A SUPPORT PROBLEM FOR THE INTERMEDIATE JACOBIANS OF l-ADIC REPRESENTATIONS

G. Banaszak, W. Gajda, P. Krasoń

Abstract. We consider the support problem of Erdös 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-Rodrigáñez and Schoof concerning the support problem for higher dimensional abelian varieties. In the Appendix C of the paper we verify a special case of the Mumford-Tate conjecture for abelian varieties.

1. Introduction.

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

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

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

$$(2) \qquad x = y$$

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] and [S]. In the present paper we investigate the support problem in the context of l-adic representations

$$\rho_l \colon G_F \to Gl(T_l).$$

The precise description of the class of representations which are considered is rather technical. It is given by Assumptions I, II in section 1.3. This class of representations contains powers of the cyclotomic character, Tate modules of abelian varieties of nondegenarate CM type, and also Tate modules of some abelian varieties with real multiplications (cf. Examples 2-6 in section 1.3).

Typeset by $\mathcal{AMS}$-TEX

Consider the reduction map

$$r_v\colon H^1_{f,S_l}(G_F;\,T_l) \to H^1(g_v;\,T_l),$$

for all $v \notin S_l$, which is defined on the subgroup $H^1_{f,S_l}(G_F;\,T_l)$ of the Galois cohomology group $H^1(G_F;\,T_l)$ (see Definition A.2, Appendix A). S_l denotes here a finite set containing primes over l in F. Let $B(F)$ be a finitely generated abelian group such that for every l there is an injective homomorphism

$$\psi_{F,l}\colon B(F) \otimes \mathbb{Z}_l \to H^1_{f,S_l}(G_F;\,T_l).$$

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 $v \notin S_l$

$$m\, r_v(\hat{P}) = 0 \qquad \textit{implies} \qquad m\, r_v(\hat{Q}) = 0.$$

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

1.1. Main results.

Let $\mathcal{P}^*$ be the infinite set of prime numbers which we define precisely in section 2 of the paper. We prove the following theorem.

Theorem A. *[Th. 1, section 3]*
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 $H^1(g_v;\,T_l)$:

$$m\, r_v(\hat{P}) = 0 \qquad \textit{implies} \qquad m\, r_v(\hat{Q}) = 0.$$

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 1).

In order to prove Theorem A we investigate representations with special properties formulated in Assumption I and Assumption II of section 1.2. 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 which satisfies Assumptions I and II. We managed to extend the method of [C-RS] to the context of such l-adic representations. The hard part of the work is to control the impact of arithmetical properties of the images of these representations on the support problem. In section 4 of the paper we derive the following corollaries of Theorem A.

Theorem B. *[Cor. 1, section 4.1]*
Let P, Q be two nontorsion elements of the group $\mathcal{O}_{F,S}^{\times}$. Assume that for almost every prime v of $\mathcal{O}_F$ and every integer m the following condition holds in the group $k_v^{\times}$:

$$m\, r_v(P) = 0 \qquad \textit{implies} \qquad m\, r_v(Q) = 0,$$

where in this case

$$r_v\,:\, \mathcal{O}_{F,S}^{\times} \to k_v^{\times}$$

is the reduction map at the prime $v \notin S$. Then there exist $a, f \in \mathbb{Z} - 0$ such that $P^a = Q^f$ in $\mathcal{O}_{F,S}^{\times}$.

Note that Theorem B was already proven in [C-RS], where it is also shown that one can choose $a = 1$.

Theorem C. *[Cor. 2, section 4.2]*
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 $K_{2n+1}(k_v)$:

$$m\, r_v(P) = 0 \qquad \textit{implies} \qquad m\, r_v(Q) = 0,$$

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 C has already been proven by a different method in [BGK]. Theorem C implies the following result concerning the reduction maps

$$r_v'\colon H_{2n+1}(K(\mathcal{O}_F); \mathbb{Z}) \to H_{2n+1}(Sl(k_v); \mathbb{Z})$$

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

Theorem D. *[Cor. 3, section 4.2]*
Let n be an even, positive integer. 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 of $\mathcal{O}_F$ and for every integer m the following condition holds in the group $H_{2n+1}(Sl(k_v); \mathbb{Z})$:

$$mr_v'(P') = 0 \qquad \textit{implies} \qquad mr_v'(Q') = 0.$$

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

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

Theorem E. *[Cor. 4, section 4.3]*
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 $End_F(A) \otimes \mathbb{Q}$ equal to a CM field E (cf. example 4, section 1)*
(2) *A has real multiplication by a totally real field $E = End_F(A) \otimes \mathbb{Q}$, $dim\, A = he$, where $e = [E : \mathbb{Q}]$ and h is odd (cf. example 5, section 1) or A is an abelian variety such that $End_F(A) = \mathbb{Z}$ and $dim\, A$ is equal to 2 or 6 (cf. example 6 (b), section 1).*

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 $A_v(k_v)$

$$m\, r_v(P) = 0 \qquad \textit{implies} \qquad m\, r_v(Q) = 0.$$

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 E: abelian varieties A with $End_F(A) = \mathbb{Z}$ such that $dim\, A$ is an odd integer [Se1] (cf. example 6 (b), section 1) and abelian varieties with real multiplication by a totally real number field $E = End_F(A) \otimes \mathbb{Q}$, such that $e = g$ [R1] (cf. example 6 (a), section 1). Note that for these abelian varieties the analogues of the open image theorem of Serre have been proven [R1] and [Se1]. The proof of Theorem E relies on the analysis of the image of the corresponding Galois representation. The information concerning the image of Galois representations on l torsion points of abelian varieties in (1) and (2) of Theorem E is contained in Theorem B1 of Appendix B and Theorem C5 of Appendix C. We would like to mention that Theorem E given above provides an answer to the question of Corrales-Rodrigáñez and Schoof about the support problem for higher dimensional abelian varieties [C-RS], p. 227, where the support problem for an elliptic curve was considered. It is known that for some families of abelian varieties of Theorem E the Mumford-Tate group over $\mathbb{Q}_l$ is equal to the identity component of the Zariski closure of the image of the Galois representation on $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$ i.e., the Mumford-Tate conjecture holds. For the CM abelian varieties of Theorem E (1) the Mumford-Tate conjecture follows by the results of Pohlman cf. [Se5]. Important special cases of the Mumford-Tate conjecture have been proven by J.P. Serre [Se1], W. Chi [C], K. Ribet [R1], R. Pink [P] and S. Tankeev [Ta2]. In Theorem C6, Appendix C we verify that the Mumford-Tate conjecture is true for some new abelian varieties belonging to the first class of varieties listed in part (2) of Theorem E.

Organization of the paper: In section 1 we introduce necessary notation and definition of the class of representations which are considered. The proof of Theorem A is contained in sections 2 and 3. In order to keep the exposition self-contained we attached three appendices at the end of the paper. In Appendix A we discuss

l-adic intermediate jacobians which were defined in a different context by C. Schoen in [Sch]. Appendix B contains a brief exposition of abelian varieties of the non-degenerate CM type following [R3], [K] and [Haz]. In the Appendix C we discuss the image of the Galois representation for abelian varieties with real multiplications for which the support problem has positive answer. The reader is advised to use the appendices as the source of explanations for the undefined symbols in the main body of the paper. In section 4 of the paper we collected the corollaries of Theorem A.

Acknowledgements: We thank K. Ribet for correspondence concerning the Galois representaton associated with CM abelian varieties. We also thank J.P. Serre, S.G. Tankeev and J.P. Wintenberger for conversations and correspondence concerning the case of the Galois representation of abelian varieties with real multiplications. The ICTP in Trieste, the MPI in Bonn, the SFB 343 in Bielefeld, CRM in Barcelona, Mathematics Departments of the Ohio State University and Northwestern University provided financial support during our visits to the institutions, while the work on this paper continued. The research was partially financed by a KBN grant.

1.2. 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 $\mathcal{O}_F$

F_v is the completion of F at v and k_v denotes the residue field $\mathcal{O}_F/v$

$G_v = G(\overline{F}_v/F_v)$

I_v is the inertia subgroup of G_v

$g_v = G(\overline{k}_v/k_v)$

T_l denotes a free $\mathbb{Z}_l$-module of finite rank d.

$V_l = T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$

$A_l = V_l/T_l$

$\rho_l :$ $G_F \to Gl(T_l)$ is a representation unramified outside a fixed finite set S_l of primes of $\mathcal{O}_F$, containing all primes over l.

$\overline{\rho_l}$ denotes the residual representation $G_F \to Gl(T_l/l)$ induced by ρ_l.

$F_l = F(A_l[l])$ denotes the number field $\bar{F}^{ker \overline{\rho_l}}$.

$G_l = G(F_l/F)$; observe that $G_l \cong \overline{\rho_l}(G_F)$ 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.

1.3. Basic Assumptions.

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 1. 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 $\overline{X} = X \otimes_F \overline{F}$ and $\overline{\mathcal{X}}_v = \mathcal{X}_v \otimes_{k_v} \overline{k}_v$. In the case when $H^i_{et}(\overline{X}; \mathbb{Z}_l(j))$ is torsion free for some i, j such that $i \neq 2j$ we put

$$T_l = H^i_{et}(\overline{X}; \mathbb{Z}_l(j)).$$

By the theorem of proper and smooth base change ([Mi1] VI, Cor. 4.2) there is a natural isomorphism of G_v-modules

$$H^i_{et}(\overline{X}; \mathbb{Z}_l(j)) \cong H^i_{et}(\overline{\mathcal{X}}_v; \mathbb{Z}_l(j)). \tag{1.1}$$

(cf. [Ja] p. 322). Since the inertia subgroup $I_v \subset G_v$ acts trivially on $H^i_{et}(\overline{\mathcal{X}}_v; \mathbb{Z}_l(j))$, we observe by (1.1) that the representation $\rho_l \colon G_F \to Gl(T_l)$ is unramified outside S_l. It follows by the theorem of Deligne [D1] (proof of the Weil conjectures, see also [Har] Appendix C, Th. 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

$$V_l = H^i_{et}(\overline{X}; \mathbb{Q}_l(j))$$

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

$$T_l = H^i_{et}(\overline{A}; \mathbb{Z}_l(j)) \cong \wedge^i H^1_{et}(\overline{A}; \mathbb{Z}_l)(j) \cong \wedge^i Hom_{\mathbb{Z}_l}(T_l(A); \mathbb{Z}_l)(j),$$

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

$$\rho_l \colon G_F \to Gl(T_l(A))$$

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

In order to formulate the second basic assumption on the representation ρ let us introduce some 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 splits completely in F. Let

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

be the decomposition of the ideal (l) in $\mathcal{O}_E$. The ring $\mathcal{O}_E$ 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 $\mathcal{O}_{\lambda_i}$ the ring of integers in E_{λ_i}. Now, it is obvious that

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

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

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

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

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

$$A_l[l] \;\cong\; \bigoplus_{i=1}^{e} A_l[\lambda_i], \tag{1.2}$$

where $dim_{\mathbb{Z}/l}\, A_l[\lambda_i] = h$, for all $1 \leq i \leq e$. By assumptions and decomposition (1.2) 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

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

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 $H_i \subset Gl_h(\mathbb{Z}/l) \cong Gl(A_l[\lambda_i])$ 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 $Im\, \overline{\rho_l} = G_l$ 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 σ_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 centralizer 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 $\sigma\, h = h\, \sigma$ for all $h \in H_i$, then σ is a scalar matrix.

(2) If $h > 1$, then 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.

