ACTA ARITHMETICA
150.4 (2011)

On arithmetic in Mordell–Weil groups

by

Grzegorz Banaszak (Poznań) and Piotr Krasoń (Szczecin)

1. Introduction. The main objective of the paper is to investigate linear dependence of points in the Mordell–Weil groups of abelian varieties via reduction maps and the height function. Let A/F be an abelian variety over a number field F. Let v be a prime ideal in $\mathcal{O}_F$ with residue field k_v. Let $\mathcal{A}$ be the Néron model of A (cf. [BLR]). The Néron model has the property that $\mathcal{A}(\mathcal{O}_F) = A(F)$. For a prime v of good reduction (cf. [ST], [La, pp. 43–48]) this gives the reduction map $r_v : A(F) \to A_v(k_v)$. In Section 5 we prove the following theorem.

Theorem 1.1. *Let F'/F be a finite extension such that A is isogenous over F' to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i/F' simple, pairwise nonisogenous abelian varieties. Assume that $\dim_{\mathrm{End}_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $\mathrm{End}_{F'}(A_i)^0 := \mathrm{End}_{F'}(A_i) \otimes \mathbb{Q}$. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all primes v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{\mathrm{tor}}$. Moreover, if $A(F)_{\mathrm{tor}} \subset \Lambda$, then the following conditions are equivalent:*

(1) *$P \in \Lambda$,*
(2) *$r_v(P) \in r_v(\Lambda)$ for almost all primes v of $\mathcal{O}_F$.*

In Section 5 (Proposition 5.6) we show that the assumption in Theorem 1.1 concerning the upper bound of the number of simple factors is crucial by giving explicit counterexamples to the detecting linear dependence problem. Our counterexamples involve the abelian surfaces $A_d := E_d \times E_d = E_d^2$ where E_d is the elliptic curve $y^2 = x^3 - d^2x$ with CM by $\mathbb{Z}[i]$ such that $E_d(\mathbb{Q})$ has rank at least 2. Note that $\dim_{\mathbb{Q}(i)} H_1(E_d(\mathbb{C}); \mathbb{Q}) = 1$. Hence A_d does not satisfy the assumption of Theorem 1.1 and is just beyond our upper bound.

It has been understood for many years and presented in numerous papers (e.g. [Ri]) that many arithmetic problems for $\mathbb{G}_{\mathrm{m}}/F$ and methods of treating them are very similar to those for A/F. This similarity has also been shown

2010 *Mathematics Subject Classification*: Primary 11G10; Secondary 14Kxx.
Key words and phrases: Mordell–Weil group, abelian variety, reduction map.

DOI: 10.4064/aa150-4-1

in [BGK1] and [BGK2]. Theorem 1.1 is an analogue for abelian varieties of a theorem of A. Schinzel [Sch, Theorem 2, p. 398], who proved that for any $\gamma_1, \ldots, \gamma_r \in F^\times$ and $\beta \in F^\times$ such that $\beta = \prod_{i=1}^r \gamma_i^{n_{v,i}} \bmod v$ for some $n_{v,1}, \ldots, n_{v,r} \in \mathbb{Z}$ and almost all primes v of $\mathcal{O}_F$ there are $n_1, \ldots, n_r \in \mathbb{Z}$ such that $\beta = \prod_{i=1}^r \gamma_i^{n_i}$. The theorem of A. Schinzel was reproved by Ch. Khare [Kh] by means of methods of C. Corralez-Rodrigáñez and R. Schoof [C-RS]. A. Schinzel's result concerns the algebraic group $\mathbb{G}_{\mathrm{m}}/F$ and as shown in [Sch, p. 419] it does not extend to $T = \mathbb{G}_{\mathrm{m}}/F \times \mathbb{G}_{\mathrm{m}}/F$ and therefore does not extend to algebraic tori and more generally to semiabelian varieties.

In Section 5 we observe that our methods of the proof of Theorem 1.1 can be used to reprove Schinzel's result. In 2002 W. Gajda posed a problem which basically asks whether the analogue of the theorem of Schinzel holds for abelian varieties. In the case of Λ cyclic and A an abelian group scheme this problem was independently posed by E. Kowalski [Ko]. The problem is also called the *detecting linear dependence problem.* Our Theorem 1.1 gives the solution to the problem modulo torsion and strengthens the results of [B], [BGK2], [GG] and [We]. Namely, T. Weston [We] obtained the result stated in Theorem 1.1 for $\mathrm{End}_{\overline{F}}(A)$ commutative. In [BGK2], together with W. Gajda, we proved Theorem 1.1 for elliptic curves without CM and more generally, for a class of abelian varieties with $\mathrm{End}_{\overline{F}}(A) = \mathbb{Z}$, without torsion ambiguity. Moreover we showed [BGK2, Theorem 2.9] that for any abelian variety, any free $\mathrm{End}_F(A)$-module $\Lambda \subset A(F)$ and any $P \in A(F)$ such that $\mathrm{End}_F(A)P$ is a free $\mathrm{End}_F(A)$-module condition (2) of Theorem 1.1 implies that there is an $a \in \mathbb{N}$ such that $aP \in \Lambda$. W. Gajda and K. Górnisiewicz [GG, Theorem 5.1] showed that the coefficient a in [BGK2, Theorem 2.9] may be taken to be equal to 1. A very short proof of [GG, Theorem 5.1] was also given in [B, Prop. 2.8]. The main result of [B] states that the problem asked by W. Gajda has an affirmative solution for all abelian varieties but under the assumption that $\mathrm{End}_F(A)P$ is a free $\mathrm{End}_F(A)$-module and Λ is a free $\mathbb{Z}$-module which has a $\mathbb{Z}$-basis linearly independent over $\mathrm{End}_F(A)$. A. Perucca [Pe2], using methods of [B], [GG] and [Kh], has generalized the results of [B] and [GG] to the case of a product of an abelian variety and a torus and removed the assumption in [B] and [GG] that $\mathrm{End}_F(A)P$ is a free $\mathrm{End}_F(A)$-module. Recently P. Jossen [Jo] has given a positive solution to the detecting linear dependence problem for simple abelian varieties. His methods are different from ours.

Our research on nonsimple abelian varieties with noncommutative endomorphism algebras led us to the discovery of the upper bound in Theorem 1.1. Consequently, we constructed (see Proposition 5.6) counterexamples to the detecting linear dependence problem. Another counterexample was found independently by P. Jossen and A. Perucca [JP].

The proof of Theorem 1.1 relies on simultaneous application of transcendental, l-adic and mod v techniques in the theory of abelian varieties over number fields, the use of semisimplicity of the ring $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and of the methods from [B] and [We]. As a corollary of Theorem 1.1 one gets the theorem of T. Weston [We].

In Section 6 we also consider a strengthening of Theorem 1.1 that could possibly be used for computer implementations. Our main result in that section is the following theorem.

Theorem 1.2. *Let A/F satisfy the hypotheses of Theorem* 1.1. *Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. There is a finite set S^{fin} of primes v of $\mathcal{O}_F$ such that the condition $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{\mathrm{fin}}$ implies $P \in \Lambda + A(F)_{\mathrm{tor}}$. Moreover if $A(F)_{\mathrm{tor}} \subset \Lambda$, then the following conditions are equivalent:*

(1) *$P \in \Lambda$,*
(2) *$r_v(P) \in r_v(\Lambda)$ for $v \in S^{\mathrm{fin}}$.*

In the proof of Theorem 1.2 we use the methods of the proof of Theorem 1.1, supported by the application of the height pairing associated with the canonical height function on A (cf. [HS], [Sil2]) and the effective Chebotarev theorem [LO]. The finite set S^{fin} depends on A, P, Λ, and the choice of a basis of $cA(F)$ (see the proof of Theorem 6.4).

Important ingredients in the proofs of Theorems 4.1 and 6.4 are Theorems 2.6, 2.7, 6.2 and 6.3 concerning the reduction map. These theorems refine previous results of [Bar] and [P] in the case of abelian varieties that are isogenous to products of simple, pairwise nonisogenous abelian varieties.

2. Setup of the problem and the reduction map.

Let A/F be an abelian variety over a number field F. Let $P, P_1, \ldots, P_r \in A(F)$. Put $\Lambda := \sum_{i=1}^{r} \mathbb{Z} P_i$. The following lemma is clear.

Lemma 2.1. *If $P \in \Lambda + T'$ in $A(L)$ for some finite extension L/F and some $T' \in A(L)_{\mathrm{tor}}$, then $P \in \Lambda + T$ in $A(F)$ for some $T \in A(F)_{\mathrm{tor}}$.* ∎

We also have

Lemma 2.2. *Let $\gamma : A \to A_1^{e_1} \times \cdots \times A_t^{e_t}$ be an isogeny defined over a finite extension L/F where $A_1, \ldots, A_t$ are simple, pairwise nonisogenous abelian varieties defined over L. If $\gamma(P) \in \sum_{i=1}^{r} \mathbb{Z}\gamma(P_i) + T'$ for some $T' \in \prod_{i=1}^{t} A_i^{e_i}(L)_{\mathrm{tor}}$, then $P \in \sum_{i=1}^{r} \mathbb{Z} P_i + T$ in $A(F)$ for some $T \in A(F)_{\mathrm{tor}}$.*

Proof. Assume $\gamma(P) \in \sum_{i=1}^{r} \mathbb{Z}\gamma(P_i) + T'$. There exists $Q \in \Lambda$ such that $M(P-Q) \in \mathrm{Ker}\,\gamma$ for M being the order of T'. Hence $M(P-Q) \in A(L)_{\mathrm{tor}}$, so $P - Q \in A(L')_{\mathrm{tor}}$ where L'/L is a finite extension. But $P - Q \in A(F)$, so $P \in Q + A(F)_{\mathrm{tor}}$. ∎

By Lemma 2.2 we can assume that $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$, where $A_1, \ldots, A_t$ are simple, pairwise nonisogenous and defined over F. By Lemma 2.1 we can also assume that F is such that $\mathrm{End}_F(A_i) = \mathrm{End}_{\overline{F}}(A_i)$ for all $i = 1, \ldots, t$. From now on we assume that F is such a field.

