat{Q})$ there is a unique prime u' in $F(\hat{R}_i')$ below w' and above v . Of course $r_{u'}(\hat{R}_i') = \hat{R}_i''$. Consider the following commutative diagram.

$$\begin{array}{ccc}
 H_{f,S_l}^1(G_{K_i}; T_l) & \xrightarrow{r_{w'}} & H^1(g_{w'}; T_l) \\
 \uparrow & & \uparrow \\
 H_{f,S_l}^1(G_{F_i(\frac{1}{\pi_i}\hat{Q})}; T_l) & \xrightarrow{r_{\beta'}} & H^1(g_{\beta'}; T_l) \\
 \uparrow & & \uparrow \\
 H_{f,S_l}^1(G_{F(\hat{R}_i')}; T_l) & \xrightarrow{r_{w'}} & H^1(g_{w'}; T_l) \\
 \uparrow & & \uparrow \\
 H_{f,S_l}^1(G_F; T_l) & \xrightarrow{r_{v'}} & H^1(g_{v'}; T_l)
 \end{array} \tag{5.16}$$

Let $Fr_{w'} \in G(K_i/F)$ be an element of the conjugacy class of the Frobenius element of w' over v . Observe that

$$Fr_{w'}(\hat{R}_i') = \hat{R}_i' + \hat{P}'_0$$

for some $\hat{P}'_0 \in A_l[l]$. Note that

$$Fr_{w'}(r_{w'}(\hat{R}'_i)) = r_{w'}(\hat{R}'_i) \tag{5.17}$$

because

$$r_{w'}(\hat{R}'_i) = r_{w'}(\hat{R}'_i) = \tilde{R}'_i \in H^1(g_v; T_l).$$

On the other hand

$$Fr_{w'}(r_{w'}(\hat{R}'_i)) = r_{w'}(Fr_{w'}(\hat{R}'_i)) = r_{w'}(\hat{R}'_i + \hat{P}'_0) = r_{w'}(\hat{R}'_i) + r_{w'}(\hat{P}'_0). \tag{5.18}$$

Eqs. (5.17) and (5.18) show that $r_{w'}(\hat{P}'_0) = 0$. This by Lemma 2.13 implies that $\hat{P}'_0 = 0$. So $Fr_{w'} \in G(K_i/F(\hat{R}'_i)) \cong H_{1,i} \rtimes G_i$. Hence $Fr_{w'} = (h_1, 0, \sigma_i)$ is conjugate to $Fr_{w'} = (0, h_2, \tau_i)$ for some $h_2 \in H_{2,i}$ and $\tau_i \in G_i$. Lemma 5.2 implies that no eigenvalue of σ_i is equal to 1. This contradicts the properties of σ_i (cf. Assumption II). So we proved that equality (5.5), and consequently equality (5.4), holds. Equality (5.4) shows that $\ker \phi_P = \ker \phi_Q$, which gives the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker(\phi_Q) & \longrightarrow & G(\bar{F}/F_l) & \xrightarrow{\phi_Q} & A[l] \longrightarrow 0 \\ & & \downarrow = & & \downarrow = & & \downarrow \psi \\ 0 & \longrightarrow & \ker(\phi_P) & \longrightarrow & G(\bar{F}/F_l) & \xrightarrow{\phi_P} & A[l] \longrightarrow 0 \end{array} \tag{5.19}$$

with ψ a G_l -equivariant map. Hence due to Assumption II (1) (v) and (2) (ii) (observe that (2) (ii) implies that the centraliser of G_l in the group $GL_d(\mathbb{F}_l)$ is contained in the group of diagonal matrices $D_d \subset GL_d(\mathbb{F}_l)$), it is clear, that ψ as a linear operator is represented by a block matrix of the form

$$\begin{pmatrix} b_1 I_h & 0 & \cdots & 0 \\ 0 & b_2 I_h & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & b_e I_h \end{pmatrix}$$

for some $b_1, b_2, \dots, b_e \in \mathbb{Z}/l$. Since $\mathcal{O}_E/(l) \cong \prod_{j=1}^e \mathbb{Z}/l$, there is a $b \in \mathcal{O}_E$ such that b modulo the ideal $(l\mathcal{O}_E)$ corresponds to the element $(b_1, \dots, b_e) \in \prod_{j=1}^e \mathbb{Z}/l$ via this isomorphism. So diagram (5.19) implies that $\phi_P = b\phi_Q$, hence ϕ_{P-bQ} is a trivial map. On the other hand the natural map