(3) If $h = 1$, we require that $G_l = G(F_l/F)$ satisfies two additional conditions:

(i) for every $1 \leq i \leq d$, there is a diagonal matrix $\sigma_i = diag\,(\mu_1, \ldots, \mu_d)$ 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 $G_l \to (\mathcal{O}_E/l)^{\times}$.

Definition 1. 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 $L \to L'$ the structure map $B(L) \to B(L')$ is a homomorphism of $\mathcal{O}_E$-modules. Let us put $B(\overline{F}) = \varinjlim_{L/F} B(L)$. 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 representation ρ (or more precisely, of the pair $(\rho,\, \mathcal{P})$) if the following conditions are satisfied:

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

$$\psi_{L,l}\, :\, B(L) \longrightarrow H^1_{f,S_l}(G_L; T_l)$$

(for the definition of $H^1_{f,S_l}(G_L; T_l)$ see Appendix A), where L is as above and $l \in \mathcal{P}$, is such that either

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

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

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 $B(\overline{F})$ is a discrete G_F-module which is divisible by l and for every L we have: $B(\overline{F})^{G_L} \cong B(L)$ and $H^0(G_L; A_l) \subset B(L)$.

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 2. Consider the l-adic representation

$$\rho_l \ : \ G(\bar{F}/F) \to Gl(\mathbb{Z}_l(1)) \cong Gl_1(\mathbb{Z}_l) \cong \mathbb{Z}_l^{\times}$$

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)

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

factors naturally through

$$\psi_{L,l} \ : \ B(L) \otimes \mathbb{Z}_l \to H^1_{f,S_l}(G_F; \mathbb{Z}_l(1))$$

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. 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

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

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]

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

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

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

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

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

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 take $T_l = T_l(A)$ the Tate module of A. Consider the l-adic representation

$$\rho_l \;:\; G_F \to Gl(T_l(A)).$$

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], Th. 1, p. 493 and Corollaries 1 and 2 of Manin's Appendix II to the book [M]) we have a natural imbedding

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

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

Example 4. 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. Appendix B Def. B1) and defined over F . Condition (i) of Assumption II (3) holds by Theorem B1 of Appendix B (for CM elliptic curves it also follows by an alternative argument cf. [C-RS], Lemma 5.1, p. 286). Condition (ii) of Assumption II (3) 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 a good reduction at l.

Example 5. Consider a simple abelian variety A/F such that $E = End_F(A) \otimes \mathbb{Q} = End_{\bar{F}}(A) \otimes \mathbb{Q}$ (cf. [R1] and [C]) where $e = [E : \mathbb{Q}]$ and $2h\,e = 2g$ with h and odd integer. In addition, we choose F to be a number field satisfying conditions indicated in a discussion which follows Theorem C1 of Appendix C and such that $E^H \subset F$. We take $\mathcal{P}$ to be the set of prime numbers $l \gg 0$ which split completely in F, abelian variety A has a good reduction at l and fulfills all the assumptions of Appendix C. Hence by Theorem C5 of Appendix C 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 $GSp_{2h}(\mathbb{F}_l)/Sp_{2h}(\mathbb{F}_l)$ 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 center is a simple group.

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

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

has eigenvalue 1 with the eigenspace of dimension 1 where

$$J_h(1) = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

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 centralizer of $Sp_{2h}(\mathbb{F}_l)$ in $Gl_{2h}(\mathbb{F}_l)$ is $(\mathbb{F}_l)^{\times} I_{2h}$.

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

There are two special cases of Example 5 that have been considered extensively in the past.

Example 6. (a) Let A/F be a simple 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, [R1] or Theorem C5 of Appendix C 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) and (2).

(b) Let A/F be a simple 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] Th. 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 the conditions (1) and (2) of Assumption II.

It is rather hard to find further examples of Mordell-Weil $\mathcal{O}_E$-modules satifying condition (2)(i) of Definition 1. 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.

2. Key Propositions.

Definition 2. *Let*

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

be the map:

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

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

$$B(F) \to B(F) \otimes \mathbb{Z}_l \to H^1_{f,S_l}(G_F; T_l) \subset J_{f,S_l}(T_l)$$

Remark 1. 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 A1 (see Appendix A). The element $\frac{1}{l}\hat{P}$ is defined up to an element of the group $A_l[l]$.

Proposition 1. *Suppose that the Assumptions I and II are fulfilled. Then we have:*

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 $H^1_{f,S_l}(G_F; T_l)/l \longrightarrow H^1_{f,S_l}(G_{F_l}; T_l)/l$ is injective for all $l \in \mathcal{P}$,*
3. *the map $B(F)/lB(F) \longrightarrow B(F_l)/lB(F_l)$ is injective for all $l \in \mathcal{P}$,*
4. *Let $P \in B(F)$. If $l \in \mathcal{P}$ does not divide $\sharp\, B(F)_{tor}$ 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 $D^0 = \prod_{j=1}^{e} D_i^0$ can be regarded as a subgroup of G_l once we identify G_l with its image via $\overline{\rho_l}$. D^0 is a normal subgroup of G_l. Assumption II (2) allows us to consider the Hochschild-Serre spectral sequence

$$E_2^{r,s} = H^r(G_l/D^0;\, H^s(D^0;\, A_l[l])) \Rightarrow H^{r+s}(G_l;\, A_l[l]). \tag{2.1}$$

Observe that $H^0(D^0;\, A_l[l]) = \oplus_{i=1}^{e} H^0(D_i^0;\, A_l[\lambda_i]) = 0$ 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 (3) (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 Prop. A1, Appendix A, we have the following short exact sequence:

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

By the long exact sequence in cohomology associated to this exact sequence and Proposition A2, we obtain the commutative diagram in which the horizontal maps are injections.

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ ker\,\alpha & \longrightarrow & H^1(G_l;\, A_l[l]) \\ \downarrow & & \downarrow \\ H^1_{f,S_l}(G_F;\, T_l)/l & \longrightarrow & H^1(G_F;\, A_l[l]) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \gamma} \\ H^1_{f,S_l}(G_{F_l};\, T_l)/l & \longrightarrow & H^1(G_{F_l};\, A_l[l]) \end{array} \tag{2.2}$$

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 the case (2) (i) of Definition 1. Because the map

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

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

$$\begin{array}{ccc} B(F)/l & \longrightarrow & H^1_{f,S_l}(G_F;\, T_l)/l \\ \downarrow & & \downarrow{\scriptstyle \alpha} \\ B(F_l)/l & \longrightarrow & H^1_{f,S_l}(G_{F_l};\, T_l)/l \end{array} \tag{2.3}$$

are isomorphisms. Since we have proved in (2) that the map α is an injection, diagram (2.3) gives the claim (3). Now consider the case (2) (ii) of Definition 1. We get the exact sequence of G_F-modules:

$$0 \longrightarrow A_l[l] \longrightarrow B(\overline{F}) \xrightarrow{l} B(\overline{F}) \longrightarrow 0$$

This gives the following commutative diagram with injective horizontal arrows:

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ ker\,\beta & \longrightarrow & H^1(G_l;\,A_l[l]) \\ \downarrow & & \downarrow \\ B(F)/l & \longrightarrow & H^1(G_F;\,A_l[l]) \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ B(F_l)/l & \longrightarrow & H^1(G_{F_l};\,A_l[l]) \end{array} \tag{2.4}$$

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 of $A_l[l]$ (1.2) and Assumption II (1) and (3) (ii) that every G_F submodule of $A_l[l]$ is of the form $A_l[\lambda_{i_1}]\oplus\cdots\oplus A_l[\lambda_{i_r}]$ for some $i_1,\ldots,i_r \in \{1,\ldots,e\}$. Hence if $Im\,\phi_P$ were a proper G_F submodule, we could assume that

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

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

$$\pi_1\ldots\pi_{i-1}\pi_{i+1}\ldots\pi_e(\sigma(\frac{1}{l}\hat{P}) - \frac{1}{l}\hat{P}) = 0 \tag{2.5}$$

for every $\sigma \in G(\bar{F}/F_l)$. The equality (2.5) takes place in $J_{f,S_l}(T_l)$ under the (2) (i) part of Definition 1 (resp. in $B(\overline{F})$ under the case (2) (ii) of Definition 1) and it implies that

$$\sigma(\pi_1\ldots\pi_{i-1}\pi_{i+1}\ldots\pi_e\frac{1}{l}\hat{P}) = \pi_1\ldots\pi_{i-1}\pi_{i+1}\ldots\pi_e\frac{1}{l}\hat{P} \tag{2.6}$$

for every $\sigma \in G(\bar{F}/F_l)$. Hence by Proposition A2 (2) (resp. by Def. 1, sec. 1.3, of the Mordell-Weil $\mathcal{O}_E$-module $\{B(L)\}$) we get

$$\pi_1\ldots\pi_{i-1}\pi_{i+1}\ldots\pi_e\frac{1}{l}\hat{P} \in H^1_{f,S_l}(G_{F_l};T_l) \quad (\in B(F_l)\ resp.). \tag{2.7}$$

So $\pi_1 \ldots \pi_{i-1}\pi_{i+1} \ldots \pi_e \hat{P} = 0$ in the group $H^1_{f,S_l}(G_{F_l};T_l)/l$ (in the group $B(F_l)/lB(F_l)$ resp.). By parts (2) and (3) of the Proposition (see also the diagram (2.3)) this implies $\pi_1 \ldots \pi_{i-1}\pi_{i+1} \ldots \pi_e \hat{P} = 0$ in the group $B(F)/lB(F)$ in both cases. Hence there is $P_1 \in B(F)$ such that $\pi_1 \ldots \pi_{i-1}\pi_{i+1} \ldots \pi_e \hat{P} = lP_1$. This gives the equality

$$\pi_1 \ldots \pi_{i-1}\pi_{i+1} \ldots \pi_e(\hat{P} - \pi_i P_2) = 0 \tag{2.8}$$

where $P_2 = uP_1 \in B(F)$ for some $u \in \mathcal{O}_E^{\times}$. Multiplying equation (2.8) by π_i we obtain the equality $l(P - \pi_i P_2) = 0$ in the group $B(F)$. Since, by assumption, $\sharp\, B(F)_l = 0$ 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:

$$\bar{\rho}_i : G_{F_i} \to Gl(A_l[\lambda_i])$$

Similarly to the definition of F_l we put $F_i = \bar{F}^{ker\,\bar{\rho}_i}$. In analogy with the definition 2 we introduce a homomorphism

$$\phi_i : G_{F_i} \to A_l[\lambda_i],$$

$$\phi_i(\sigma) = \sigma(\frac{1}{\pi_i}\hat{P}) - \frac{1}{\pi_i}\hat{P}.$$

Proposition 2. *We have:*

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* $H^1_{f,S_l}(G_F;T_l)/\lambda_i \longrightarrow H^1_{f,S_l}(G_{F_i};T_l)/\lambda_i$ *is injective for all* $l \in \mathcal{P}$ *and* $1 \leq i \leq e$.
3. *the map* $B(F)/\lambda_i B(F) \longrightarrow B(F_i)/\lambda_i B(F_i)$ *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* $\sharp\, B(F)_{tor}$ *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 1. 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

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

denote the reduction map at a prime ideal v of $\mathcal{O}_F$ (see Appendix A). 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 1 below).

We need some additional notations. 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 A1 of the Appendix. The Galois group G_{F_l} acts on the set

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

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

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

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

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

where

$$H_1 = Gal(F_l(\frac{1}{l}\hat{Q})/F_l) \qquad\qquad H_2 = Gal(F_l(\frac{1}{l}\hat{P})/F_l).$$

By Proposition 1 (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.