We define $r(A) := A_1 \times \cdots \times A_t$. The abelian variety $r(A)$ is called the *radical* of A. Although it certainly depends on the decomposition of A into simple factors, it is unique up to isogeny.

So, assume that $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$ where $A_1, \ldots, A_t$ are simple abelian varieties defined over F. Let $\mathcal{R} := \mathrm{End}_F(A)$. Let $\mathcal{R}_i := \mathrm{End}_F(A_i)$ and $D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$ for all $1 \leq i \leq t$. Then $\mathcal{R} = \prod_{i=1}^t M_{e_i}(\mathcal{R}_i)$. Let $\mathcal{L}_i$ be the Riemann lattice such that $A_i(\mathbb{C}) \cong \mathbb{C}^g / \mathcal{L}_i$ for all $1 \leq i \leq t$. Then $V_i := \mathcal{L}_i \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finite-dimensional vector space over D_i. For each $1 \leq i \leq t$ there is a lattice $\mathcal{L}_i' \subset \mathcal{L}_i$ of index $M_{1,i} := [\mathcal{L}_i : \mathcal{L}_i']$ which is a free $\mathcal{R}_i$-submodule of $\mathcal{L}_i$ of rank $\dim_D V_i$. Let $K/\mathbb{Q}$ be a finite extension such that $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ for each $1 \leq i \leq t$. Hence $V_i \otimes_{\mathbb{Q}} K$ is a free $M_{d_i}(K)$-module of rank $\dim_{D_i} V_i$. Moreover, $\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_K \subset M_{d_i}(K)$ is an $\mathcal{O}_K$-order in $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ and $\mathcal{L}_i' \otimes_{\mathbb{Z}} \mathcal{O}_K$ is a free $\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_K$-module of rank $\dim_D V_i$. Let l be a prime number. For an abelian variety A let $A[l^n]$ be the subgroup of l^n-torsion points of the group $A(F^{\mathrm{s}})$ of F^{s}-valued points. Here F^s denotes the separable closure of F. Let $T_l(A) = \varprojlim A[l^n]$ be the Tate module of A. We have $T_l(A_i) \cong \mathcal{L}_i \otimes_{\mathbb{Z}} \mathbb{Z}_l$ for every prime $l \in \mathbb{Z}$ and every $1 \leq i \leq t$. For a prime ideal $\lambda \,|\, l$ in $\mathcal{O}_K$ let ϵ denote the index of ramification of λ over l.

Let L/F be a finite extension. From now on w will denote a prime of $\mathcal{O}_L$ over a prime v of $\mathcal{O}_F$. Let S be a finite set of primes of $\mathcal{O}_F$ which contains the primes that ramify in L. By the Néron mapping property, $A(L) = \mathcal{A}(\mathcal{O}_{L,S})$ since the natural map $\mathrm{spec}\, \mathcal{O}_{L,S} \to \mathrm{spec}\, \mathcal{O}_F$ is étale. Moreover $\mathcal{A}(\mathcal{O}_{L,S}) = \mathcal{A} \otimes_{\mathcal{O}_F} \mathcal{O}_{L,S}(\mathcal{O}_{L,S})$ by universality of the fiber product. Hence if $v \notin S$ is a prime of good reduction we get the *reduction map*

$$r_w : A(L) \to A_w(k_w).$$

Put $c := |A(F)_{\mathrm{tor}}|$ and $\Omega := cA(F)$. Note that Ω is torsion free. The question we will consider is when the condition $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ implies $P \in \Lambda + A(F)_{\mathrm{tor}}$.

Remark 2.3. The condition $r_v(P) \in r_v(\Lambda)$ implies $r_v(cP) \in r_v(c\Lambda)$. Moreover $cP \in c\Lambda + A(F)_{\mathrm{tor}}$ is equivalent to $P \in \Lambda + A(F)_{\mathrm{tor}}$. Hence without loss of generality we may assume that $P \in \Omega$, $P \neq 0$, $\Lambda \subset \Omega$ and $\Lambda \neq \{0\}$.

Let $P_1, \ldots, P_r, \ldots, P_s$ be a $\mathbb{Z}$-basis of Ω such that

$$\Lambda = \mathbb{Z}d_1P_1 + \cdots + \mathbb{Z}d_rP_r + \cdots + \mathbb{Z}d_sP_s, \tag{2.1}$$

where $d_i \in \mathbb{Z} \setminus \{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$. We put $\Omega_j := cA_j(F)$.

Note that $\Omega = \bigoplus_{j=1}^{t} \Omega_j^{e_j}$. For $P \in \Omega = \sum_{i=1}^{s} \mathbb{Z}P_i$ we write

$$P = n_1P_1 + \cdots + n_rP_r + \cdots + n_sP_s \tag{2.2}$$

where $n_i \in \mathbb{Z}$. Since $\Lambda \subset \Omega$ and Ω is a finitely generated free abelian group, the following condition holds: $P \in \Lambda$ if and only if $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_K$. The membership $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_K$ is equivalent to $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for all prime ideals $\lambda \,|\, l$ in $\mathcal{O}_K$ and all prime numbers l.

Now we need some strengthening of the results of [BGK2], [BGK3], [Bar] and [P] concerning the reduction map for $A = A_1 \times \cdots \times A_t$, i.e. $e_1 = \cdots = e_t = 1$ in our notation. Although the proofs use techniques from [BGK2] and [BGK3] we include complete arguments here since very important parts of the proof of Theorem 4.1 rely heavily on Theorem 2.6 and its proof. Moreover to obtain the proof of Theorem 6.2 in Section 6 we need to modify carefully the proof of Theorem 2.6. The assertion of Theorem 6.2 is essential to prove Theorems 6.3 and 6.4, the main results of Section 6. We also mention that Step 1 of the proof of Theorem 2.6 generalizes an argument of [Kh-P].

Let L/F be any finite extension. Let $P_{i1}, \ldots, P_{ir_i} \in A_i(L)$ be linearly independent over $\mathcal{R}_i$ for each $1 \le i \le t$. Put $L_{l^\infty} := L(A[l^\infty])$, $G_{l^\infty} := G(L_{l^\infty}/L)$, $H_{l^\infty} := G(\overline{F}/L_{l^\infty})$ and $H_{l^k} := G(\overline{F}/L_{l^k})$ for all $k \ge 1$. For each $1 \le i \le t$ and $1 \le j \le r_i$ let

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

denote the inverse limit over k of the Kummer maps

$$\phi_{ij}^{(k)} : H_{l^k} \to A_i[l^k], \qquad \phi_{ij}^{(k)}(\sigma) := \sigma\left(\frac{1}{l^k}P_{ij}\right) - \frac{1}{l^k}P_{ij}.$$

The following lemma is a straightforward generalization of [BGK2, Lemma 2.12].

Lemma 2.4. *If $\alpha_{11}, \ldots, \alpha_{1r_1} \in \mathcal{R}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_l, \ldots, \alpha_{t1}, \ldots, \alpha_{tr_t} \in \mathcal{R}_t \otimes_{\mathbb{Z}} \mathbb{Z}_l$ are such that $\sum_{i=1}^{t} \sum_{j=1}^{r_i} \alpha_{ij}\phi_{ij} = 0$, then $\alpha_{ij} = 0$ in $\mathcal{R}_i$ for all $1 \le i \le t$ and $1 \le j \le r_i$.*

Define the following maps:

$$\Phi_i^k : H_{l^k} \to A_i[l^k]^{r_i}, \qquad \Phi_i^k(\sigma) := (\phi_{i1}^{(k)}(\sigma), \ldots, \phi_{ir_i}^{(k)}(\sigma)).$$

Then define $\Phi^k : H_{l^k} \to \bigoplus_{i=1}^{t} A_i[l^k]^{r_i}$ as $\Phi^k := \bigoplus_{i=1}^{t} \Phi_i^k$. Consider also the maps

$$\Phi_i : H_{l^\infty} \to T_l(A_i)^{r_i}, \qquad \Phi_i(\sigma) := (\phi_{i1}(\sigma), \ldots, \phi_{ir_i}(\sigma)),$$

and again define $\Phi : H_{l^\infty} \to \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}$ to be $\Phi := \bigoplus_{i=1}^{t} \Phi_i$.