$$\theta : B(F)/lB(F) \rightarrow H^1(G_{F_l}; T_l/l) = \text{Hom}(G_{F_l}; A_l[l]),$$

$$\theta(X) = \phi_X$$

(where ϕ_X is the map from Definition 4.1) is an injection since it can be expressed as a composition of the injective map from Proposition 4.3 (3) and the bottom horizontal, injective maps from diagrams: (4.5)–(4.7). Hence $P = bQ$ in $B(F)/lB(F)$. So the image of P in

$$B_0 = B(F)/\{cQ: c \in \mathcal{O}_E\}$$

is contained in the group lB_0 for all primes $l \in \mathcal{P}^*$. Since by our assumption $B(F)$ and therefore B_0 are finitely generated, we conclude that $\bigcap_{l \in \mathcal{P}^*} lB_0$ is finite. Hence $aP = bQ$ for some $a \in \mathbb{Z} - \{0\}$ and $b \in \mathcal{O}_E$. For $f = -b$ we obtain $aP + fQ = 0$. \square

6. Applications

In this section we give applications of Theorem 5.1 to the l -adic representations which were already discussed in Examples 3.3–3.7.

6.1. The cyclotomic character

Consider the cyclotomic character

$$\rho_l : G(\bar{F}/F) \rightarrow GL(\mathbb{Z}_l(1)) \cong GL_1(\mathbb{Z}_l) \cong \mathbb{Z}_l^\times$$

(see Example 3.3). There is a commutative diagram.

$$\begin{array}{ccc} \mathcal{O}_{F,S}^\times & \longrightarrow & \prod_{v \notin S_l} (k_v)_l^\times \\ \downarrow & & \downarrow \\ H_{f,S_l}^1(G_F; \mathbb{Z}_l(1)) & \longrightarrow & \prod_{v \notin S_l} H^1(g_v; \mathbb{Z}_l(1)) \end{array} \tag{6.1}$$

where the left vertical arrow factors as

$$\mathcal{O}_{F,S}^\times \rightarrow \mathcal{O}_{F,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_l \rightarrow H_{f,S_l}^1(G_F; \mathbb{Z}_l(1)).$$

This map has finite kernel with order prime to l . Diagram (6.1) and Theorem 5.1 applied to ρ_l imply the following corollary.

Corollary 6.2. *Let P, Q be two nontorsion elements of the group $\mathcal{O}_{F,S}^\times$. Assume that for almost every v and every integer m the following condition holds:*

$$mr_v(P) = 0 \text{ in } (k_v)^\times \text{ implies } mr_v(Q) = 0 \text{ in } (k_v)^\times.$$

Then there exist $a, f \in \mathbb{Z} - \{0\}$ such that $P^a = Q^f$ in $\mathcal{O}_{F,S}^\times$.

6.2. *K*-theory of number fields

Let n be a positive integer. Consider the one-dimensional representation

$$\rho_l : G_F \rightarrow GL(\mathbb{Z}_l(n+1)) \cong \mathbb{Z}_l^\times,$$

which is given by the $(n+1)$ th tensor power of the cyclotomic character. We use the notation of Example 3.4. We have the following commutative diagram:

$$\begin{CD} K_{2n+1}(F)/C_F @>>> \prod_{v \notin S_l} K_{2n+1}(k_v)_l \\ @V \psi_{F,l} VV @VV = V \\ H^1(G_F; \mathbb{Z}_l(n+1)) @>>> \prod_{v \notin S_l} H^1(g_v; \mathbb{Z}_l(n+1)) \end{CD} \tag{6.3}$$

Note that in this case

$$H^1(G_F; \mathbb{Z}_l(n+1)) \cong H^1(G_{F,S_l}; \mathbb{Z}_l(n+1)) \cong H_{f,S_l}^1(G_F; \mathbb{Z}_l(n+1))$$

and

$$K_{2n+1}(k_v)_l \cong H^1(g_v; \mathbb{Z}_l(n+1)) \cong H^0(g_v; \mathbb{Q}_l/\mathbb{Z}_l(n+1)).$$

It follows by the definition of $B(L)$ that

$$\psi_{L,l} \otimes \mathbb{Z}_l : B(L) \otimes \mathbb{Z}_l \cong H^1(G_L; \mathbb{Z}_l(n+1)).$$

Hence as a consequence of Theorem 5.1 we get the following corollary (cf. [BGK]).