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
F_l(\frac{1}{l}\hat{P}) \arrow[d, dash] \arrow[dr, dash] & & F_l(\frac{1}{l}\hat{Q}) \arrow[dl, dash] \arrow[d, dash] \\
F(\hat{R}) \arrow[dr, dash] & F_l \arrow[d, dash] & F(\hat{R}') \arrow[dl, dash] \\
 & F &
\end{tikzcd} \tag{2.9}$$

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 A1. The Galois group G_{F_i} acts on the set

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

which is contained in $J_{f,S_l}(T_l)$. 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

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

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

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

where

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

By Proposition 2 (4) the group $H_{1,i}$ ($H_{2,i}$, respectively) 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 1 below.

(2.10)

$$\begin{tikzcd}
 & K_i \arrow[dl, dash] \arrow[dr, dash] & \\
F_i(\frac{1}{\pi_i}\hat{P}) \arrow[d, dash] \arrow[dr, dash] & & F_i(\frac{1}{\pi_i}\hat{Q}) \arrow[dl, dash] \arrow[d, dash] \\
F(\hat{R}_i) \arrow[dr, dash] & F_i \arrow[d, dash] & F(\hat{R}'_i) \arrow[dl, dash] \\
 & F &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & w \arrow[dl, dash] & w' \arrow[dr, dash] & \\
\beta \arrow[d, dash] \arrow[dr, dash, shorten >=0.3em] & & & \beta' \arrow[dll, dash] \arrow[d, dash] \\
u \arrow[dr, dash] & \cdot \arrow[d, dash] & & u' \arrow[dll, dash] \\
 & v & &
\end{tikzcd}$$

Remark 2. Observe that

$$F_l(\frac{1}{l}\hat{P}) = F_1(\frac{1}{\pi_1}\hat{P}) \ldots F_i(\frac{1}{\pi_i}\hat{P}) \ldots F_e(\frac{1}{\pi_e}\hat{P}),$$
$$F_l(\frac{1}{l}\hat{Q}) = F_1(\frac{1}{\pi_1}\hat{Q}) \ldots F_i(\frac{1}{\pi_i}\hat{Q}) \ldots F_e(\frac{1}{\pi_e}\hat{Q}).$$

In addition there is an equality

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

since by Proposition 2 (4) there are $[F_i(\frac{1}{\pi_i}\hat{P}) : F_i]$ different imbeddings of $F(\hat{R}_i)$ into $\bar{F}$ that fix F. Hence from diagram (2.10) we find out that $F(\hat{R}_i) \cap F_i = F$.

3. The support problem for l-adic representations.

Theorem 1. *Let $\mathcal{P}^*$ be the infinite set of prime numbers introduced in section 2. 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 $v \notin S_l$

$$m\, r_v(\hat{P}) = 0 \qquad \textit{implies} \qquad m\, r_v(\hat{Q}) = 0.$$

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

Lemma 1. *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 $G_i = Im\, \bar{\rho}_i \subset Gl_h(\mathbb{F}_l)$. 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 $h_1 \in H_{1,i}$ the element $(h_1, 0, \sigma_i) \in (H_{1,i} \oplus \{0\}) \rtimes G_i$ 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. $\square$

Remark 3. Observe, that by Assumption II there exists a matrix $\sigma_i \in G_i$, such that 1 is an eigenvalue of σ_i with an eigenspace of dimension 1, for every $l \in \mathcal{P}$ and every $1 \leq i \leq e$.

Proof of Theorem 1. We want to prove that

$$F_l(\frac{1}{l}\hat{P}) = F_l(\frac{1}{l}\hat{Q}). \tag{3.1}$$

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

$$F_i(\frac{1}{\pi_i}\hat{P}) = F_i(\frac{1}{\pi_i}\hat{Q}). \tag{3.2}$$

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

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

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

$$Gal(K_i/F_i) \cong H_{1,i} \oplus H_{2,i} \cong A_l[\lambda_i] \oplus A_l[\lambda_i]. \tag{3.3}$$

We need the following:

Lemma 2. *We have the following equality*

$$K_i \cap F_l = F_i.$$

Proof. By (3.3) 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 $K_i \cap F_l = F_i$.
Let $h > 1$. 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 (i), (ii) 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 $G(F_l/F_i)^{ab} = G(F_l/F_i)/[G(F_l/F_i), G(F_l/F_i)]$ 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 $G(F_l/F_i)^{ab}$, 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 1. Consider the following tower of fields.

$$\begin{tikzcd}
 & K_iF_l \arrow[dl, dash] \arrow[d, dash] & \\
K_i \arrow[d, dash] & F_l \arrow[dl, dash] \arrow[dr, dash] & \\
F_i \arrow[dr, dash] & & F_1 \dots F_{i-1}F_{i+1} \dots F_e \arrow[dl, dash] \\
 & F &
\end{tikzcd} \tag{3.4}$$

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 2, Remark 2 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 1.

By the choice of prime v we see that

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

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 finitness of $H^0(g_v;\, A_l)$, shows that there is an m such that

$$H^0(g_v;\, A_l) = H^0(g_v;\, A_l)[l^m] = H^0(g_v;\, A_l)[\pi_i^m] \tag{3.5}$$

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 (2.10). Consider the following commutative diagram.

$$\begin{tikzcd}
H^1_{f,S_l}(G_{K_i};\, T_l) \arrow[r, "r_w"] & H^1(g_w;\, T_l) \\
H^1_{f,S_l}(G_{F_i(\frac{1}{\pi_i}\hat{P})};\, T_l) \arrow[r, "r_\beta"] \arrow[u] & H^1(g_\beta;\, T_l) \arrow[u] \\
H^1_{f,S_l}(G_{F(\hat{R}_i)};\, T_l) \arrow[r, "r_u"] \arrow[u] & H^1(g_u;\, T_l) \arrow[u] \\
H^1_{f,S_l}(G_F;\, T_l) \arrow[r, "r_v"] \arrow[u] & H^1(g_v;\, T_l) \arrow[u, "\cong"']
\end{tikzcd} \tag{3.6}$$

The lowest right vertical arrow in the diagram (3.6) 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 A2. 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

$$\frac{t_v}{l}\, r_v(\hat{P}) = \frac{t_v}{l}\pi_i\, r_u(\hat{R}_i) = l^{m-1}\pi_i\, r_u(\hat{R}_i) = c\prod_{j\neq i}\pi_j^{m-1}(\pi_i^m\, r_u(\hat{R}_i)) = 0 \tag{3.7}$$

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 (3.5).
By the assumption of Theorem 1, equality (3.7) implies that

$$\frac{t_v}{l} r_v(\hat{Q}) = 0. \tag{3.8}$$

Since $H^1(g_v;\, T_l)$ is cyclic, the equality (3.8) implies that

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

This gives

$$r_v(\hat{Q}) = \pi_i\, \tilde{R}_i''. \tag{3.9}$$

for some $\tilde{R}_i'' \in H^1(g_v;\, T_l)$. By Proposition A1 we can find an element $\hat{R}_i'' \in J_{f,S_l}(T_l)$ such that

$$\pi_i\, \hat{R}_i'' = \hat{Q}. \tag{3.10}$$

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 3.6 with $\hat{P}$ and $\hat{R}_i$ replaced by $\hat{Q}$ and $\hat{R}_i''$ we obtain by (3.10) that

$$r_v(\hat{Q}) = \pi_i\, r_{u''}(\hat{R}_i''). \tag{3.11}$$

in the group $H^1(g_{u''};\, T_l)$, hence also in $H^1(g_{w'};\, T_l)$. By (3.9) and (3.11) we get

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

Because $A_l[\pi_i] \subset H^1_{f,S_l}(G_{K_i};\, T_l)$ (cf. proof of Lemma A2 and diagram (A.2)), by Lemma A3 there exists $\hat{P}_0 \in H^1_{f,S_l}(G_{K_i};\, T_l)$ such that $r_{w'}(\hat{P}_0) = r_{u''}(\hat{R}_i'') - \tilde{R}_i''$. We have the following equality

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

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 $r_{u'}(\hat{R}'_i) = \tilde{R}''_i$. Consider the following commutative diagram.

$$
\begin{array}{ccc}
H^1_{f,S_l}(G_{K_i}; T_l) & \xrightarrow{r_{w'}} & H^1(g_{w'}; T_l) \\
\uparrow & & \uparrow \\
H^1_{f,S_l}(G_{F_i(\frac{1}{\pi_i}\hat{Q})}; T_l) & \xrightarrow{r_{\beta'}} & H^1(g_{\beta'}; T_l) \\
\uparrow & & \uparrow \\
H^1_{f,S_l}(G_{F(\hat{R}'_i)}; T_l) & \xrightarrow{r_{u'}} & H^1(g_{u'}; T_l) \\
\uparrow & & {\scriptstyle =}\uparrow \\
H^1_{f,S_l}(G_F; T_l) & \xrightarrow{r_{v'}} & H^1(g_{v'}; T_l)
\end{array}
\tag{3.12}
$$

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

$$Fr_{w'}(r_{w'}(\hat{R}'_i)) = r_{w'}(\hat{R}'_i) \tag{3.13}$$

because

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

On the other hand

$$Fr_{w'}(r_{w'}(\hat{R}'_i)) = r_{w'}(Fr_{w'}(\hat{R}'_i)) = r_{w'}(\hat{R}'_i + \hat{P}'_0) = r_{w'}(\hat{R}'_i) + r_{w'}(\hat{P}'_0). \tag{3.14}$$

Equations (3.13) and (3.14) show that $r_{w'}(\hat{P}'_0) = 0$. This by lemma A3 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 1 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 the equality (3.2), and consequently the equality (3.1), holds. Equality (3.1) shows that $ker\, \phi_P = ker\, \phi_Q$, which gives the following commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & ker(\phi_Q) & \longrightarrow & G(\bar{F}/F_l) & \xrightarrow{\phi_Q} & A[l] & \longrightarrow & 0 \\
 & & {\scriptstyle =}\downarrow & & {\scriptstyle =}\downarrow & & {\scriptstyle \psi}\downarrow & & \\
0 & \longrightarrow & ker(\phi_P) & \longrightarrow & G(\bar{F}/F_l) & \xrightarrow{\phi_P} & A[l] & \longrightarrow & 0
\end{array}
\tag{3.15}
$$

with ψ a G_l-equivariant map. Hence due to Assumption II (1) (v) and (3) (ii) (observe that (3) (ii) implies that the centralizer 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

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

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 (3.15) implies that $\phi_P = b\,\phi_Q$, hence ϕ_{P-bQ} is a trivial map. On the other hand the natural map

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

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

(where ϕ_X is the map from Def. 2, sec. 2) is an injection since it can be expressed as a composition of the injective map from Proposition 1 (3) and the bottom horizontal, injective maps from diagrams (2.2), (2.3) and (2.4). 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 $aP + fQ = 0$. $\square$

4. Examples. In this section we give applications of Theorem 1 to the l-adic representations which were already discussed in Examples 2 - 6 in Section 1.

4.1 The cyclotomic character.
Consider the cyclotomic character

$$\rho_l \;:\; G(\bar{F}/F) \to Gl(\mathbb{Z}_l(1)) \cong Gl_1(\mathbb{Z}_l) \cong \mathbb{Z}_l^{\times},$$

(see Example 2, Sect. 1). There is a commutative diagram.

$$\begin{array}{ccc} \mathcal{O}_{F,S}^{\times} & \longrightarrow & \prod_{v \notin S_l} (k_v)_l^{\times} \\ \downarrow & & =\downarrow \\ H^1_{f,S_l}(G_F;\, \mathbb{Z}_l(1)) & \longrightarrow & \prod_{v \notin S_l} H^1(g_v;\, \mathbb{Z}_l(1)) \end{array} \tag{4.1}$$

where the left vertical arrow factors as:

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

This map has finite kernel with order prime to l. Diagram (4.1) and Theorem 1 applied to ρ_l imply the following corollary.