Lemma 2.5. *The image of Φ is open in $\bigoplus_{i=1}^{t} T_l(A_i)^{r_i}$.*

Proof. Let $T := \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}$ and $W := T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \bigoplus_{i=1}^{t} V_{il}^{r_i}$ where $V_{il} := T_l(A_i) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Denote by $\Phi \otimes 1$ the composition of Φ with the obvious natural inclusion $T \hookrightarrow W$. Put $M := \operatorname{Im}(\Phi \otimes 1) \subset W$. Both M and W are $\mathbb{Q}_l[G_{l^\infty}]$-modules. It is enough to show that $\operatorname{Im} \Phi$ has a finite index in T (cf. [Ri, Th. 1.2]). Hence it is enough to show that $\Phi \otimes 1$ is onto. Observe that V_{il} is a semisimple $\mathbb{Q}_l[G_{l^\infty}]$-module for each $1 \le i \le t$ because it is a direct summand of the semisimple $\mathbb{Q}_l[G_{l^\infty}]$-module $V_l(A) = \bigoplus_{i=1}^{t} V_{il}$ (cf. [Fa, Th. 3]). Note that G_{l^∞} acts on V_{il} via the quotient $G(L(A_i[l^\infty])/L)$. If $\Phi \otimes 1$ is not onto we have a decomposition $W = M \oplus M_1$ of $\mathbb{Q}_l[G_{l^\infty}]$-modules with M_1 nontrivial. Let $\pi_{M_1} : W \to W$ be the projection onto M_1 and let $\pi_i : W \to V_{il}$ be a projection that maps M_1 nontrivially. Denote $\widetilde{\pi}_i := \pi_i \circ \pi_{M_1}$. By [Fa, Cor. 1] we get $\operatorname{Hom}_{G_{l^\infty}}(V_{il}, V_{i'l}) \cong \operatorname{Hom}_L(A_i, A_{i'}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = 0$ for all $i \ne i'$. Hence

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

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

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

for all $h \in H_{l^\infty}$. Since $\beta_{ij} \in \mathcal{R}_i \otimes \mathbb{Q}_l$, we can multiply the last equality by a suitable power of l to get

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

for some $\alpha_{ij} \in \mathcal{R}_i \otimes \mathbb{Z}_l$. Since the maps: $\mathcal{R}_i \otimes \mathbb{Z}_l \hookrightarrow \mathcal{R}_i \otimes \mathbb{Q}_l$, $\operatorname{Hom}(H_{l^\infty}, T_l) \hookrightarrow \operatorname{Hom}(H_{l^\infty}, V_l)$ are imbeddings of $\mathcal{R} \otimes \mathbb{Z}_l$-modules, we obtain $\sum_{j=1}^{r_i} \alpha_{ij} \phi_{ij} = 0$. By Lemma 2.4 we get $\alpha_{i1} = \cdots = \alpha_{ir_i} = 0$, hence $\beta_{i1} = \cdots = \beta_{ir_i} = 0$ because $\mathcal{R}$ is torsion free. This contradiction shows that $M_1 = 0$. ∎

Theorem 2.6. *Let $Q_{ij} \in A_i(L)$ for $1 \le j \le r_i$ be independent over $\mathcal{R}_i$ for each $1 \le i \le t$. There is a set of primes w of $\mathcal{O}_L$ of positive density such that $r_w(Q_{ij}) = 0$ in $A_{iw}(k_w)_l$ for all $1 \le j \le r_i$ and $1 \le i \le t$.*

Proof. We divide the proof into two steps.

Step 1. We argue as in the proof of [BGK3, Proposition 2]. By Lemma 2.5 there is an $m \in \mathbb{N}$ such that $l^m \bigoplus_{i=1}^{t} T_l(A_i)^{r_i} \subset \Phi(H_{l^\infty}) \subset \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}$. Let Γ be the $\mathcal{R}$-submodule of $A(L)$ generated by all the points Q_{ij}. Hence $\Gamma = \sum_{i=1}^{t} \sum_{j=1}^{r_i} \mathcal{R}_i Q_{ij}$. For $k \ge m$ consider the commutative diagram

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

The maps $\overline{\Phi}$ and $\overline{\Phi^k}$, for all $k \geq 1$, are naturally induced by Kummer maps. For $k \gg 0$ the images of the middle and bottom horizontal arrows in this diagram are isomorphic. Hence $G\big(L_{l^{k+1}}\big(\frac{1}{l^{k+1}}\Gamma\big)/L_{l^{k+1}}\big)$ maps onto $G\big(L_{l^k}\big(\frac{1}{l^k}\Gamma\big)/L_{l^k}\big)$ via the left bottom vertical arrow in the diagram because the map $\overline{\Phi^k}$ is injective for each $k \geq 1$. So a quick look at the tower of fields

$$\begin{tikzcd}
 & L_{l^{k+1}}\big(\frac{1}{l^{k+1}}\Gamma\big) & \\
 & L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big) \arrow[u, dash] & \\
L_{l^k}\big(\frac{1}{l^k}\Gamma\big) \arrow[ur, dash] & & L_{l^{k+1}} \arrow[ul, dash] \\
 & L_{l^k} \arrow[ul, dash, "\mathrm{id}"] \arrow[ur, dash, "h"'] &
\end{tikzcd}$$

gives

$$L_{l^k}\left(\frac{1}{l^k}\Gamma\right) \cap L_{l^{k+1}} = L_{l^k} \quad \text{for } k \gg 0. \tag{2.3}$$

Step 2. Let $h \in G(L_{l^\infty}/L_{l^k})$ be the automorphism which acts on T_lA as a homothety $1 + l^k u$ for some $u \in \mathbb{Z}_l^\times$. Such a homothety exists for $k \gg 0$ by the result of Bogomolov [Bo, Cor. 1, p. 702]. Let h also denote, by a slight abuse of notation, the projection of h onto $G(L_{l^{k+1}}/L_{l^k})$. By (2.3) we can choose $\sigma \in G\big(L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/L\big)$ such that $\sigma_{|L_{l^k}(\frac{1}{l^k}\Gamma)} = \mathrm{id}$ and $\sigma_{|L_{l^{k+1}}} = h$. By the Chebotarev density theorem there is a set of primes w of $\mathcal{O}_L$ of positive density such that there is a prime w_1 in $\mathcal{O}_{L_{l^{k+1}}(\frac{1}{l^k}\Gamma)}$ over w whose Frobenius in $L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/L$ equals σ.

Let $l^{c_{ij}}$ be the order of the element $r_w(Q_{ij})$ in the group $A_{iw}(k_w)_l$, for some $c_{ij} \geq 0$. Let w_2 be the prime of $\mathcal{O}_{L_{l^k}(\frac{1}{l^k}\Gamma)}$ below w_1. Consider the following commutative diagram:

$$\begin{tikzcd}
A_i(L) \arrow[r, "r_w"] \arrow[d] & A_{iw}(k_w)_l \arrow[d, "="] \\
A_i\big(L_{l^k}\big(\frac{1}{l^k}\Gamma\big)\big) \arrow[r, "r_{w_2}"] \arrow[d] & A_{iw}(k_{w_2})_l \arrow[d] \\
A_i\big(L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)\big) \arrow[r, "r_{w_1}"] & A_{iw}(k_{w_1})_l
\end{tikzcd} \tag{2.4}$$

Observe that all vertical arrows in the diagram (2.4) are injective. Let $R_{ij} := \frac{1}{l^k}Q_{ij} \in A\big(L_{l^k}\big(\frac{1}{l^k}\Gamma\big)\big) \subset A\big(L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)\big)$. The element $r_{w_1}(R_{ij})$ has order $l^{k+c_{ij}}$ in the group $A_{iw_1}(k_{w_1})_l$ because $l^{k+c_{ij}}r_{w_1}(R_{ij}) = l^{c_{ij}}r_w(Q_{ij}) = 0$. By the choice of w, we have $k_w = k_{w_2}$, hence $r_{w_1}(R_{ij})$ comes from an element of $A_{iw}(k_w)_l$. If $c_{ij} \geq 1$ then

$$h(l^{c_{ij}-1}r_{w_1}(R_{ij})) = (1 + l^k u)l^{c_{ij}-1}r_{w_1}(R_{ij})$$

since $l^{c_{ij}-1}r_{w_1}(R_{ij}) \in A_{iw}(k_w)[l^{k+1}]$. On the other hand, by the choice of w, Frobenius at w_1 acts on $l^{c_{ij}-1}r_{w_1}(R_{ij})$ via h. So $h(l^{c_{ij}-1}r_{w_1}(R_{ij})) = l^{c_{ij}-1}r_{w_1}(R_{ij})$ because $r_{w_1}(R_{ij}) \in A_{iw}(k_w)_l$. Hence, $l^{c_{ij}-1}ur_{w_1}(Q_{ij}) = 0$ but this is impossible since the order of $r_{w_1}(Q_{ij})$ is $l^{c_{ij}}$. Hence we must have $c_{ij} = 0$. ∎

THEOREM 2.7. *Let l be a prime number and let $m \in \mathbb{N} \cup \{0\}$. Let L/F be a finite extension, let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be arbitrary torsion elements for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$. There is a set of primes w of $\mathcal{O}_L$ of positive density such that*

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \quad \text{in } A_{iw}(k_w)_l$$

for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{iw}(k_{w'})$ is the corresponding reduction map.

Proof. This follows immediately from Theorem 2.6 by taking $L(A[l^m])$ for L and putting $Q_{ij} := P_{ij} - T_{ij}$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$. ∎

REMARK 2.8. Theorem 2.6 obviously follows from Theorem 2.7.

REMARK 2.9. We have recently learned that A. Perucca, using different methods, obtained analogous theorems to our Theorems 2.6 and 2.7, for the setting of semiabelian varieties [Pe1, Propositions 11 and 12].