Corollary 6.4. *Let P, Q be two nontorsion elements of the group $K_{2n+1}(F)$. Assume that for almost every v and every integer m the following condition holds:*

$$mr_v(P) = 0 \text{ in } K_{2n+1}(k_v) \text{ implies } mr_v(Q) = 0 \text{ in } K_{2n+1}(k_v).$$

Then the elements P and Q of $K_{2n+1}(F)$ are linearly dependent over \mathbb{Z} .

Theorem 5.1 and Corollary 6.4 have the following consequence for the reduction maps

$$r'_v : H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z}) \rightarrow H_{2n+1}(SL(k_v); \mathbb{Z})$$

defined on the integral homology of the *K*-theory spectrum $K(\mathcal{O}_F)$.

Corollary 6.5. *Let P', Q' be two nontorsion elements of the group $H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z})$. Assume that for almost every prime ideal v and for every integer m the following*

condition holds in $H_{2n+1}(SL(k_v); \mathbb{Z})$:

$$mr'_v(P') = 0 \text{ implies } mr'_v(Q') = 0.$$

Then the elements P' and Q' are linearly dependent in the group $H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z})$.

Proof. Consider the following commutative diagram:

$$\begin{CD} K_{2n+1}(\mathcal{O}_F) @>>> \prod_v K_{2n+1}(k_v) \\ @V h_F VV @VV \prod_v h_v V \\ H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z}) @>>> \prod_v H_{2n+1}(SL(k_v); \mathbb{Z}). \end{CD} \tag{6.6}$$

The horizontal maps in diagram (6.6) are induced by the reductions at prime ideals of \mathcal{O}_F . The vertical maps are the Hurewicz maps from K -theory to the integral homology of the special linear group. Since the rational Hurewicz map

$$h_F \otimes \mathbb{Q}: K_{2n+1}(\mathcal{O}_F) \otimes \mathbb{Q} \rightarrow H_{2n+1}(K(\mathcal{O}_F); \mathbb{Q})$$

is an isomorphism cf. [Bo], we can find $c, d \in \mathbb{Z}$ and nontorsion elements $P, Q \in K_{2n+1}(\mathcal{O}_F)$, such that

$$h_F(P) = cP' \quad \text{and} \quad h_F(Q) = dQ'. \tag{6.7}$$

Hence we can check that for every prime ideal v the image of the reduction map r'_v is contained in the torsion subgroup of $H_{2n+1}(SL(k_v); \mathbb{Z})$.

It follows by [A] that kernels of the Hurewicz maps h_F and h_v , for any v , are finite groups of exponents which are divisible only by primes smaller than the number $\frac{n+1}{2}$. Let \mathcal{P}^* be the set of all prime numbers l which are bigger than $\frac{n+1}{2}$ and relatively prime to $cd\#C_F$. Let $l \in \mathcal{P}^*$. Consider the following diagram obtained from (6.6).

$$\begin{CD} K_{2n+1}(\mathcal{O}_F) \otimes \mathbb{Z}_l @>>> \prod_v K_{2n+1}(k_v)_l \\ @V h_F VV @VV \prod_v h_v V \\ H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z}) \otimes \mathbb{Z}_l @>>> \prod_v H_{2n+1}(SL(k_v); \mathbb{Z})_l. \end{CD} \tag{6.8}$$

To simplify notation we keep denoting the Hurewicz maps and the reduction maps in (6.8) by the same symbols as in diagram (6.6). Let \hat{P} (\hat{Q} resp.) denote as before the image of P (Q resp.) via the map

$$K_{2n+1}(\mathcal{O}_F) \rightarrow (K_{2n+1}(\mathcal{O}_F)/C_F) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong H^1(G_F; \mathbb{Z}_l(n+1)).$$