Corollary 1. *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*

$$m\, r_v(P) = 0 \quad in \quad (k_v)^{\times} \qquad implies \qquad m\, r_v(Q) = 0 \quad in \quad (k_v)^{\times}.$$

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

4.2 K-theory of number fields.

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

$$\rho_l \;:\; G_F \to Gl(\mathbb{Z}_l(n+1)) \cong \mathbb{Z}_l^{\times}$$

which is given by the $(n+1)$-th tensor power of the cyclotomic character. We use the notation of Example 3, Sec. 1. We have the following commutative diagram.

$$\begin{array}{ccc} K_{2n+1}(F)/C_F & \longrightarrow & \prod_{v \notin S_l} K_{2n+1}(k_v)_l \\ \big\downarrow \psi_{J,l} & & = \big\downarrow \\ H^1(G_F;\, \mathbb{Z}_l(n+1)) & \longrightarrow & \prod_{v \notin S_l} H^1(g_v;\, \mathbb{Z}_l(n+1)) \end{array} \tag{4.2}$$

Note that in this case

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

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

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

Hence as a consequence of Theorem 1 we get the following corollary (cf. [BGK]):

Corollary 2. *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*

$$m\, r_v(P) = 0 \quad in \quad K_{2n+1}(k_v) \qquad implies \qquad m\, r_v(Q) = 0 \quad in \quad K_{2n+1}(k_v).$$

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

Theorem 1 and Corollary 2 have the following consequence for the reduction maps

$$r'_v \colon H_{2n+1}(K(\mathcal{O}_F);\, \mathbb{Z}) \to H_{2n+1}(Sl(k_v);\, \mathbb{Z})$$

on the integral homology of the special linear group.

Corollary 3. *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 $H_{2n+1}(Sl(k_v);\, \mathbb{Z})$:*

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

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.

$$\begin{array}{ccc} K_{2n+1}(\mathcal{O}_F) & \longrightarrow & \prod_v K_{2n+1}(k_v) \\ {\scriptstyle h_F}\big\downarrow & & {\scriptstyle \prod_v h_v}\big\downarrow \\ H_{2n+1}(K(\mathcal{O}_F);\, \mathbb{Z}) & \longrightarrow & \prod_v H_{2n+1}(Sl(k_v);\, \mathbb{Z}). \end{array} \tag{4.3}$$

The horizontal maps in the diagram (4.3) 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

$$h_F \otimes \mathbb{Q}\colon \quad K_{2n+1}(\mathcal{O}_F) \otimes Q \to H_{2n+1}(K(\mathcal{O}_F);\, \mathbb{Q})$$

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

$$h_F(P) = cP' \qquad \text{and} \qquad h_F(Q) = dQ'. \tag{4.4}$$

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 $cd\sharp C_F$. Let $l \in \mathcal{P}^*$. Consider the following diagram obtained from (4.3).

$$\begin{array}{ccc} K_{2n+1}(\mathcal{O}_F) \otimes \mathbb{Z}_l & \longrightarrow & \prod_v K_{2n+1}(k_v)_l \\ {\scriptstyle h_F}\big\downarrow & & {\scriptstyle \prod_v h_v}\big\downarrow \\ H_{2n+1}(K(\mathcal{O}_F);\, \mathbb{Z}) \otimes \mathbb{Z}_l & \longrightarrow & \prod_v H_{2n+1}(Sl(k_v);\, \mathbb{Z})_l. \end{array} \tag{4.5}$$

To simplify notation we keep denoting the Hurewicz maps and the reduction maps in (4.5) by the same symbols as in the diagram (4.3). Let $\hat{P}$ ($\hat{Q}$ resp.) denote as before the image of P (Q resp.) via the map

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

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 the diagram (4.5) that

$$0 = mh_v(r_v(P)) = mr'_v h_F(P)) = c\, mr'_v(P')$$

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 $r'_v(P') \in H_{2n+1}(Sl(k_v); \mathbb{Z})_{tor}$, 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 (4.5) 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 the diagram (4.5) 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 1. Hence by Theorem 1, there are a, $b \in \mathbb{Z}$ such that

$$aP = bQ. \tag{4.6}$$

in the group $K_{2n+1}(\mathcal{O}_F)$.
Applying h_F to equality (4.6) and using (4.4) we get

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

4.3 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

$$\rho_l \;:\; G_F \to Gl(T_l(A)).$$

In this subsection we follow the notation introduced in Examples 4 - 6 of Section 1.3. For any abelian variety A/F there is the following commutative diagram

$$\begin{array}{ccc} A(F) & \longrightarrow & \prod_{v \notin S_l} A_v(k_v)_l \\ {\scriptstyle \psi_{L,l}}\downarrow & & \downarrow \\ H^1_{f,S_l}(G_F;\, T_l(A)) & \longrightarrow & \prod_v H^1(g_v;\, T_l(A)). \end{array} \tag{4.7}$$

A_v denotes the reduction of A mod v. Observe that the right vertical arrow is an injection. Theorem 1, Examples 4, 5 and 6 of Section 1.3, and the diagram (4.7) imply the following corollary.

Corollary 4.

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 $End_F(A) \otimes \mathbb{Q}$ equal to a CM field E (cf. example 4, section 1)*

(2) *A has real multiplication by a totally real field $E = End_F(A) \otimes \mathbb{Q}$ and $dim\, A = he$, where $e = [E : \mathbb{Q}]$ and h is odd (cf. example 5, section 1) or A is an abelian variety such that $End_F(A) = \mathbb{Z}$ and $dim\, A$ is equal to 2 or 6 (cf. example 6 (b), section 1).*

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 $A_v(k_v)$

$$m\, r_v(P) = 0 \qquad implies \qquad m\, r_v(Q) = 0.$$

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

Appendix A. l-adic Intermediate Jacobians.

Definition A1. *Define*

$$H^1_f(G_F;T_l), \quad (\,resp.\ H^1_f(G_F;V_l)\,)$$

to be the kernel of the natural map:

$$H^1(G_F;T_l)\to\prod_v H^1(G_v;T_l)/H^1_f(G_v;T_l)$$

$$(\,resp.\ H^1(G_F;V_l)\to\prod_v H^1(G_v;V_l)/H^1_f(G_v;V_l)\,)$$

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

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

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

$$H^1_f(G_v;V_l)=\begin{cases} Ker\,(\,H^1(G_v;V_l)\to H^1(I_v;V_l)\,) & \text{if } v\nmid l\\ \\ Ker\,(\,H^1(G_v;V_l)\to H^1(G_v;V_l\otimes_{\mathbb{Q}_l}B_{crys})\,) & \text{if } v\mid l\,,\end{cases}$$

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

We have the natural maps

$$H^1_f(G_F;T_l)\to\prod_v H^1_f(G_v;T_l),$$

$$H^1_f(G_F;V_l)\to\prod_v H^1_f(G_v;V_l).$$

Definition A2. *We also define*

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

as the kernel of the natural map:

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

$$(\,resp.\ H^1(G_F;V_l)\to\prod_{v\notin S_l} H^1(G_v;T_l)/H^1_f(G_v;V_l)\,).$$

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

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

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

Definition A3. *We put*

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

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

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

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 A1. 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 A2. 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
$$H^1(G_{F,\Sigma}; T_l) = H^1(G_F; T_l).$$

Lemma A1. *For every prime w of $\mathcal{O}_L$ which is not over primes in S_l, we have:*

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

Proof. First part of the lemma is obvious from the definition of $H^1_f(G_w; T_l)$. The second part follows immediately from the first part and the diagram (A1). Note that $H^1(G_w; V_l)/H^1_f(G_w; V_l)$ is a $\mathbb{Q}_l$-vector space. To prove the third part consider the following commutative diagram.

$$\text{(A.1)} \qquad \begin{array}{ccccc}
H^0(g_w;\ A_l) & \longrightarrow & H^1(g_w;\ T_l) & \longrightarrow & H^1_f(G_w;\ V_l) \\
{\scriptstyle =}\downarrow & & \downarrow & & \downarrow \\
H^0(G_w;\ A_l) & \longrightarrow & H^1(G_w;\ T_l) & \longrightarrow & H^1(G_w;\ V_l) \\
\downarrow & & \downarrow & & \downarrow \\
H^0(I_w;\ A_l) & \xrightarrow{0} & H^1(I_w;\ T_l) & \longrightarrow & H^1(I_w;\ V_l)
\end{array}$$

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.

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

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 A3. 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 A2. *For any finite extension L/F the following equalities hold.*

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

Proof. The first equality follows from Lemma A1 and the exact sequence.

$$0 \to H^1_{f,S_l}(G_L; T_l) \to H^1(G_L; T_l) \to \prod_{w \notin S_l} H^1(G_w; T_l)/H^1_f(G_w; T_l).$$

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

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

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

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

So the second equality in the statement of lemma A2 also holds . $\square$

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

$$\begin{array}{ccc} H^1_{f,S_l}(G_L; T_l) & \longrightarrow & H^1(g_w;\, T_l) \\ \uparrow & & \uparrow \\ H^0(G_L; A_l) & \longrightarrow & H^0(g_w;\, A_l). \end{array} \tag{A.2}$$

The bottom horizontal arrow is obviously an injection. Hence, by Lemmas A1 and A2, we obtain the following:

Lemma A3. *For any finite extension L/F and any prime $w \notin S_l$ in $\mathcal{O}_L$ the natural map*

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

is an imbedding.

Proposition A1. *We have the following exact sequences*

$$0 \to A_l \to J(T_l) \to J(V_l) \to 0$$
$$0 \to A_l \to J_{f,S_l}(T_l) \to J_{f,S_l}(V_l) \to 0$$

In particular

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

and the groups

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

are divisible.

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

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

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

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

This short exact sequence fits into the following commutative diagram

(A.3)

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

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 A1. $\square$

Proposition A2. *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) $H^1_{f,S_l}(G_L; T_l) \cong J_{f,S_l}(T_l)^{G_L}$.