3. Remarks on semisimple algebras and modules. In this section we recall some basic properties of modules over semisimple algebras which will be used in the proof of Theorem 4.1 in the next section. Let D be a division algebra and let $e \in \mathbb{N}$ be a fixed natural number. Denote by K_i the left ideal of $M_e(D)$ consisting of the ith column matrices

$$\boldsymbol{\alpha}_i := \begin{bmatrix} 0 & \dots & a_{1i} & \dots & 0 \\ 0 & \dots & a_{2i} & \dots & 0 \\ \vdots & \dots & \vdots & \dots & \vdots \\ 0 & \dots & a_{ei} & \dots & 0 \end{bmatrix}.$$

Let W be a D-vector space and let $e \in \mathbb{N}$ be a natural number. Then $W^e := \underbrace{W \times \dots \times W}_{e\,\text{times}}$ is an $M_e(D)$-module. For $\omega \in W$ put

$$\boldsymbol{\omega} := \begin{bmatrix} \omega \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in W^e.$$

The following lemma is elementary:

Lemma 3.1. *Every nonzero simple submodule of the $M_e(D)$-module W^e has the form*

$$K_1\boldsymbol{\omega} = \{\boldsymbol{\alpha}_1\boldsymbol{\omega} : \boldsymbol{\alpha}_1 \in K_1\} = \left\{ \begin{bmatrix} a_{11}\omega \\ a_{21}\omega \\ \vdots \\ a_{e1}\omega \end{bmatrix} : a_{i1} \in D,\ 1 \le i \le e \right\}$$

for some $\omega \in W$.

Let $e_i \in \mathbb{N}$ and let D_i be a division algebra for each $1 \le i \le t$. We will often use the following notation: $\mathbb{D} := \prod_{i=1}^t D_i$, $\mathrm{e} := (e_1, \dots, e_t)$ and $\mathbb{M}_{\mathrm{e}}(\mathbb{D}) := \prod_{i=1}^t M_{e_i}(D_i)$. If W_i is a vector space over D_i for each $1 \le i \le t$ then the space $W := \bigoplus_{i=1}^t W_i^{e_i}$ has a natural structure of $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$-module.

Corollary 3.2. *Every nonzero simple $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$-submodule of*

$$W = \bigoplus_{i=1}^{t} W_i^{e_i}$$

has the form

$$\begin{aligned} K(j)_1\boldsymbol{\omega}(j) &= \{\boldsymbol{\alpha}(j)_1\boldsymbol{\omega}(j) : \boldsymbol{\alpha}(j)_1 \in K(j)_1\} \\ &= \left\{ \begin{bmatrix} a_{11}\omega(j) \\ a_{21}\omega(j) \\ \vdots \\ a_{e_j1}\omega(j) \end{bmatrix} : a_{k1} \in D_j,\ 1 \le k \le e_j \right\} \end{aligned}$$

for some $1 \le j \le t$ and some $\omega(j) \in W_j$, where $K(j)_1 \subset M_{e_j}(D_j)$ denotes the left ideal of $M_{e_j}(D_j)$ which consists of the first column matrices.

Let D_i be a finite-dimensional division algebra over $\mathbb{Q}$ for every $1 \le i \le t$. The trace homomorphisms $\mathrm{tr}_i : M_{e_i}(D_i) \to \mathbb{Q}$, for all $1 \le i \le t$, give the trace homomorphism $\mathrm{tr} : \mathbb{M}_{\mathrm{e}}(\mathbb{D}) \to \mathbb{Q}$, where $\mathrm{tr} := \sum_{i=1}^t \mathrm{tr}_i$. Let W_i be a finite-dimensional D_i-vector space for each $1 \le i \le t$. Then $W = \bigoplus_{i=1}^t W_i^{e_i}$ is a finitely generated $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$-module. The homomorphism tr gives a natural map of $\mathbb{Q}$-vector spaces

$$\mathrm{tr} : \mathrm{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(W, \mathbb{M}_{\mathrm{e}}(\mathbb{D})) \to \mathrm{Hom}_{\mathbb{Q}}(W, \mathbb{Q}). \tag{3.1}$$

Lemma 3.3. *The map* (3.1) *is an isomorphism.*

Proof. For each $1 \le i \le t$ we have the trace map

$$\mathrm{tr}_i : \mathrm{Hom}_{M_{e_i}(D_i)}(W_i^{e_i}, M_{e_i}(D_i)) \to \mathrm{Hom}_{\mathbb{Q}}(W_i^{e_i}, \mathbb{Q}). \tag{3.2}$$

The map (3.1) is naturally compatible with the maps (3.2) via natural isomorphisms

$$\bigoplus_{i=1}^{t} \mathrm{Hom}_{M_{e_i}(D_i)}(W_i^{e_i}, M_{e_i}(D_i)) \cong \mathrm{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(W, \mathbb{M}_{\mathrm{e}}(\mathbb{D})), \tag{3.3}$$

$$\bigoplus_{i=1}^{t} \mathrm{Hom}_{\mathbb{Q}}(W_i^{e_i}, \mathbb{Q}) \cong \mathrm{Hom}_{\mathbb{Q}}(W, \mathbb{Q}). \tag{3.4}$$

In other words $\mathrm{tr} = \sum_{i=1}^t \mathrm{tr}_i$. Hence it is enough to prove the lemma for the maps (3.2). Since $M_{e_i}(D_i)$ is a simple ring for which every simple module is isomorphic to $K(i)_1$ it is enough to prove that

$$\mathrm{tr}_i : \mathrm{Hom}_{M_{e_i}(D_i)}(K(i)_1, M_{e_i}(D_i)) \cong \mathrm{Hom}_{\mathbb{Q}}(K(i)_1, \mathbb{Q}). \tag{3.5}$$

Notice that every map $\phi \in \mathrm{Hom}_{M_{e_i}(D_i)}(K(i)_1, M_{e_i}(D_i))$ is determined by the image of the element

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \in K(i)_1.$$

Since ϕ is an $M_{e_i}(D_i)$-module homomorphism we have

$$\phi\left(\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}\right) = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1e_i} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \tag{3.6}$$

for some $c_{11}, c_{12}, \dots, c_{1e_i} \in D_i$. The map (3.5) is injective (cf. [Re, Theorem 9.9]). From the definition of $K(i)_1$ and (3.6) it follows that the dimensions of the $\mathbb{Q}$-vector spaces $\mathrm{Hom}_{M_{e_i}(D_i)}(K(i)_1, M_{e_i}(D_i))$ and $\mathrm{Hom}_{\mathbb{Q}}(K(i)_1, \mathbb{Q})$ are equal. Hence (3.5) is an isomorphism. ∎

Remark 3.4. Since the algebra $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$ is semisimple, the module W is semisimple, so for every $\boldsymbol{\pi} \in \mathrm{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(W, \mathbb{M}_{\mathrm{e}}(\mathbb{D}))$ there is an $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$-homomorphism $\boldsymbol{s} : \mathrm{Im}\,\boldsymbol{\pi} \to W$ such that $\boldsymbol{\pi} \circ \boldsymbol{s} = \mathrm{id}$. Because of (3.3) we can write $\boldsymbol{\pi} = \prod_{i=1}^{t} \boldsymbol{\pi}(i)$ for some $\boldsymbol{\pi}(i) \in \mathrm{Hom}_{M_{e_i}(D_i)}(W_i^{e_i}, M_{e_i}(D_i))$. Note that $\mathrm{Im}\,\boldsymbol{\pi} = \prod_{i=1}^{t} \mathrm{Im}\,\boldsymbol{\pi}(i)$. For each $1 \le i \le t$ we can find an $M_{e_i}(D_i)$-homomorphism $\boldsymbol{s}(i) : \mathrm{Im}\,\boldsymbol{\pi}(i) \to W_i^{e_i}$ such that $\boldsymbol{\pi}(i) \circ \boldsymbol{s}(i) = \mathrm{id}$ and $\boldsymbol{s} = \bigoplus_{i=1}^{t} \boldsymbol{s}(i)$ because $M_{e_i}(D_i)$ is simple. By [Re, Theorem 7.3], every simple $M_{e_i}(D_i)$-submodule of $M_{e_i}(D_i)$ is isomorphic to $K(i)_1$. Since $\dim_{D_i} M_{e_i}(D_i) = e_i^2$ and $\dim_{D_i} K(i)_1 = e_i$ we see that $M_{e_i}(D_i)$ is a direct sum of e_i simple $M_{e_i}(D_i)$-submodules. Hence every $M_{e_i}(D_i)$-submodule of $M_{e_i}(D_i)$ is a direct sum of at most e_i simple $M_{e_i}(D_i)$-submodules.

4. Detecting linear dependence in Mordell–Weil groups.

The proof of the following theorem combines the approach of Weston [We] with our Theorem 2.7, the results of Section 3 and the approach from [B] concerning Riemann lattices. The main idea of proof is to replace the investigation of linear relations over $\mathbb{Z}$ by the investigation of linear relations over $\mathbb{M}_{\mathrm{e}}(\mathbb{D})$. To get the result one also needs a careful application of arithmetic in a noncommutative framework.