Let S_l denote the finite set of primes of \mathcal{O}_F which are over l . Let $v \notin S_l$ and assume that $mr_v(\hat{P}) = 0$ in the group $K_{2n+1}(k_v)_l \cong H^1(g_v; \mathbb{Z}_l(n+1))$. Since $r_v(P) = r_v(\hat{P})$, it follows by diagram (6.8) that

$$0 = mh_v(r_v(P)) = mr'_v h_F(P) = cmr'_v(P')$$

in the group $H_{2n+1}(SL(k_v); \mathbb{Z})_l$. Since c is relatively prime to l , the last equality implies that

$$mr'_v(P') = 0.$$

Since $r'_v(P') \in H_{2n+1}(SL(k_v); \mathbb{Z})_{\text{tor}}$, there is a natural number m_0 which is prime to l and such that

$$m_0 mr'_v(P') = 0$$

in the group $H_{2n+1}(SL(k_v); \mathbb{Z})$. Hence, by assumption

$$m_0 mr'_v(Q') = 0$$

in the group $H_{2n+1}(SL(k_v); \mathbb{Z})$. Since m_0 is prime to l we get

$$mr'_v(Q') = 0$$

in the group $H_{2n+1}(SL(k_v); \mathbb{Z})_l$. We multiply the last equality by d . The commutativity of diagram (6.8) gives then the following equality in the group $H_{2n+1}(SL(k_v); \mathbb{Z})_l$:

$$0 = mr'_v(dQ') = mr'_v(h_F(Q)) = h_v(mr_v(Q)).$$

Since by the choice of l the map h_v in diagram (6.8) is injective, for $v \notin S_l$, from the last equality we obtain the following:

$$mr_v(\hat{Q}) = mr_v(Q) = 0.$$

Thus we have checked that the elements \hat{P} and \hat{Q} satisfy the assumption of Theorem 5.1. Hence by Theorem 5.1, there are $a, b \in \mathbb{Z}$ such that

$$aP = bQ. \tag{6.9}$$

in the group $K_{2n+1}(\mathcal{O}_F)$.

Applying h_F equality (6.9) and using (6.7) we get

$$acP' = bdQ'. \quad \square$$

6.3. Abelian varieties

Let A/F be a simple abelian variety of dimension g defined over the number field F . As usual $T_l = T_l(A)$ denotes the Tate module of A . Consider the l -adic representation

$$\rho_l : G_F \rightarrow GL(T_l(A)).$$

We follow the notation introduced in Examples 3.5–3.7. For any abelian variety A/F there is the following commutative diagram:

$$\begin{array}{ccc} A(F) & \longrightarrow & \prod_{v \notin S_l} A_v(k_v)_l \\ \psi_{F,l} \downarrow & & \downarrow \\ H_{f,S_l}^1(G_F; T_l(A)) & \longrightarrow & \prod_v H^1(g_v; T_l(A)). \end{array} \tag{6.10}$$

A_v denotes the reduction of $A \bmod v$. Observe that the right vertical arrow is an injection. Theorem 5.1, Examples 3.5–3.7, and diagram (6.10) imply the following corollary.

Corollary 6.11. *Let A be an abelian variety of dimension $g \geq 1$, defined over the number field F and such that A satisfies one of the following conditions:*

- (1) *A has the nondegenerate CM type with $\text{End}_F(A) \otimes \mathbb{Q}$ equal to a CM field E such that $E^H \subset F$ (cf. example 3.5).*
- (2) *A is a simple, principally polarized with real multiplication by a totally real field $E = \text{End}_F(A) \otimes \mathbb{Q}$ such that $E^H \subset F$, and the field F is sufficiently large.² We also assume that $\dim A = he$, where $e = [E : \mathbb{Q}]$ and h is odd (cf. example 3.6) or A is simple, principally polarised such that $\text{End}_F(A) = \mathbb{Z}$ and $\dim A$ is equal to 2 or 6 (cf. example 3.7 (b)).*

Let P, Q be two nontorsion elements of the group $A(F)$. Assume that for almost every prime v of \mathcal{O}_F and for every integer m the following condition holds in $A_v(k_v)$

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

Then there exist $a \in \mathbb{Z} - \{0\}$ and $f \in \mathcal{O}_E - \{0\}$ such that $aP + fQ = 0$ in $A(F)$.

²It means that G_l^{alg} is connected and $\tilde{\rho}_l(G_F) \subset G(l)^{\text{alg}}(\mathbb{F}_l)$ for almost all l . For details see the beginning of Section 3 of [BGK1].