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.

$$
\text{(A.4)} \qquad
\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
H^1_{f,S_l}(G_L; T_l) & \longrightarrow & H^1_{f,S_l}(G_{L'}; T_l)^{G(L'/L)} \\
\downarrow & & \downarrow \\
H^1(G_L; T_l) & \xrightarrow[\cong]{} & H^1(G_{L'}; T_l)^{G(L'/L)} \\
\downarrow & & \downarrow \\
\prod_{w \notin S_l} H^1(I_w;\ T_l) & \longrightarrow & \prod_{w \notin S_l} \big(\prod_{w'|w} H^1(I_{w'};\ T_l)\big)^{G(L'/L)}
\end{array}
$$

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 Th. 8.1 and Cor. 8.3 Chap. I of [CF] and Kummer pairing we get the following commutative diagram

$$
\text{(A.5)} \qquad
\begin{array}{ccc}
H^1(I_w;\ T_l) & \longrightarrow & H^1(I_{w'};\ T_l) \\
\big\downarrow = & & \big\downarrow = \\
Hom_{cts}(I_w;\ T_l) & \longrightarrow & Hom_{cts}(I_{w'};\ T_l) \\
\big\downarrow \cong & & \big\downarrow \cong \\
Hom_{cts}(\mathbb{Z}_l(1);\ T_l) & \longrightarrow & Hom_{cts}(\ Z_l(1);\ T_l)
\end{array}
$$

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 $\mathbb{Z}_l(1) \to \mathbb{Z}_l(1)$. Because T_l is a free Z_l-module, every nontrivial homomorphism of $\mathbb{Z}_l$-modules $\mathbb{Z}_l(1) \to T_l$ is injective. Hence the bottom horizontal arrow in the diagram (A.5) is injective. So the bottom horizontal arrow in diagram (A.4) is also an imbedding. Now claim (2) follows by taking direct limits over L' in diagram (A.4) and chasing the resulting diagram. $\square$

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

$$r_v\colon H^1_{f,S_l}(G_F;\, T_l) \to H^1(g_v;\, T_l).$$

Proposition A3. *Let $\hat{P} \in H^1_{f,S_l}(G_F;\, T_l)$ 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 $F(A[M])$. Consider the following commutative diagram.

$$\text{(A.6)}\qquad \begin{array}{ccc} H^1_{f,S_l}(G_F;\, T_l)/M & \xrightarrow{r_v} & H^1(g_v;\, T_l)/M \\ {\scriptstyle h_1}\downarrow & & \downarrow \\ H^1_{f,S_l}(G_F;\, A[M]) & \xrightarrow{r_v} & H^1(g_v;\, A[M]) \\ {\scriptstyle h_2}\downarrow & & \downarrow \\ H^1_{f,S_l}(G_{F_M};\, A[M]) & \xrightarrow{r_w} & H^1(g_w;\, A[M]) \\ {\scriptstyle h_3}\downarrow & & \downarrow \\ Hom(G_{F_M};\, A[M]) & \xrightarrow{r_w} & Hom(G_w;\, A[M]) \\ {\scriptstyle h_4}\downarrow\cong & & \downarrow = \\ Hom(G_{F_M}^{ab};\, A[M]) & \xrightarrow{r_w} & Hom(g_w;\, A[M]) \end{array}$$

The horizontal arrows in the diagram (A.6) are induced by the reduction maps. We describe the vertical maps. By Proposition 1 (1) the map h_2 is an injection. 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:

$$\text{(A.7)}\qquad 0 \longrightarrow A[l] \longrightarrow J_{f,S_l}(T_l) \xrightarrow{\times l} J_{f,S_l}(T_l) \longrightarrow 0.$$

The vertical maps on the right hand side of the diagram (A.6) are defined in the similar way. Consider the nontorsion element $\hat{P} \in H^1_{f,S_l}(G_F;\, T_l)$. Let l^s be the largest power of l such that $\hat{P} = l^s \hat{R}$ for an $\hat{R} \in H^1_{f,S_l}(G_F;\, T_l)$. Such an l^s exists since $H^1_{f,S_l}(G_F;\, T_l)$ is a finitely generated $\mathbb{Z}_l$-module. We put $M = M_1 l^s$. Let P' be the image of $\hat{P}$ in $Hom(G_{F_M}^{ab};\, A[M])$ 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 (A.6) 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 A1.
Let $\hat{P} \in H^1_{f,S_l}(G_F; T_l)$ be an element which maps onto a generator of the free Z_l - module $H^1_{f,S_l}(G_F; T_l)/tor$. 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 $H^1(g_v; T_l)$.

Appendix B. Nondegenarate CM abelian varieties.

Let A/F be a simple abelian variety of dimension g with complex multiplication by a CM field E cf. [La]. We assume that the CM data is defined over F and in addition that the Hilbert class field E^H of E is contained in F. In ths appendix, following [R3], we discuss CM abelian varieties of nodegenerate type. Let (E, S) be the CM-type of A and let (E', R) be its reflex type. Let $L/\mathbb{Q}$ be a finite Galois extension containing E. Put $G = G(L/\mathbb{Q})$, $H = G(L/E)$ and $H' = G(L/E')$. We identify S with a subset of right cosets in $H \backslash G$. Let T be an algebraic torus defined over a number field. The character group of T is by definition

$$X(T) = Hom_{\overline{\mathbb{Q}}}(T, \mathbb{G}_m).$$

For a number field K we put $T_K = Res_{K/\mathbb{Q}}(\mathbb{G}_m)$. Observe that

$$X(T_K) = \{ \sum_{\sigma \in \text{Hom }(K;\mathbb{C})} n_\sigma[\sigma];\ n_\sigma \in \mathbb{Z}\}.$$

K. Ribet in [R3] p. 85 defines a homomorphism of tori

$$\phi :\ T_{E'} \to T_E$$

by giving the following homomorphism on character groups

$$\phi^* :\ X(T_E) \to X(T_{E'})$$

$$[\sigma] \to \sum_{\gamma \in R} [\gamma\sigma].$$

The image of ϕ is an algebraic torus which is equal to the Mumford-Tate group of A cf. [D2, Ex. 3.7] and [W, p. 128-129]. The dimension of $Im\,\phi$ is by definition the rank of the CM-type (E, S) and the rank of the abelian variety A. It is easy to see that the rank of (E, S) equals the rank of the matrix

$$\big(i(\tau, \sigma)\big)_{\tau \in H' \backslash G,\ \sigma \in H \backslash G}$$

where the entries are defined by the formula

$$i(\tau, \sigma) = \begin{cases} 1, & \text{if } \sigma\tau^{-1} \in \tilde{S} \\ 0, & \text{if } \sigma\tau^{-1} \notin \tilde{S} \end{cases}$$

and $\tilde{S} = \{g \in G: \quad Hg \in S\}$.

Definition B1. *We say that the CM-type (E, S) is nondegenerate if the rank of (E, S) equals $g{+}1$. We say that the CM abelian variety A is nondegenerate if its type is nodegenerate. This means that the Mumford-Tate group of A (for the definition see [D2]) is of maximal possible dimension.*

Example B1. In [R3], Example 3.7 it is shown that all CM abelian varieties of dimension smaller than 4 are nondegenerate. Kubota in [K] Th. 2, p. 121 showed that the Jacobian variety of the curve $y^2 = 1{-}x^p$, where p is an odd prime is of nondegenerate CM-type. For examples of CM varieties A with rank smaller than $dim\, A{+}1$ (which are called degenerate), we refer the reader to papers [R3], sec. 3, p. 89 and [Haz], sec. 5, p. 747.

Let $\rho_l : G_F \to Gl(T_l(A)) = Gl_{2g}(\mathbb{Z}_l)$ be the l-adic representation of the Galois group G_F on the Tate module of A. According to Corollary 2, p. 502 of [ST], the image of this representation is an abelian group contained in the subgroup $(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_l)^\times$ of $Gl_{2g}(T_l(A))$. We have the following commutative diagram

$$\text{(B.1)}\qquad \begin{array}{ccccc} & & G_F & \xrightarrow{\rho_l} & Gl_{2g}(\mathbb{Z}_l) \\ & & \downarrow & & \uparrow \\ \prod_{v|l} \mathcal{O}_{F,v}^\times & \xrightarrow{c_l} & G_F^{ab} & \xrightarrow{\rho_l^{ab}} & (\mathcal{O}_E \otimes \mathbb{Z}_l)^\times, \end{array}$$

where the map c_l is the restriction to $\prod_{v|l} \mathcal{O}_{F,v}^\times$ of the composition of natural maps:

$$\prod_v \mathcal{O}_{F,v}^\times \to (F^\times \prod_v \mathcal{O}_{F,v}^\times)/F^\times \to I_F/F^\times \to G_F^{ab}.$$

The map on the right side in the above sequence of maps is the global norm residue symbol of global class field theory, ([N], p. 94). Let l be a prime of good reduction for A relatively prime to the class number of F. The natural isomorphism

$$Cl(\mathcal{O}_F) \cong I_F/(F^\times \prod_v \mathcal{O}_{F,v}^\times)$$

[N], Prop. 2.3, p. 77 and Artin global reciprocity law, [N], Th. 6.5, p. 94, show that the image of ρ_l is equal to the image of the composition $\rho_l^{ab} \circ c_l$. According to [ST], p. 511 there is a homomorphism of algebraic tori

$$\text{(B.2)}\qquad \psi\colon T_F \to T_E$$

over $\mathbb{Q}$, such that after base change to $\mathbb{Q}_l$ we obtain a map of tori

$$\text{(B.3)}\qquad \psi_l\colon T_{F_l} \to T_{E_l}$$

over $\mathbb{Q}_l$, where $T_{F_l} = \prod_{v|l} Res_{F_v/\mathbb{Q}_l}(\mathbb{G}_m)$ and $T_{E_l} = \prod_{\lambda|l} Res_{E_\lambda/\mathbb{Q}_l}(\mathbb{G}_m)$. For any torus $T/\mathbb{Q}_l$ put

$$T(\mathbb{Z}_l) = \{t \in T(\mathbb{Q}_l); \quad \chi(t) \in \mathbb{Z}_l^\times, \quad \text{for all} \quad \chi \in (X(T))_{\mathbb{Q}_l}\},$$

where $(X(T))_{\mathbb{Q}_l}$ is the group of characters of T defined over $\mathbb{Q}_l$ cf. [O], p. 115, [R3], p. 77 and [V], p. 134-139. Short computation shows that

$$T_{F_l}(\mathbb{Z}_l) = \prod_{v|l} \mathcal{O}_{F,v}^\times \quad \text{and} \quad T_{E_l}(\mathbb{Z}_l) = \prod_{\lambda|l} \mathcal{O}_{E,\lambda}^\times$$

The map (B.3) gives a group homomorphism

$$\psi_l(\mathbb{Z}_l)\colon T_{F_l}(\mathbb{Z}_l) \to T_{E_l}(\mathbb{Z}_l) \tag{B.4}$$

which by Theorem 11, p. 512 and Corollary 2, p. 513 of [ST] can be identified with the map $\rho_l^{ab} \circ c_l$.

Theorem B1. *Let A/F be a simple abelian variety of nodegenerate CM-type. Then for all primes l of good reduction for A that are split in F, the image of the reduced representation*

$$\bar{\rho}_l\colon G_F \to Gl_{2g}(\mathbb{F}_l)$$

consists of all diagonal matrices of the form

$$\{diag(x_1, y_1, \ldots, x_g, y_g) \in Gl_{2g}(\mathbb{F}_l)\colon \quad x_1 y_1 = \cdots = x_g y_g\}.$$

Proof. By [R3], Prop. 3.8 we have the following commutative triangle:

$$\begin{tikzcd} T_F \arrow[rr, "\psi"] \arrow[dr, "N_{F/E'}"'] & & T_E \\ & T_{E'} \arrow[ur, "\phi"'] & \end{tikzcd} \tag{B.2}$$

Since l splits completely in F and E by assumption, we have

$$T_{F_l} = \prod_{i=1}^{[F:\mathbb{Q}]} \mathbb{G}_m \qquad T_{E_l} = \prod_{i=1}^{2g} \mathbb{G}_m.$$

Since A is nondegenerate, the image of ψ has dimension $g+1$ (cf. [R3], Cor. 3.9). Thus the image of the map $\psi_l : T_{F_l} \to T_{E_l}$ is a torus of dimension $g+1$. Denote by E^+ the maximal totally real subfield of E and put

$$E_l^+ = E^+ \otimes \mathbb{Q}_l \cong \mathcal{O}_{E^+} \otimes \mathbb{Q}_l.$$