Theorem 4.1. *Let F'/F be a finite extension such that A is isogenous over F' to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i/F' simple, pairwise nonisogenous abelian varieties. Assume that $\dim_{\mathrm{End}_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \ge e_i$ for each $1 \le i \le t$, where $\mathrm{End}_{F'}(A_i)^0 := \mathrm{End}_{F'}(A_i) \otimes \mathbb{Q}$. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all primes v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{\mathrm{tor}}$. Moreover if $A(F)_{\mathrm{tor}} \subset \Lambda$, then the following conditions are equivalent:*

1. *$P \in \Lambda$,*
2. *$r_v(P) \in r_v(\Lambda)$ for almost all primes v of $\mathcal{O}_F$.*

Proof. Assume that $P \notin \Lambda$. This implies that $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l (cf. Remark 2.3). We can consider the equality (2.2) in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$ (cf. Remark 2.3). Since $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$, there is $1 \le j_0 \le s$ such that $\lambda^{m_1} \parallel n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for some natural numbers $m_1 < m_2$. Fix such an m_2, for example $m_2 = m_1 + 1$. Consider the map of $\mathbb{Z}$-modules

$$\pi : \Omega \to \mathbb{Z}, \qquad \pi(R) := \mu_{j_0},$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \le i \le s$. By abuse of notation denote also by π the map $\pi \otimes \mathbb{Q} : \Omega \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$. By Lemma 3.3 there is a map $\boldsymbol{\pi} \in \mathrm{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q}, \mathbb{M}_{\mathrm{e}}(\mathbb{D}))$ such that $\mathrm{tr}(\boldsymbol{\pi}) = \pi$. By Remark

3.4 there is $\boldsymbol{s} \in \operatorname{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(\operatorname{Im}\boldsymbol{\pi}, \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\boldsymbol{\pi} \circ \boldsymbol{s} = \mathrm{id}$. Moreover for all $1 \le i \le t$ there are $\boldsymbol{\pi}(i) \in \operatorname{Hom}_{M_{e_i}(D_i)}(\Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q}, M_{e_i}(D_i))$ and $\boldsymbol{s}(i) \in \operatorname{Hom}_{M_{e_i}(D_i)}(\operatorname{Im}\boldsymbol{\pi}(i), \Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\boldsymbol{\pi}(i) \circ \boldsymbol{s}(i) = \mathrm{id}$ and $\boldsymbol{\pi} = \prod_{i=1}^{t} \boldsymbol{\pi}(i)$, $\boldsymbol{s} = \prod_{i=1}^{t} \boldsymbol{s}(i)$. Moreover $\operatorname{Ker}\boldsymbol{\pi} = \prod_{i=1}^{t} \operatorname{Ker}\boldsymbol{\pi}(i)$ and we have $\Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \operatorname{Im}\boldsymbol{s}(i) \oplus \operatorname{Ker}\boldsymbol{\pi}(i)$ and $\Omega \otimes_{\mathbb{Z}} \mathbb{Q} \cong \operatorname{Im}\boldsymbol{s} \oplus \operatorname{Ker}\boldsymbol{\pi}$. By Lemma 3.1 we can represent $\operatorname{Im}\boldsymbol{s}(i)$ and $\operatorname{Ker}\boldsymbol{\pi}(i)$ as direct sums of simple $M_{e_i}(D_i)$-submodules as follows:

$$\operatorname{Im}\boldsymbol{s}(i) = \bigoplus_{k=1}^{k_i} K(i)_1 \boldsymbol{\omega}_k(i), \qquad \operatorname{Ker}\boldsymbol{\pi}(i) = \bigoplus_{k=k_i+1}^{u_i} K(i)_1 \boldsymbol{\omega}_k(i).$$

Let $p_i = \dim_{\operatorname{End}_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q})$. Observe that $k_i \le e_i \le p_i$ for every $1 \le i \le t$. It is easy to observe that the elements $\omega_1(i), \ldots, \omega_{k_i}(i), \ldots, \omega_{u_i}(i)$ give a basis of the D_i-vector space $\Omega_i \otimes_{\mathbb{Z}} \mathbb{Q}$. We can assume without loss of generality that $\omega_{k_i+1}(i), \ldots, \omega_{u_i}(i) \in \Omega_i$. Tensoring the map π with $\mathcal{O}_K$ we will denote the resulting map $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K \to \mathcal{O}_K$ also by π. Similarly tensoring the maps $\boldsymbol{\pi}(i)$ and $\boldsymbol{s}(i)$ with K we get $M_{e_i}(D_i) \otimes_{\mathbb{Q}} K$-linear homomorphisms $\Omega_i^{e_i} \otimes_{\mathbb{Z}} K \to M_{e_i}(D_i) \otimes_{\mathbb{Q}} K$ and $\operatorname{Im}\boldsymbol{\pi}(i) \to \Omega_i^{e_i} \otimes_{\mathbb{Z}} K$ also denoted by $\boldsymbol{\pi}(i)$ and $\boldsymbol{s}(i)$ respectively. Note that for each $1 \le i \le t$ the K-vector space $\Omega_i \otimes_{\mathbb{Z}} K$ is a free $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$-module. Recall that $\mathcal{R} \subset \mathbb{M}_{\mathrm{e}}(\mathbb{D})$, $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{M}_{\mathrm{e}}(\mathbb{D})$ and Ω is a finitely generated $\mathcal{R}$-module. Hence there is a natural number M_0 such that the following homomorphisms of $\mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_K$-modules are well defined:

$$M_0\boldsymbol{\pi} : \Omega \otimes_{\mathbb{Z}} \mathcal{O}_K \to \mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_K, \qquad \boldsymbol{s} : M_0\boldsymbol{\pi}(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K) \to \Omega \otimes_{\mathbb{Z}} \mathcal{O}_K.$$

We can restrict the trace homomorphism to $\mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_K \subset D \otimes_{\mathbb{Q}} K$ to get an $\mathcal{O}_K$-linear homomorphism $\mathrm{tr} : \mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_K \to K$. Note that $\mathrm{tr}\, M_0\boldsymbol{\pi} = M_0\pi$ and $M_0\boldsymbol{\pi} \circ \boldsymbol{s} = M_0\, \mathrm{id}_{M_0\boldsymbol{\pi}(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K)}$. Consider now the module of the first column matrices $K(i)_1 \subset M_{e_i}(\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_K)$. Define the $M_{e_i}(\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_K)$-module

$$\boldsymbol{\Gamma}(i) := \sum_{k=1}^{k_i} K(i)_1 M_0 \boldsymbol{\omega}_k(i) + \sum_{k=k_i+1}^{u_i} K(i)_1 \boldsymbol{\omega}_k(i) \subset \Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathcal{O}_K$$

and the $\mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_K$-module $\boldsymbol{\Gamma} := \bigoplus \boldsymbol{\Gamma}(i) \subset \Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$. Put $M_2 := [\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K : \boldsymbol{\Gamma}]$ and $M_3 := [\boldsymbol{\Gamma} : M_2 \Omega \otimes_{\mathbb{Z}} \mathcal{O}_K]$. The choice of j_0 yields $\pi(P) \notin \pi(\Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda)$ $+ \lambda^m \pi(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_\lambda)$ for every $m \ge m_2$. Fix any such m for the rest of the proof. Hence

$$M_0\boldsymbol{\pi}(P) \notin M_0\boldsymbol{\pi}(\Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda) + M_0 \lambda^m \boldsymbol{\pi}(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_\lambda) \tag{4.1}$$

because $\mathrm{tr}\, M_0\boldsymbol{\pi} = M_0\pi$. Put $K(i)_{1,\lambda} := K(i)_1 \otimes_{\mathcal{O}_K} \mathcal{O}_\lambda \subset M_{e_i}(\mathcal{R}_{i,\lambda})$, where $\mathcal{R}_{i,\lambda} := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$. Let $Q \in \Lambda$ be an arbitrary element. We can write

$$M_2(P\otimes 1)=\sum_{i=1}^{t}\sum_{k=1}^{k_i}\boldsymbol{\alpha}_k(i)_1 M_0\boldsymbol{\omega}_k(i)+\sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i}\boldsymbol{\alpha}_k(i)_1\boldsymbol{\omega}_k(i),$$

$$M_2(Q\otimes 1)=\sum_{i=1}^{t}\sum_{k=1}^{k_i}\boldsymbol{\beta}_k(i)_1 M_0\boldsymbol{\omega}_k(i)+\sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i}\boldsymbol{\beta}_k(i)_1\boldsymbol{\omega}_k(i),$$

for some $\boldsymbol{\alpha}_k(i)_1,\boldsymbol{\beta}_k(i)_1\in K(i)_{1,\lambda}$ with $1\le k\le u_i$ and $1\le i\le t$. Then

$$M_0\boldsymbol{\pi}(M_2(P\otimes 1-Q\otimes 1))=M_0^2\prod_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1-\boldsymbol{\beta}_k(i)_1)\boldsymbol{\pi}(\boldsymbol{\omega}_k(i)).\tag{4.2}$$

Since $\boldsymbol{\pi}=\prod_{i=1}^{t}\boldsymbol{\pi}(i)$ maps the module $\Omega\otimes_{\mathbb{Z}}\mathbb{Q}=\bigoplus_{i=1}^{t}\Omega_i^{e_i}\otimes_{\mathbb{Z}}\mathbb{Q}$ into the ring $\mathbb{M}_{\mathrm{e}}(\mathbb{D})=\prod_{i=1}^{t}M_{e_i}(D_i)$ componentwise, we replaced $\sum_{i=1}^{t}$ by $\prod_{i=1}^{t}$. Hence (4.1) and (4.2) give $M_0^2\prod_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1-\boldsymbol{\beta}_k(i)_1)\boldsymbol{\pi}(\boldsymbol{\omega}_k(i))\notin\lambda^m M_0\boldsymbol{\pi}(M_2\Omega\otimes_{\mathbb{Z}}\mathcal{O}_\lambda)$, so

$$M_0^2\prod_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1-\boldsymbol{\beta}_k(i)_1)\boldsymbol{\pi}(\boldsymbol{\omega}_k(i))\notin\lambda^m M_0\boldsymbol{\pi}(M_3\boldsymbol{\Gamma}).\tag{4.3}$$