Acknowledgments

We thank the ICTP in Trieste, the MPI in Bonn, the SFB 343 in Bielefeld, CRM in Barcelona, Mathematics Departments of the Ohio State University, Northwestern University and the Isaac Newton Institute in Cambridge for hospitality and financial support during our visits to the institutions, while the work on this paper continued. We thank the anonymous referee for useful remarks and suggestions which improved the exposition. The research was partially financed by a KBN grant 2 PO3A 048 22.

References

- [A] D. Arlettaz, The Hurewicz homomorphism in algebraic K -theory, *J. Pure Appl. Algebra*. 71 (1991) 1–12.
- [Ba] G. Banaszak, $\text{Mod } p$ logarithms $\log_2 3$ and $\log_3 2$ differ for infinitely many primes, *Ann. Math. Sil.* 12 (1998) 141–148.
- [BGK] G. Banaszak, W. Gajda, P. Krasoń, A support problem for K -theory of number fields, *C. R. Acad. Sci. Paris Sér. I Math.* 331 (3) (2000) 185–190.
- [BGK1] G. Banaszak, W. Gajda, P. Krasoń, On Galois representations for abelian varieties with complex and real multiplications, preprint, 2002.
- [BE] S. Bloch, E. Esnault, The coniveau filtration and non-divisibility for algebraic cycles, *Math. Ann.* 304 (1996) 303–314.
- [BK] S. Bloch, K. Kato, L -functions and Tamagawa numbers of motives, *Grothendieck Festschrift I* (1990) 333–400.
- [Bo] A. Borel, Stable real cohomology of arithmetic groups, *Ann. Sci. Ecole. Norm. Sup.* 4^{ième} Sér. 7 (1974) 235–272.
- [CF] J.W.S. Cassels, A. Fröhlich (Eds.), *Algebraic Number Theory*, Academic Press, London, New York, 1967.
- [C-RS] C. Corralez-Rodríguez, R. Schoof, Support problem and its elliptic analogue, *J. Number Theory* 64 (1997) 276–290.
- [C] W. Chi, l -adic and λ -adic representations associated to abelian varieties defined over a number field, *Amer. J. Math.* 114 (3) (1992) 315–353.
- [D1] P. Deligne, La conjecture de Weil I, *Publ. Math. IHES* 43 (1974) 273–307.
- [DF] W. Dwyer, E. Friedlander, Algebraic and étale K -theory, *Trans. Amer. Math. Soc.* 292 (1985) 247–280.
- [Har] R. Hartshorne, *Algebraic Geometry*, *GTA* 52, Springer, Berlin, 1977.
- [Ja] U. Janssen, On the l -adic cohomology of varieties over number fields and its Galois cohomology. Galois groups over \mathbb{Q} , in: *Mathematical Science Research Institute Publication*, Vol. 16, Springer, New York, Berlin, 1989.
- [La] S. Lang, *Complex Multiplication*, Springer, Berlin, 1983.
- [Mi1] J.S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, NJ, 1980.
- [Mi2] J.S. Milne, in: G. Cornell, J.H. Silverman (Eds.), *Abelian varieties*, *Arithmetic Geometry*, Springer, Berlin, 1986, pp. 103–150.
- [M] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1988.
- [R1] K.A. Ribet, Galois action on division points of abelian varieties with real multiplications, *Amer. J. Math.* 98 (3) (1976) 751–804.
- [R2] K.A. Ribet, Dividing rational points of abelian varieties of CM type, *Compositio Math.* 33 (1976) 69–74.
- [S] A. Schinzel, O pokazatelnych sravneniach, *Matematicheskie Zapiski* 2 (1996) 121–126.

- [Sc] C. Schoen, Complex varieties for which the Chow group $mod n$ is not finite, preprint, 1997.
- [Sel] J.P. Serre, Résumés des cours au Collège de France, Ann. Collège France (1985–1986) 95–100.
- [ST] J.P. Serre, J. Tate, Good reduction of abelian varieties, Ann. Math. 68 (1968) 492–517.
- [Sil] J. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer, Berlin, 1986.
- [T] J. Tate, Relation between K_2 and Galois cohomology, Invent. Math. 36 (1976) 257–274.