We fix an isomorphism of $\mathbb{Q}_l$-vector spaces

$$E_l \cong E_l^+ \oplus E_l^+.$$

This isomorphism and the representation $\rho_l \otimes \mathbb{Q}_l$ defines a representation

$$\rho_l^+ \otimes \mathbb{Q}_l \,:\, G_F \longrightarrow Gl_2(E_l^+).$$

such that

$$\det_{E_l^+} \circ\, (\rho_l^+ \otimes \mathbb{Q}_l) = \chi_c$$

(cf. [R1], Lemma 4.5.1), where χ_c denotes the composition of the cyclotomic character $G_F \to \mathbb{Q}_l^\times$ and the obvious imbedding $Q_l \to E_l^+$. Since l splits completely in E, the representation $\rho_l \otimes \mathbb{Q}_l : G_F \longrightarrow Gl_{2g}(\mathbb{Q}_l)$ is diagonalizable and there exists a basis of E_l over $\mathbb{Q}_l$ such that

$$Im\,\rho_l \subset \{diag(x_1, y_1, \ldots, x_g, y_g) \in Gl_{2g}(\mathbb{Q}_l) : \quad x_1 y_1 = \cdots = x_g y_g\}.$$

Let T_{nd} denote the following torus:

$$\{diag(x_1, y_1, \ldots, x_g, y_g) \in Gl_{2g} : \quad x_1 y_1 = \cdots = x_g y_g\}$$

over $\mathbb{Q}_l$. One can easily check that there is a natural isomorphism (over $\mathbb{Q}_l$) of group schemes

$$T_{nd} \cong \underbrace{(\mathbb{G}_m \times_{\mathbb{Q}_l} \mathbb{G}_m) \times_{\mathbb{G}_m} \cdots \times_{\mathbb{G}_m} (\mathbb{G}_m \times_{\mathbb{Q}_l} \mathbb{G}_m)}_{g-times} \cong \mathbb{G}_m^{g+1},$$

where the structure map for $\times_{\mathbb{G}_m}$ product is the group structure map $\mathbb{G}_m \times_{\mathbb{Q}_l} \mathbb{G}_m \to \mathbb{G}_m$ of the group scheme $\mathbb{G}_m$. The torus T_{nd} is contained in T_{E_l}. This shows that the image of the map $\psi_l = \psi \otimes \mathbb{Q}_l$ is a subtorus of T_{nd}, which is split and of dimension $g{+}1$, hence $Im\,\psi_l = T_{nd}$. It follows that ψ_l can be written as the composition of homomorphisms of tori

$$\psi_l \,:\, T_{F_l} \longrightarrow T_{nd} \longrightarrow T_{E_l}. \tag{B.5}$$

Taking corresponding $\mathbb{Z}_l$-models of maps of tori in (B.5) (cf. [V], Prop. 6.13, p. 138), we get a map of schemes

$$\Psi_l \,:\, \mathcal{T}_{F_l} \longrightarrow \mathcal{T}_{nd} \longrightarrow \mathcal{T}_{E_l}. \tag{B.6}$$

Taking fibers in (B.6) over $spec\,\mathbb{F}_l$ we get maps of split tori

$$\bar{\psi}_l \,:\, \bar{T}_{F_l} \longrightarrow \bar{T}_{nd} \longrightarrow \bar{T}_{E_l} \tag{B.7}$$

On the other hand by [O], Th. 2.3.1, [R3], p. 93 and [V], Prop. 6.14, p. 139, we have the commutative diagram

$$\begin{array}{ccccc} T_{F_l}(\mathbb{Z}_l) & \longrightarrow & T_{nd}(\mathbb{Z}_l) & \longrightarrow & T_{E_l}(\mathbb{Z}_l) \\ \downarrow & & \downarrow & & \downarrow \\ \bar{T}_{F_l}(\mathbb{F}_l) & \longrightarrow & \bar{T}_{nd}(\mathbb{F}_l) & \longrightarrow & \bar{T}_{E_l}(\mathbb{F}_l) \end{array} \tag{B.8}$$

where the compositions of horizontal maps are $\psi_l(\mathbb{Z}_l)$, $\bar{\psi}_l(\mathbb{F}_l)$ and the vertical maps are reductions mod l. Hence, by (B.1), (B.2), (B.4), (B.7) and (B.8) we see that $Im\,\bar{\rho}_l = \bar{T}_{nd}(\mathbb{F}_l)$. $\square$

Appendix C. Abelian varieties with real multiplication.

Let E be a totally real extension of $\mathbb{Q}$ of degree $[E;\mathbb{Q}] = e$. Let A/F be a polarized simple abelian variety of dimension g of type E, which means that $E \subset End_{\bar{F}}(A) \otimes_Z \mathbb{Q}$ and the polarization is over F cf. [R1] chap. II.1 or [C] Chap. 1.1. We assume that $E = End_F(A) \otimes_{\mathbb{Z}} \mathbb{Q} = End_{\bar{F}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and in addition that $E^H \subset F$. Since $End_{\bar{F}}(A) \cap E = R_E$ is an order in $\mathcal{O}_E$ we observe that $R_E \otimes_{\mathbb{Z}} \mathbb{Z}_l = \mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_l$ for l that does not divide the index $[\mathcal{O}_E\,;\,R_E]$. In this appendix we consider such primes l that additionally split completely in E. The polarisation of A gives $\mathbb{Q}_l$-bilinear, nondegenerate alternating pairing

$$\langle\ ,\ \rangle\ :\ V_l(A) \times V_l(A) \rightarrow \mathbb{Q}_l(1) \tag{C.1}$$

which is Galois equivariant and such that for every $x, y \in V_l(A)$ and $\phi \in End_{\bar{F}}(A) \otimes_Z \mathbb{Q}$ we have

$$\langle\, \phi(x),\, y\rangle = \langle\, x,\, \phi'(y)\rangle,$$

where ϕ' denotes the effect of Rosati involution of the ring $End_{\bar{F}}(A) \otimes_Z \mathbb{Q}$ on the element ϕ. Theorem 2, Type I, p. 201 of [M] implies that the Rosati involution acts trivially on E. Let us restrict the pairing (C.1) to $T_l(A) \times T_l(A)$. The vertical arrows in the diagram (C.2)

$$\begin{array}{ccc} T_l(A) \times T_l(A) & \xrightarrow{\langle\, ,\, \rangle} & \mathbb{Z}_l(1) \\ \downarrow & & \downarrow \\ V_l(A) \times V_l(A) & \xrightarrow{\langle\, ,\, \rangle} & \mathbb{Q}_l(1) \end{array} \tag{C.2}$$

are injective. Under our assumption on l and E the pairing (C.1) splits into non-degenerate, $\mathbb{Q}_l$ bilinear, alternating pairings (cf. [C], Lemma 1.2.1, p. 319)

$$\langle\ ,\ \rangle\ :\ V_\lambda(A) \times V_\lambda(A) \rightarrow \mathbb{Q}_l(1) \tag{C.3}$$

Reducing modulo l and splitting into λ components the top horizontal arrow in diagram (C.2), it follows again by [C], Lemma 1.2.1, p. 319 that for each prime λ of $\mathcal{O}_E$ that divides l there is a nondegenerate bilinear, alternating pairing

$$\langle\, ,\, \rangle_\lambda \,:\, A[\lambda] \times A[\lambda] \to \mathbb{Z}/l(1) \tag{C.4}$$

such that for every $\alpha \in \mathbb{F}_l$

$$\langle\, \alpha x,\, y\rangle_\lambda = \langle\, x,\, \alpha y\rangle_\lambda = \alpha\langle\, x,\, y\rangle_\lambda.$$

We are going to investigate the image of the residual representation

$$\overline{\rho_l} \,:\, G_F \to Gl(A[l]) \cong Gl_{2g}(\mathbb{F}_l)$$

of the representation

$$\rho_l \,:\, G_F \to Gl(T_l(A)) \cong Gl_{2g}(\mathbb{Z}_l)$$

for abelian varieties A/F and prime l satisfying all the above assumptions. As usual we let G_l to denote the image of $\overline{\rho_l}$. Because of the pairings (C.3) and (C.4) for an appropriate choice of bases in the $\mathbb{F}_l$ vector spaces $A[\lambda]$ we get

$$G_l \,\subset\, \prod_{\lambda | l} GSp_{A[\lambda]}(\mathbb{F}_l) \,\cong\, \prod_{\lambda | l} GSp_{2h}(\mathbb{F}_l) \subset Gl_{2g}(\mathbb{F}_l)$$

where $2he = 2g$ and GSp denote the respective groups of symplectic similitudes.

Let us introduce some notation. For an algebraic group scheme G/S over the base scheme S we denote by G' the derived group scheme of G, as defined in [SGA3] XXII, 6.2. If G is an algebraic group over a field, then G' is the commutator subgroup of G. We put $\tilde{G}$ to be the universal cover of G and $G(S)_u$ to be the image of the natural map $\tilde{G}(S) \to G(S)$. Observe that if G is simply connected, i.e., if $\tilde{G} = G$, then we get $G(S)_u = G(S)$. Let G_l^{alg} be the algebraic envelope of the image of $\rho_l \otimes \mathbb{Q}_l$ in the group $Gl_{2g}/\mathbb{Q}_l$ i.e. the Zariski closure of the image. Enlarging F, if necessary we can assume that G_l^{alg} is connected for any l. This is justified by the results of Serre, [Se4] (see also [LP2]). Let $\mathcal{G}_l^{alg}$ be the Zariski closure of the image of ρ_l in the algebraic group $Gl_{2g}/\mathbb{Z}_l$, endowed with the unique structure of reduced closed subscheme. It follows by [LP1], Prop.1.3 (see also [Wi], Th.1) that for $l \gg 0$ the scheme $\mathcal{G}_l^{alg}$ is smooth over $\mathbb{Z}_l$. Let $G(l)^{alg}$ be the algebraic envelope of the image of $\overline{\rho_l}$ in $Gl_{2g}/\mathbb{F}_l$. Observe that G_l^{alg} is the general fiber of $\mathcal{G}_l^{alg}$ over $spec\,\mathbb{Z}_l$ cf. [Wi] 2.1. On the other hand, by [Wi] Lemme 5 and by [Se3], pp. 43-46, $G(l)^{alg}$ is the special fiber of $\mathcal{G}_l^{alg}$ over $spec\,\mathbb{Z}_l$. By definition, we have

$$G_l^{alg} \subset \prod_{\lambda | l} GSp_{V_\lambda(A)} \cong \prod_{\lambda | l} GSp_{2h}/\mathbb{Q}_l \subset Gl_{2g}/\mathbb{Q}_l \tag{C.5}$$

$$G(l)^{alg} \subset \prod_{\lambda | l} GSp_{A[\lambda]} \cong \prod_{\lambda | l} GSp_{2h}/\mathbb{F}_l \subset Gl_{2g}/\mathbb{F}_l \tag{C.6}$$

J. P. Serre used the results of Nori [No] on subgroups of $Gl_{2g}(\mathbb{F}_l)$ to ivestigate the group $G(l)^{alg}$. We collect the results of Serre on $G(l)^{alg}$ proven in [Se2] and [Se3] in the following theorem.