Hence for some $1\le i\le t$ and $1\le k\le k_i$ we obtain

$$\boldsymbol{\alpha}_k(i)_1-\boldsymbol{\beta}_k(i)_1\notin\lambda^m M_3K(i)_{1,\lambda}.\tag{4.4}$$

Recall from Section 2 that ϵ denotes the ramification index of the prime ideal $\lambda\subset\mathcal{O}_K$ over l. Observe that $A_i[\lambda^{\epsilon n}]\cong\mathcal{L}_i\otimes_{\mathbb{Z}}\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}_i\otimes_{\mathbb{Z}}\mathcal{O}_\lambda$ for every $n\in\mathbb{N}$ because $l\mathcal{O}_K=\prod_{\lambda|l}\lambda^\epsilon$, $A_i[l^n]\cong\mathcal{L}_i\otimes_{\mathbb{Z}}\mathbb{Z}_l/l^n\mathcal{L}_i\otimes_{\mathbb{Z}}\mathbb{Z}_l$ and $A_i[l^n]=\bigoplus_{\lambda|l}A_i[\lambda^{\epsilon n}]$. Recall that we chose, for each $1\le i\le t$, a lattice $\mathcal{L}_i'\subset\mathcal{L}_i$ such that $\mathcal{L}_i'$ is a free $\mathcal{R}_i$-module. Let $M_4:=\max_{1\le i\le t}[\mathcal{L}_i:\mathcal{L}_i']$. Put $\mathcal{L}:=\bigoplus_{i=1}^{t}\mathcal{L}_i$ and $\mathcal{L}':=\bigoplus_{i=1}^{t}\mathcal{L}_i'$. By the Snake Lemma the kernel of the following natural map of $\mathcal{O}_\lambda$-modules is finite and annihilated by $\lambda^{\epsilon m_4}$:

$$z(n,\lambda):\mathcal{L}'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda\to\mathcal{L}\otimes_{\mathbb{Z}}\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}\otimes_{\mathbb{Z}}\mathcal{O}_\lambda,\tag{4.5}$$

where $l^{m_4}\,\|\,M_4$. Let m_0 and m_3 denote the natural numbers with $l^{m_0}\,\|\,M_0$ and $l^{m_3}\,\|\,M_3$. Let $\eta_1(i),\dots,\eta_{p_i}(i)$ be a basis of $\mathcal{L}_i'$ over $\mathcal{R}_i$. Recall that we denoted by p_i the natural number $\dim_{\mathrm{End}_{F'}(A_i)^0}H_1(A_i(\mathbb{C});\mathbb{Q})$. Since $\mathcal{L}_i'$ is a free $\mathcal{R}_i$-module and $H_1(A_i(\mathbb{C});\mathbb{Q})=\mathcal{L}_i\otimes\mathbb{Q}$, it follows that the quotient $\mathcal{L}_i'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}_i'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda$ is a free $\mathcal{R}_{i,\lambda}/\lambda^{\epsilon n}\mathcal{R}_{i,\lambda}$-module with basis $\overline{\eta_1(i)},\dots,\overline{\eta_{p_i}(i)}$. Here $\overline{\eta_k(i)}$ denotes the image of $\eta_k(i)$ in $\mathcal{L}'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}'\otimes_{\mathbb{Z}}\mathcal{O}_\lambda$ for each $1\le k\le p_i$. By the assumptions, $p_i\ge e_i$. Let $T_k(i)$ be the image of $\overline{\eta_k(i)}$ via the map $z(n,\lambda)$ for all $1\le i\le t$ and $1\le k\le p_i$. Take $n\in\mathbb{N}$ such that $\epsilon n>m+\epsilon m_0+\epsilon m_3+\epsilon m_4$ and put $L:=F(A[l^n])=F(r(A)[l^n])$. Observe that $A[l^n]\subset A(L)$. By Theorem 2.7 there is a set of primes w of $\mathcal{O}_L$ of positive density such that $r_w(\omega_k(i))=0$ for $1\le i\le t$, $k_i+1\le k\le u_i$ and $r_w(\omega_k(i))=r_w(T_k(i))$ for all $1\le i\le t$,

$1 \le k \le k_i$. Choose such a prime w. Since $r_w(P) \in r_w(\Lambda)$ we take $Q \in \Lambda$ such that $r_w(P) = r_w(Q)$. Applying the reduction map r_w to the equation

$$M_2(P-Q) = \sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)M_0\boldsymbol{\omega}_k(i) + \sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)\boldsymbol{\omega}_k(i),$$

we obtain

$$0 = \sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)M_0 r_w(\boldsymbol{T}_k(i)).$$

Since the map r_w is injective on the l-torsion subgroup of $A(L)$ ([HS, Theorem C.1.4, p. 263], [K, pp. 501–502]) we obtain

$$0 = \sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)M_0\boldsymbol{T}_k(i).$$

Therefore $\sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)M_0\overline{\boldsymbol{\eta}}_k(i) \in \operatorname{Ker} z(n,\lambda)$. Hence, the element $\lambda^{\epsilon m_0+\epsilon m_4}\sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)\boldsymbol{\eta}_k(i)$ maps to zero in the $\mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{O}_\lambda$-module $\mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda/\lambda^{\epsilon n}\mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$. Hence

$$\sum_{i=1}^{t}\sum_{k=1}^{k_i}(\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1)\boldsymbol{\eta}_k(i) \in \lambda^{\epsilon n-\epsilon m_0-\epsilon m_4}\mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda.$$

Since $\eta_1(i), \ldots, \eta_{p_i}(i)$ is a basis of $\mathcal{L}'_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ over $\mathcal{R}_{i,\lambda}$, we obtain

$$\boldsymbol{\alpha}_k(i)_1 - \boldsymbol{\beta}_k(i)_1 \in \lambda^{\epsilon n-\epsilon m_0-\epsilon m_4}K(i)_{1,\lambda} \tag{4.6}$$

for all $1 \le i \le t$ and $1 \le k \le k_i$. But (4.6) contradicts (4.4) because we chose n such that $\epsilon n - \epsilon m_0 - \epsilon m_4 > m + \epsilon m_3$. ■

Corollary 4.2 (Weston [We, p. 77]). *Let A be an abelian variety defined over a number field such that $\operatorname{End}_{\overline{F}}(A)$ is commutative. Then Theorem 4.1 holds for A.*

Proof. Since $\operatorname{End}_{\overline{F}}(A)$ is commutative, A is isogenous to $A_1 \times \cdots \times A_t$ with A_i simple, pairwise nonisogenous. In this case the assumption in Theorem 4.1, $\dim_{\operatorname{End}_{F'}(A_i)^0} H_1(A_i(\mathbb{C});\mathbb{Q}) \ge 1$ for each $1 \le i \le t$, always holds. ■

Corollary 4.3. *Let $A = E_1^{e_1} \times \cdots \times E_t^{e_t}$, where $E_1, \ldots, E_t$ are pairwise nonisogenous elliptic curves defined over F. Assume that $1 \le e_i \le 2$ if $\operatorname{End}_F(E_i) = \mathbb{Z}$ and $e_i = 1$ if $\operatorname{End}_F(E_i) \ne \mathbb{Z}$. Then Theorem 4.1 holds for A.*

Proof. Observe that for an elliptic curve E/F we have

$$\dim_{\mathrm{End}_F(E)^0} H_1(E(\mathbb{C});\mathbb{Q}) = \begin{cases} 2 & \text{if } \mathrm{End}_F(E) = \mathbb{Z}, \\ 1 & \text{if } \mathrm{End}_F(E) \neq \mathbb{Z}. \end{cases} \blacksquare$$

REMARK 4.4. Theorem 4.1 and in particular Corollary 4.3 answer the question of T. Weston [We, p. 77] concerning the noncommutative endomorphism algebra case. In the special case of the commutative endomorphism algebra our methods are similar to Weston's [We], but we have also used some different techniques which gave us important insights on how to deal with the noncommutative case.

REMARK 4.5. The assumption that $e_i \leq p_i$ for all i in Theorem 4.1 cannot be omitted. The inequality $p_i < e_i$ for an i makes $k_i > p_i$ possible. But in this case the key property (4.6) cannot be obtained and our argument breaks down. In the next section we will see that for some abelian surfaces for which the assumption $e_i \leq p_i$ does not hold we can construct explicit counterexamples to the problem of detecting linear dependence.

5. Counterexamples to the problem of detecting linear dependence via reduction maps. The hypothesis in Theorem 4.1 that A is isogenous over F' to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with $\dim_{\mathrm{End}_{F'}(A_i)^0} H_1(A_i(\mathbb{C});\mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$ cannot be omitted. In fact in Proposition 5.6 we produce counterexamples to the problem of detecting linear dependence. Our basic conterexamples concern abelian surfaces that are products of two CM elliptic curves. Of course taking products of abelian varieties with our abelian surfaces produces counterexamples to this problem for abelian varieties in each dimension ≥ 2. The idea of the proof of Proposition 5.6 is based on the counterexample of A. Schinzel [Sch, p. 419] for the product of two $\mathbb{G}_{\mathrm{m}}$'s. A. Schinzel produces a counterexample to the statement that a system of exponential equations is soluble in integers if and only if it is soluble modulo p for every prime p. His counterexample is based on the following system of exponential congruences:

$$2^x 3^y \equiv 1 \bmod p, \qquad 2^y 3^z \equiv 4 \bmod p, \tag{5.1}$$

which has a solution for every p (see [Sch] for details). On the other hand it is clear that the system of exponential equations:

$$2^x 3^y = 1, \qquad 2^y 3^z = 4$$

has no integral solution.

REMARK 5.1. The methods of the proof of Theorem 4.1 work for algebraic tori over a number field F. Let T/F be an algebraic torus and let F'/F be a finite extension that splits T. Hence $T \otimes_F F' \cong \mathbb{G}_{\mathrm{m}}^e$ where $\mathbb{G}_{\mathrm{m}} := \operatorname{spec} F'[t, t^{-1}]$. For any field extension $F' \subset M \subset \overline{F}$ we have $\mathrm{End}_M(\mathbb{G}_{\mathrm{m}}) = \mathbb{Z}$

and $H_1(\mathbb{G}_{\mathrm{m}}(\mathbb{C});\mathbb{Z}) = \mathbb{Z}$. Hence the condition:

$$e \leq \dim_{\mathrm{End}_{F'}(\mathbb{G}_{\mathrm{m}})^0} H_1(\mathbb{G}_{\mathrm{m}}(\mathbb{C});\mathbb{Q}) = 1,$$

analogous to the corresponding condition of Theorem 4.1, means that $e = 1$.

Remark 5.2. The analogue of Theorem 4.1 for one-dimensional tori is basically [Sch, Theorem 2]. Observe that torsion ambiguity that appears in Theorem 4.1 can be removed in the case of one-dimensional tori by use of an argument similar to the proof of [BGK2, Theorem 3.12].

The case of abelian varieties. Let $E := E_d$ be the elliptic curve over $\mathbb{Q}$ given by the equation $y^2 = x^3 - d^2x$. It has CM by $\mathbb{Z}[i]$. It has been shown that the rank of $E_d(\mathbb{Q})$ can reach 6 (see [RS, Table 2, p. 464]). For example the rank of $E_{1254}(\mathbb{Q})$ is 3. From now on we assume that the rank of $E_d(\mathbb{Q})$ is at least 2.

Lemma 5.3. *For every $d > 1$ and for each $p \nmid 2d$ the group $E_p(\mathbb{F}_p)$ does not have p-torsion.*

Proof. For each $d > 1$ we have $E[2] \subset E(\mathbb{Q})$. Hence by [Sil1, Prop. 3.1, p. 176], the group $E[2]$ injects into $E_p(\mathbb{F}_p)$ by the reduction map r_p for every $p \nmid 2d$. Hence $4 \mid |E_p(\mathbb{F}_p)|$ for this p. On the other hand by the Theorem of Hasse we have $|E_p(F_p)| < p + 1 + 2\sqrt{p}$, which implies that $|E_p(F_p)| < 4p$ for every $p \geq 3$. This implies that p does not divide $|E_p(\mathbb{F}_p)|$ whenever $p \nmid 2d$. ■

Consider now the curve E_d over $\mathbb{Q}(i)$. It is easy to observe that

$$\mathrm{rank}_{\mathbb{Z}}\, E_d(\mathbb{Q}(i)) = 2\,\mathrm{rank}_{\mathbb{Z}}\, E_d(\mathbb{Q}).$$

Lemma 5.4. *Let $E/\mathbb{Q}(i) := E_d/\mathbb{Q}(i)$. Let p be any prime such that $p \nmid 2d$. Let v denote a prime of $\mathbb{Z}[i]$ over p. There is an element $\gamma(v) \in \mathbb{Z}[i]$ such that*

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v).$$

Proof. Let v denote a prime over p for each $p \nmid 2d$. If p splits completely in $\mathbb{Q}(i)/\mathbb{Q}$ then $k_v = \mathbb{F}_p$. In this case $E_v(k_v) = E_p(\mathbb{F}_p)$ and $E_v(k_v)$ does not have p-torsion by Lemma 5.3. If p is inert in $\mathbb{Q}(i)/\mathbb{Q}$, then by use of [Sil1, Theorem 4.1, Chap. V], cf. p. 309 loc. cit., we observe that E_v is supersingular, hence $E_v(k_v)$ does not have p-torsion by the theorem of Deuring [De] (cf. [Sil1, Theorem 3.1, p. 137]). Note that $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z}[i]$. Hence $E(\overline{\mathbb{Q}(i)})_{\mathrm{tor}} \cong \mathbb{Q}(i)/\mathbb{Z}[i]$. On the other hand the reduction map gives a natural isomorphism

$$E(\overline{\mathbb{Q}(i)})_{\mathrm{tor}\neq p} \cong E_v(\overline{k_v})_{\mathrm{tor}\neq p}.$$

Hence we can identify $E_v(k_v)$ with a subgroup of $E[c] \cong \frac{1}{c}\mathbb{Z}[i]/\mathbb{Z}[i]$ for some $c \in \mathbb{Z}[i]$ with $c \nmid p$. Note that in our case $E_v(k_v)$ is the fixed points of $\mathrm{Fr}_v \in G(\overline{k_v}/k_v)$ acting on $E_v(\overline{k_v})_{\mathrm{tor}\neq p}$. Hence $E_v(k_v)$ is a cyclic $\mathbb{Z}[i]$-submodule of the cyclic $\mathbb{Z}[i]$-module $E[c]$. So for each $p \nmid 2d$ there is a $\gamma(v) \in \mathbb{Z}[i]$ such that $E_v(k_v)$ is precisely the subgroup of $E[c]$ annihilated by multiplication by $\gamma(v)$. Thus for each $p \nmid 2d$ we have $E_v(k_v) \cong \frac{1}{\gamma(v)}\mathbb{Z}[i]/\mathbb{Z}[i] \cong \mathbb{Z}[i]/\gamma(v)$. Hence $E_v(k_v)$ has a cyclic $\mathbb{Z}[i]$-module structure. ∎

We consider the abelian surface $A_d := E_d \times E_d = E_d^2$ over $\mathbb{Q}(i)$.

Remark 5.5. For the surface A_d one has $e = 2 > \dim_{\mathbb{Q}(i)} H_1(E_d(\mathbb{C});\mathbb{Q}) = 1$. Hence A is just outside of the family of abelian varieties considered in Theorem 4.1.

In the proposition below we present a counterexample to the problem of detecting linear dependence for abelian varieties.

Proposition 5.6. *There is a nontorsion point $P \in A_d(\mathbb{Q}(i))$ and a free $\mathbb{Z}[i]$-module $\Lambda \subset A_d(\mathbb{Q}(i))$ such that $P \notin \Lambda$ and $r_v(P) \in r_v(\Lambda)$ for all primes $v \nmid 2d$ in $\mathbb{Z}[i]$.*

Proof. By our assumption that the rank of $E_d(\mathbb{Q})$ is at least 2, we can find two points $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ independent over $\mathbb{Z}[i]$. Let $P, P_1, P_2, P_3 \in A(\mathbb{Q}(i))$ be defined as follows:

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \quad P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \quad P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \quad P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

Let $\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$. We observe that Λ is free over $\mathbb{Z}[i]$, hence also free over $\mathbb{Z}$. However Λ is not free over $\operatorname{End}_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$. Moreover it is clear that $P \notin \Lambda$.

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$, $\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$. We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$. The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0, \qquad r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}.$$

Because $E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v)$, there are $c_1, c_2 \in \mathbb{Z}[i]$ such that via this isomorphism we can make the identifications $\overline{Q_1} = c_1 \bmod \gamma(v)$ and $\overline{Q_2} = c_2 \bmod \gamma(v)$. Hence the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1c_1 + r_2c_2 \equiv 0 \bmod \gamma(v), \qquad r_2c_1 + r_3c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution. Therefore assume that $c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$. Let $D := \gcd(c_1, c_2)$. Then it is easy to check that

$$\gcd(c_1^2/D, c_2) = D,$$

and since $D \mid c_1$ it follows that the equation $rc_1^2/D + r_3c_2 = c_1$ has a solution in $r, r_3 \in \mathbb{Z}[i]$. Putting

$$r_1 := -rc_2/D, \qquad r_2 := rc_1/D$$

we find that $r_1, r_2, r_3 \in \mathbb{Z}[i]$ satisfy the above system of congruences. ∎

6. Detecting linear dependence via a finite number of reductions. Let A/F be an abelian variety defined over a number field F. Let

$$\beta_H : A(F) \otimes_{\mathbb{Z}} \mathbb{R} \times A(F) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$$

be the height pairing defined by the canonical height function on A (cf. [HS], [Sil2]). It is known (loc. cit.) that β_H is a positive definite, symmetric bilinear form. Moreover if $R \in A(F)$ then $\beta_H(R, R) = 0$ iff R is a torsion point.

For our purposes, as explained in Section 2, we will assume that $\Lambda \subset \Omega$, where $\Omega := cA(F)$.