Theorem C1. *([Se2], [Se3]) The group $G(l)^{alg}$ is reductive and in addition:*

(1) *the index $[G(l)^{alg}(\mathbb{F}_l) : G_l \cap G(l)^{alg}(\mathbb{F}_l)]$ is bounded independently of l,*
(2) *there is a finite extension K/F such that $\overline{\rho_l}(G_K) \subset G(l)^{alg}(\mathbb{F}_l)$.*

Following [Se2] p. 22, we write:

$$G(l)^{alg} = T(l)(G(l)^{alg})'$$

where $(G(l)^{alg})'$ is the derived subgroup of $G(l)^{alg}$ and $T(l)$ is a torus which is the connected component of the center of $G(l)^{alg}$. The groups $(G(l)^{alg})'$ and $T(l)$ commute elementwise. It is worth pointing out that the group $(G(l)^{alg})'$ is denoted by $N(l)$ in [Wi] and by $\tilde{G}$ in [No]. Enlarging F if necessary, we can assume that $\overline{\rho_l}(G_F) \subset G(l)^{alg}(\mathbb{F}_l)$ so from now on we assume that the abelian variety A is defined over such a field F. This is justified by Theorem C1 (2). Observe that by (C.6) we have:

$$(G(l)^{alg})' \ \subset \prod_{\lambda | l} Sp_{2h}. \tag{C.7}$$

Lemma C2. *Let A/F be an abelian variety with with real multiplication by a totally real field $E = End_F(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree $e = [E : \mathbb{Q}]$ such that $g = eh$ with h odd. We have equalities of ranks of group schemes over $\mathbb{Q}_l$:*

$$rank \ (G_l^{alg})' \ = rank \prod_{\lambda | l} Sp_{2h}/\mathbb{Q}_l \tag{C.8}$$

Proof. Let $g = Lie(G_l^{alg})$. Then $g = g^{ss} \oplus \mathbb{Q}_l$, where $g^{ss} = Lie((G_l^{alg})')$. Note that by (C.5) we have

$$g^{ss} \ \subset \bigoplus_{\lambda | l} sp_{2h}(V_\lambda), \tag{C.9}$$

where $V_\lambda = V_l(A) \otimes_E E_\lambda$. Put $\bar{V}_\lambda = V_\lambda \otimes \overline{\mathbb{Q}}_l$. In order to prove (C.8) it is enough to show that

$$g^{ss} \otimes \overline{\mathbb{Q}}_l \ = \ \bigoplus_{\lambda | l} sp_{2h}(\overline{V}_\lambda). \tag{C.10}$$

Projecting onto the λ component we see that the image of $g^{ss} \otimes \overline{\mathbb{Q}}_l$ in $sp_{2h}(\overline{V}_\lambda)$ is semisimple. Hence, using the structure of the universal enveloping algebra of a semisimple lie algebra [H] pp. 89-94 and the properties of the irreducible standard cyclic modules [H] pp. 107-110, we get a decomposition

$$\bar{V}_\lambda = E(\omega_1) \otimes_{\overline{\mathbb{Q}}_l} \cdots \otimes_{\overline{\mathbb{Q}}_l} E(\omega_r),$$

where $E(\omega_i)$, for all $1 \leq i \leq r$, are the irreducible (orthogonal or symplectic) Lie algebra modules of the highest weight ω_i corresponding to simple Lie algebras g_i which are factors of the image

$$Im\,\big(\, g^{ss} \otimes \overline{\mathbb{Q}}_l \to sp_{2h}(\overline{V}_\lambda)\,\big) = \; g_1 \oplus \cdots \oplus g_r.$$

By Corollary 5.11 [P] all simple factors of $g^{ss} \otimes \overline{\mathbb{Q}}_l$ are of classical type A, B, C and D and the weights $\omega_1, \ldots, \omega_r$ are minimal (= miniscule = microweight). The reader can find the table of all minimal weights for corresponding type in [H] exer. 13.13 p. 72 or [Bour] Chap. VIII, 7.3. Since $dim_{\overline{\mathbb{Q}}_l}\, \overline{V}_\lambda = 2h$, where h odd by assumption, we observe by computing the dimensions of $E(\omega_i)$'s for types A, B, C and D (use [Ta1] section 4.8.1 and [Bour] Chap. VIII, Tables 1, 2 pp. 213-214, cf. [C] p. 332), that the tensor product $E(\omega_1) \otimes_{\overline{\mathbb{Q}}_l} \cdots \otimes_{\overline{\mathbb{Q}}_l} E(\omega_r)$ can consist of only one space $E(\omega_1)$ and g_1 has the type C symplectic representation on $E(\omega_1)$. Hence

$$Im\,\big(\, g^{ss} \otimes \overline{\mathbb{Q}}_l \to sp_{2h}(\overline{V}_\lambda)\,\big) = \; sp_{2h}(\overline{V}_\lambda).$$

By the result of Faltings [Fa] cf. [Se1] 2.5.4 the representations

$$g^{ss} \otimes \overline{\mathbb{Q}}_l \;\to\; sp_{2h}(\overline{V}_\lambda)$$

are pairwise not isomorphic, for any two of the ideals $\lambda | l$. Hence, by the structure theorem of semisimple Lie algebras, [H] Th. 5.2, we deduce that the natural map

$$g^{ss} \otimes \overline{\mathbb{Q}}_l \;\to\; sp_{2h}(\overline{V}_{\lambda_1}) \oplus sp_{2h}(\overline{V}_{\lambda_2})$$

is surjective for any pair of ideals λ_1, λ_2 dividing l. By [R1], Lemma, p. 790, this implies (C.10). $\square$

Lemma C3. *Let A be an abelian variety with with real multiplication by a totally real field $E = End_F(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree $e = [E : \mathbb{Q}]$ such that $g = eh$ with h odd. There are equalities of ranks of group schemes over $\mathbb{F}_l$:*

$$\text{(C.11)} \qquad rank\ (G(l)^{alg})' \; = rank\ (\prod_{\lambda | l}\ Sp_{2h}/\mathbb{F}_l)$$

for all $l \gg 0$.

Proof. By [LP1] Prop.1.3 and by [Wi], Th.1 and 2.1, for $l \gg 0$ the group scheme $\mathcal{G}_l^{alg}$ over $spec\, \mathbb{Z}_l$ is smooth and reductive. For such an l the structure morphism $(\mathcal{G}_l^{alg})' \to spec\, \mathbb{Z}_l$ is the base change of the smooth morphism $\mathcal{G}_l^{alg} \to$

$D_{\mathbb{Z}_l}(D_{\mathbb{Z}_l}(\mathcal{G}_l^{alg}))$ via the unit section of $D_{\mathbb{Z}_l}(D_{\mathbb{Z}_l}(\mathcal{G}_l^{alg}))$, see [SGA3] XXII, Th. 6.2.1, p. 256. Hence, the group scheme $(\mathcal{G}_l^{alg})'$ is also smooth over $\mathbb{Z}_l$. By [SGA3] *loc. cit*, the group scheme $(\mathcal{G}_l^{alg})'$ is semisimple. By [SGA3] XIX, Th. 2.5, p. 12, applied to the special fiber of the base scheme $spec\,\mathbb{Z}_l$, there exists an étale neighborhood $S' \to spec\,\mathbb{Z}_l$ of the geometric point over the special point such that $\mathcal{G}_{l,S'}^{alg} = \mathcal{G}_l^{alg} \times_{spec\,\mathbb{Z}_l} S'$ has a maximal torus $\mathcal{T}_{S'}$. By [SGA3] XXII, Th. 6.2.8 p. 260, $(\mathcal{G}_{l,S'}^{alg})' \cap \mathcal{T}_{S'}$ is a maximal torus of $(\mathcal{G}_{l,S'}^{alg})'$. By definition of the maximal torus and by [SGA3] XIX, Th. 2.5, p. 12 applied to the special point of $spec\,\mathbb{Z}_l$, we obtain that the special and the generic fibers of $(\mathcal{G}_{l,S'}^{alg})'$ have the same rank. On the other hand, it is clear that the generic (resp. special) fibers of $(\mathcal{G}_{l,S'}^{alg})'$ and $(\mathcal{G}_l^{alg})'$ have the same rank. Hence, for $l \gg 0$:

$$rank\ (G_l^{alg})' = rank\ (G(l)^{alg})'. \tag{C.12}$$

Observe that

$$rank\ Sp_{2h}/\mathbb{Q}_l = rank\ Sp_{2h}/\mathbb{F}_l = h. \tag{C.13}$$

Equalities (C.12), (C.13) and Lemma C.2 show that the ranks of the group schemes at both ends of the bottom horizontal arrow in the diagram

$$\begin{array}{ccc} (G_l^{alg})' & \longrightarrow & \prod_{\lambda|l} Sp_{2h}/\mathbb{Q}_l \\ \downarrow & & \downarrow \\ (\mathcal{G}_l^{alg})' & \longrightarrow & \prod_{\lambda|l} Sp_{2h}/\mathbb{Z}_l \\ \uparrow & & \uparrow \\ (G(l)^{alg})' & \longrightarrow & \prod_{\lambda|l} Sp_{2h}/\mathbb{F}_l \end{array} \tag{C.14}$$

are the same. This concludes the proof. $\square$

Lemma C4. *Under assumptions of Lemmas C2 and C3 we have equalities of group schemes:*

$$(G_l^{alg})' = \prod_{\lambda|l} Sp_{2h}/\mathbb{Q}_l \tag{C.15}$$

$$(G(l)^{alg})' = \prod_{\lambda|l} Sp_{2h}/\mathbb{F}_l \tag{C.16}$$

for all $l \gg 0$.

Proof. We prove the equality (C.16). The proof of the equality (C.15) is very similar and we leave it for the reader. Let

$$\underline{\rho}_l\ :\ G(l)^{alg} \to Gl_{2g}$$

denote the inclusion representation induced by $G(l)^{alg} \subset Gl_{2g}$. By the result of Faltings [Fa] the representation $\underline{\rho}_l$ is semisimple and the commutant of $\underline{\rho}_l(G(l)^{alg})$ in the matrix ring $M_{2g,2g}(\mathbb{F}_l)$ is $End_{\bar{F}}(A) \otimes_{\mathbb{Z}} \mathbb{F}_l$. Projecting onto the λ component we obtain the representation

$$\underline{\rho}_\lambda \,:\, G(l)^{alg} \to\, GSp_{A[\lambda]} \,\cong\, GSp_{2h}.$$

The commutant of $\underline{\rho}_\lambda$ is $\mathbb{F}_l$ because $End_{\bar{F}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \,=\, E$ and l splits completely in E, by assumption. This implies that $\underline{\rho}_\lambda$ is absolutely irreducible. Since $T(l)$ is abelian and it commutes elementwise with $(G(l)^{alg})'$, the restriction of ρ_λ to the derived subgroup:

$$\underline{\rho}_\lambda \,:\, (G(l)^{alg})' \to\, Sp_{2h}$$

is also absolutely irreducible. By Schur's lemma the image $\underline{\rho}_\lambda(Z((G(l)^{alg})')$ of the center of $(G(l)^{alg})'$ is contained in the scalars of Sp_{2h}. This implies that

$$Z((G(l)^{alg})') \,\subset\, Z(\prod_{\lambda|l} Sp_{2h}). \tag{C.17}$$

To simplify notation, we put $G_1 = (G(l)^{alg})'$ and $G_2 = \prod_{\lambda|l} Sp_{2h}$. Note that G_1 and G_2 are reductive groups. Let T be a maximal torus in G_1. Since by Lemma C3 the ranks of G_1 and G_2 are equal, T is also the maximal torus of G_2. Let $h \in Z(G_2)$. By [H], Chap. 26.2, Cor. A (b) we see that $h \in T$. Let C denote the commutant of G_1 in the ring $M_{2g,2g}(\mathbb{F}_l)$. Since $G_1 \subset G_2$, we have $h \in C^\times$, hence $h \in C^\times \cap T = Z(G_1)$. Thus we have $Z(G_2) \subset Z(G_1)$. Together with (C.17) this implies that

$$Z((G(l)^{alg})') \,=\, Z(\prod_{\lambda|l} Sp_{2h}). \tag{C.18}$$

To finish the proof we use the same argument as in the proof of [Wi], Lemme 7 (see also [LP1], Lemma 4.4, p. 577). Let R_1 (R_2, respectively) be the roots of G_1' (G_2', resp.) with respect to the torus T. The roots R_1 form a symmetric subset of R_2 which is closed by [SGA3] XXIII, Cor 6.6. By [Bour] Chap. VI, 1.7, Prop. 23 we obtain equality $R_1 = R_2$. Hence $G_1' = G_2'$, so $G_1 = TG_1' = TG_2' = G_2$. □

Theorem C5. *Let A be an abelian variety with with real multiplication by a totally real field $E = End_F(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree $e = [E : \mathbb{Q}]$ such that $g = eh$ with h odd. Consider the residual representation $\overline{\rho_l}$: $G_F \to Gl_{2g}(\mathbb{F}_l)$ induced by the action on the l-torsion points of A. We have equality:*

$$(\overline{\rho_l}(G_F))' \,=\, \prod_{\lambda|l} Sp_{2h}(\mathbb{F}_l), \tag{C.19}$$

for all $l \gg 0$.

Proof. Since Sp_{2h} is simply connected, it follows by (C.16) that $(G(l)^{alg})'$ is simply connected. So $(G(l)^{alg})'(\mathbb{F}_l) = (G(l)^{alg})'(\mathbb{F}_l)_u$. Hence, by a theorem of Serre (cf. [Wi], Th.4) we get

$$(G(l)^{alg})'(\mathbb{F}_l) \ \subset \ (\overline{\rho_l}(G_F))'.$$

On the other hand, by (C.6) and Th. C1 (2) it is clear that

$$(\overline{\rho_l}(G_F))' \ \subset \ (G(l)^{alg})'(\mathbb{F}_l). \quad \square$$

We finish this section with verification of the Mumford-Tate conjecture for the abelian varieties A/F considered in this appendix. This has been expected by the experts (cf. [P, p. 190]). We refer the reader to [P] and also to [G] for an up-to-date discussion concerning the current status of the Mumford-Tate conjecture. Let us fix some notation first. We choose an embedding of F into the field of complex numbers $\mathbb{C}$. Let $W = H^1(A(\mathbb{C}), \mathbb{Q})$ denote the singular cohomology group with rational coefficients and let

$$W \otimes_{\mathbb{Q}} \mathbb{C} = W^{1,0} \oplus W^{0,1},$$

where $\overline{W^{1,0}} = W^{0,1}$, be its associated Hodge decomposition. Define the cocharacter

$$\mu_\infty : \mathbb{G}_{m,\mathbb{C}} \to Gl(W \otimes_{\mathbb{Q}} \mathbb{C}) = Gl_{2g}(\mathbb{C})$$

such that, for any $z \in \mathbb{C}^\times$, the automorphism $\mu_\infty(z)$ of the space $W \otimes_{\mathbb{Q}} \mathbb{C}$ is the multiplication by z on $W^{1,0}$ and the identity on $W^{0,1}$. Recall that the Mumford-Tate group of the abelian variety $A/\mathbb{C}$ is the smallest algebraic subgroup $MT \subset Gl_{2g}(\mathbb{Q})$, defined over $\mathbb{Q}$, such that $MT \otimes_{\mathbb{Q}} \mathbb{C}$ contains the image of μ_∞. Note that MT is a reductive subgroup of the group of symplectic similitudes GSp_{2g}. According to the Mumford-Tate conjecture (cf. [Se5], C.3.1), for the abelian variety A defined over the number field F, for any rational prime l we should have:

$$G_l^{alg} = MT_l. \tag{C.20}$$

where $MT_l = MT \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Recall that due to our assumptions on A and F, the group G_l^{alg} is connected. It was proved by Deligne [D2], I, Prop. 6.2 that

$$G_l^{alg} \subset MT_l, \tag{C.21}$$

for any l.

Theorem C6. *Let A be an abelian variety with with real multiplication by a totally real field $E = End_F(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree $e = [E : \mathbb{Q}]$ such that $g = eh$ with h odd. Then the Mumford-Tate conjecture holds for A.*

Proof. By [LP1], Th. 4.3. to verify the Mumford-Tate conjecture for all primes l it is enough to show it for at least one prime number l. Let H denote the Hodge group of A, see [D2], Section 3 or [G], p. 312. By definition, the Mumford-Tate group and the Hodge group of A are related by equality

$$MT \;=\; \mathbb{G}_m \, H,$$

where $\mathbb{G}_m$ is in the center of MT. Hence, $(MT)' = (H)'$. The group H is semisiple (cf. [G] Prop. B.63), hence $H = (H)'$ (cf. [H], Th. 27.5). Put $H_l = H \otimes_{\mathbb{Q}} \mathbb{Q}_l$. By (C.15) and (C.21) for $l \gg 0$ and such that l is splitting completely in E, we get:

$$\prod_{\lambda | l} Sp_{2h} = (G_l^{alg})' \subset (H_l)'.$$

On the other hand,

$$H_l \subset \prod_{\lambda | l} Sp_{2h}$$

(see Lemma B.60 and Lemma B.62 of [G]). Hence, we have

(C.22) $$H_l = (G_l^{alg})' = \prod_{\lambda | l} Sp_{2h}.$$

Using the theorem of Bogomolov we get from this

(C.23) $$MT_l = \mathbb{G}_m \, H_l = \mathbb{G}_m \, (G_l^{alg})' \subset G_l^{alg}.$$

The inclusions (C.21) and (C.23) imply the equality (C.20) for A. $\square$

References

[A] D. Arlettaz, *The Hurewicz homomorphism in algebraic K-theory*, J. of Pure and Applied Algebra. **71** (1991), 1 - 12.

[AB] D. Arlettaz, G. Banaszak, *On the non-torsion elements in the algebraic K-theory of rings of integers*, J. reine angew. Math. **461** (1995), 63 - 79.

[Ba] G. Banaszak, *Mod p logarithms $log_2 3$ and $log_3 2$ differ for infinitely many primes*, Annales Mathematicae Silesianae **12** (1998), 141 - 148.

[BG] G. Banaszak, W. Gajda, *Euler systems of higher K-theory of number fields*, Journal of number theory **58, No. 2** (1996), 213 - 252.

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

[BE] S. Bloch, E. Esnault, *The coniveau filtration and non-divisibility for algebraic cycles*, Mathematische Annalen **304** (1996), 303 - 314.

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

[Bo] A. Borel, *Stable real cohomology of arithmetic groups*, Ann. Scient. Ec. Norm. Sup. 4^{ieme} **séries 7** (1974), 235-272.

[BT] A. Borel, J. Tits, *Homomorphisms "abstraits" de groupes algébraiques simples*, Ann. of Math. **97 (2)** (1973), 499-571.

[Bour] N. Bourbaki, *Groups et algèbres de Lie*, Hermann, 1975.

[CF] J.W.S. Cassels, A. Fröhlich eds., *Algebraic number theory*, Academic Press, London and New York, 1967.

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

[C] W. Chi, *l-adic and λ-adic representations associated to abelian varieties defined over a number field*, American Jour. of Math. **114, No. 3** (1992), 315-353.

[D1] P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES **43** (1974), 273-307.

[D2] P. Deligne, *Hodge cycles on abelian varieties*, Lecture Notes in Mathematics **900** (1982), 9-100.

[SGA3] dirige par M. Demazure, A. Grothendieck, *Schemas en Groupes III*, LNM 151, 152, 153, Springer-Verlag, 1970.

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

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

[F] M. Flach, *A generalization of the Cassels-Tate pairing*, J. reine.angew. Math. **412** (1990), 113-127.

[G] B. Gordon, *A survey of the Hodge Conjecture for abelian varieties*, Appendix B in "A survey of the Hodge conjecture", by J. Lewis (1999), AMS, 297-356.

[Har] R. Hartshorne, *Algebraic Geometry*, GTA 52, Springer-Verlag, 1977.

[Haz] F. Hazama, *Hodge cycles on abelian varieties of S_n-type*, J. of Algebraic Geometry **9** (2000), 711-753.

[HS] P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, Springer-Verlag, 1971.

[H] J.E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, 1975.

[I] T. Ichikawa, *Algebraic groups associated with abelian varieties*, Math. Ann **289** (1991), 133-142.

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

[Ja] U. Janssen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology. Galois groups over* $\mathbb{Q}$ (1989), Math. Sci. Res. Inst. Pub. 16, Springer, New York, Berlin.

[K] T. Kubota, *On the field extension by complex multiplication*, Trans. AMS **118 No. 6** (1965), 113-122.

[LP1] M. Larsen, R. Pink, *Abelian varieties, l-adic representations and l independence* **302** (1995), Math. Annalen, 561-579.

[LP2] M. Larsen, R. Pink, *A connectedness criterion for l-adic representations* **97** (1997), Israel J. of Math, 1-10.

[La] S. Lang, *Complex Multiplication*, Springer Verlag, 1983.

[Mi1] J.S. Milne, *Étale cohomology*, Princeton University Press, 1980.

[Mi2] J.S. Milne, *Abelian varieties Arithmetic Geometry G. Cornell, J.H. Silverman (eds.)* (1986), Springer-Verlag, 103-150.

[M] D. Mumford, *Abelian varieties*, Oxford University Press, 1988.

[N] J. Neukirch, *Class Field Theory*, Springer Verlag, 1986.

[No] M. V. Nori, *On subgroups of $Gl_n(\mathbb{F}_p)$*, Invent. Math. **88** (1987), 257-275.

[O] T. Ono, *Arithmetic of algebraic tori*, Annals of Mathematics **74. No. 1** (1961), 101-139.

[P] R. Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. reine angew. Math. **495** (1998), 187-237.

[R1] K. A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, American Jour. of Math. **98, No. 3** (1976), 751-804.

[R2] K. A. Ribet, *Dividing rational points of abelian varieties of CM type*, Compositio math. **33** (1976), 69-74.

[R3] K. A. Ribet, *Division points of abelian varieties with complex multiplication*, Mem. Soc. Math. de France 2e serie **2** (1980), 75-94.

[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).

[Se1] J.P. Serre, *Résumés des cours au Collège de France*, Annuaire du Collège de France (1985-1986), 95-100.

[Se2] J.P. Serre, *Lettre à Daniel Bertrand du 8/6/1984*, Oeuvres. Collected papers. IV. (1985 - 1998), Springer-Verlag, Berlin, 21 - 26.

[Se3] J.P. Serre, *Lettre à Marie-France Vignéras du 10/2/1986*, Oeuvres. Collected papers. IV. (1985-1998), Springer-Verlag, Berlin, 38-55.

[Se4] J.P. Serre, *Lettres à Ken Ribet du 1/1/1981 et du 29/1/1981*, Oeuvres. Collected papers. IV. (1985-1998), Springer-Verlag, Berlin, 1-20.

[Se5] J.P. Serre, *Représetantions l-adiques, in "Algebraic Number Theory" (ed. S.Iyanaga)* (1977), Japan Society for the promotion of Science, 177-193.

[ST] J.P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Math. **68** (1968), 492-517.

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

[Ta1] S.G. Tankeev, *On algebraic cycles on surfaces and abelian varieties*, Izv. Acad. Nauk SSSR. Ser. Mat. **45, No. 2,** (1981), 398-434.

[Ta2] S.G. Tankeev, *On the Mumford-Tate conjecture for abelian varieties*, Algebraic Geometry 4, J. Math. Sci **81 no. 3** (1996), 2719-2737.

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

[V] V.E. Voskresensky, *Algebraiceskije tory*, Izdatelstvo "Nauka", 1977.

[W] S. White, *Sporadic cycles on CM abelian varieties*, Compositio Mathematica **88** (1993), 123-142.

[Wi] J. P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, preprint (October 3, 2000), 1-25.

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

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

current: Department of Mathematics, Northwestern University, Evanston, USA
E-mail address: `GAJDA@math.northwestern.edu`

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