LEMMA 6.1. *Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$ such that $\Lambda \subset \Omega$. Let r denote the rank of Λ. Let $P_1, \ldots, P_r, \ldots, P_s$ be a $\mathbb{Z}$-basis of Ω such that $\Lambda = \mathbb{Z}d_1P_1 + \cdots + \mathbb{Z}d_rP_r$. Then the determination of whether $P \in \Lambda$ or not requires checking only a finite number of tuples $(n_1, \ldots, n_r)$.*

Proof. For any $P \in A(F)$ we can write

$$cP = \sum_{i=1}^{s} n_i P_i. \tag{6.1}$$

We get

$$c^2 \beta_H(P, P) = \sum_{i,j} n_i n_j \beta_H(P_i, P_j). \tag{6.2}$$

Since $\beta_H(P, P) > 0$ and β_H is positive definite, there is a constant C which depends only on the points $P, P_1, \ldots, P_s$ such that

$$|n_i| \le C \quad \text{for all } 1 \le i \le s. \tag{6.3}$$

Hence if $P \in \Lambda$ then $P = \sum_{i=1}^{r} k_i d_i P_i$ for some $k_1, \ldots, k_r \in \mathbb{Z}$. It follows that $|d_i k_i| \le C$, so $|k_i| \le C/d_i \le C$ for each $1 \le i \le r$. Hence, one needs to check only a finite number, in fact not larger than $(2C+1)^r$, of tuples $(n_1, \ldots, n_r)$ to determine whether $P \in \Lambda$ or not. ∎

We will apply Lemma 6.1 in the proof of Theorem 6.4.

THEOREM 6.2. *Let $A = A_1 \times \cdots \times A_t$ be a product of simple, pairwise nonisogenous abelian varieties. Let l be a prime number and let $Q_{ij} \in A_i(L)$ for $1 \le j \le r_i$ be independent over $\mathcal{R}_i$ for each $1 \le i \le t$. Let L/F be a finite extension and $L_{l^m} := L(A[l^m])$. Let k be a natural number such that the image of $\overline{\rho}_{l^{k+1}} : G_{L_{l^k}} \to GL_{\mathbb{Z}/l^{k+1}}(A[l^{k+1}])$ contains a nontrivial homothety and $L_{l^k}\big(\frac{1}{l^k}\Gamma\big) \cap L_{l^{k+1}} = L_{l^k}$. Let d be the discriminant of $L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/\mathbb{Q}$.*

There are effectively computable constants b_1 and b_2 such that $r_w(Q_{ij}) = 0$ in $A_{iw}(k_w)_l$ for all $1 \le j \le r_i$ and $1 \le i \le t$ for some prime w of $\mathcal{O}_L$ such that $N_{L/\mathbb{Q}}(w) \le b_1 d^{b_2}$.

Proof. We argue as in the proof of Theorem 2.6 but instead of using the classical Chebotarev theorem we use the effective Chebotarev theorem [LO, p. 416]. Namely our assumption on k gives $h \in G(L_{l^\infty}/L_{l^k})$ which acts on $A[l^{k+1}]$ as a homothety $1 + l^k u$ with $u \in \mathbb{Z}_l^\times$ and gives an element $\sigma \in G\big(L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/L\big)$ such that $\sigma_{|L_{l^k}(\frac{1}{l^k}\Gamma)} = \mathrm{id}$ and $\sigma_{|L_{l^{k+1}}} = h$ (cf. Step 1 of the proof of Theorem 2.6). Now by the effective Chebotarev theorem there is a prime w of $\mathcal{O}_L$ such that $N_{L/\mathbb{Q}}(w) \le b_1 d^{b_2}$ and a prime w_1 in $\mathcal{O}_{L_{l^{k+1}}(\frac{1}{l^k}\Gamma)}$ over w whose Frobenius in $L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/L$ is equal to σ. Using this choice of w and w_1 we finish the proof by the same argument as in Step 2 of the proof of Theorem 2.6. ∎

Theorem 6.3. *Let $A = A_1 \times \cdots \times A_t$ be a product of simple, pairwise nonisogenous abelian varieties. Let l be a prime number and let $m \in \mathbb{N} \cup \{0\}$. Let L/F be a finite extension, let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be arbitrary torsion elements for all $1 \le j \le r_i$ and $1 \le i \le t$. Let $k \ge m$ be a natural number such that the image of $\overline{\rho}_{l^{k+1}} : G_{L_{l^k}} \to GL_{\mathbb{Z}/l^{k+1}}(A[l^{k+1}])$ contains a nontrivial homothety and $L_{l^k}\big(\frac{1}{l^k}\Gamma\big) \cap L_{l^{k+1}} = L_{l^k}$. Let d be the discriminant of $L_{l^{k+1}}\big(\frac{1}{l^k}\Gamma\big)/\mathbb{Q}$. There are effectively computable constants b_1 and b_2 and there is a prime w of $\mathcal{O}_L$ such that $N_{L/\mathbb{Q}}(w) \le b_1 d^{b_2}$ and*

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \quad \text{in } A_{iw}(k_w)_l$$

for all $1 \le j \le r_i$ and $1 \le i \le t$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{iw}(k_{w'})$ is the reduction map.

Proof. Follows immediately from Theorem 6.2 in the same way as Theorem 2.7 follows from Theorem 2.6. ∎

Effective computation of constants in the Lagarias–Odlyzko theorem is difficult (cf. [Se, Sections 2.2–2.5]). However, under the assumption of the generalized Riemann hypothesis J.-P. Serre proved $N_{L/\mathbb{Q}}(w) \le 70(\log d_L)^2$ ([Se, Théorème 5]). Assuming GRH, one can also get rid of the discriminant d_L and obtain the following inequality ([Se, Théorème 6]): $N_{L/\mathbb{Q}}(w) \le 280n^2(\log n + \sum_{q \in S} \log q)^2$, where $n = [L : Q]$ and S is the finite set of rational primes that ramify in L.

Theorem 6.4. *Let A/F satisfy the hypotheses of Theorem 4.1. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. There is a finite set S^{fin} of primes v of $\mathcal{O}_F$, depending on A, P, Λ and also on the basis $P_1, \ldots, P_s$ of $A(F)$, such that the following condition holds: if $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{\mathrm{fin}}$ then*

$P \in \Lambda + A(F)_{\mathrm{tor}}$. *Hence if* $A(F)_{\mathrm{tor}} \subset \Lambda$ *then the following conditions are equivalent:*

(1) $P \in \Lambda$,
(2) $r_v(P) \in r_v(\Lambda)$ *for all* $v \in S^{\mathrm{fin}}$.

Proof. To construct S^{fin} we will carefully analyze the proof of Theorem 4.1. Notice that in the proof we used, in fact, the existence of a prime w satisfying the assertion of Theorem 2.7. Now we will apply Theorem 6.3 instead of Theorem 2.7 in order to obtain an appropriate contradiction. The finiteness of S^{fin} will follow by application of both the canonical height function and the Theorem of Lagarias and Odlyzko [LO, p. 416]. By explanation similar to that in Section 2 we can assume that $P \in \Omega$ and $\Lambda \subset \Omega$. Clearly, we can assume that $P \neq 0$. Consider the projections $\pi_j : \Omega \to \mathbb{Z}$, $\pi_j(R) = \mu_j$, $j = 1, \ldots, s$, for $R = \sum_{j=1}^{n} \mu_j P_j$. In the same way as in the proof of Theorem 4.1 we construct for each π_j the homomorphism $\boldsymbol{\pi}_j \in \mathrm{Hom}_{\mathbb{M}_{\mathrm{e}}(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q}, \mathbb{M}_{\mathrm{e}}(\mathbb{D}))$ such that $\mathrm{tr}(\boldsymbol{\pi}_j) = \pi_j$. As in the proof of Theorem 4.1, we construct the maps $\boldsymbol{s}_j$, $\boldsymbol{\pi}(i)_j$, $\boldsymbol{s}(i)_j$, where $\boldsymbol{\pi}_j = \prod_{i=1}^{t} \boldsymbol{\pi}(i)_j$, $\boldsymbol{s}_j = \prod_{i=1}^{t} \boldsymbol{s}(i)_j$. Moreover $\mathrm{Ker}\, \boldsymbol{\pi}_j = \prod_{i=1}^{t} \mathrm{Ker}\, \boldsymbol{\pi}(i)_j$. Next we construct the number $M_{0,j}$ and the lattice

$$\boldsymbol{\Gamma}(i)_j := \sum_{k=1}^{k_{i,j}} M_{0,j} \mathcal{R}_i \boldsymbol{\omega}_k(i)_j + \sum_{k=k_{i,j}+1}^{u_{i,j}} \mathcal{R}_i \boldsymbol{\omega}_k(i)_j \subset \Omega_i \otimes_{\mathbb{Z}} \mathcal{O}_K$$

and then the lattice $\boldsymbol{\Gamma}_j := \bigoplus_{i=1}^{t} \boldsymbol{\Gamma}(i)_j$. Then we define $M_{2,j} := [\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K : \boldsymbol{\Gamma}_j]$ and $M_{3,j} := [\boldsymbol{\Gamma}_j : M_{2,j} \Omega \otimes_{\mathbb{Z}} \mathcal{O}_K]$. For $n_j \neq 0$ in the decomposition (2.2) of P we consider every $l \mid n_j$ and every $\lambda \mid l$ and consider the ramification index $\epsilon_{j,\lambda}$ of λ over l. Next we define $m_{1,j,\lambda}$ such that $\lambda^{m_{1,j,\lambda}} \parallel n_j$. We put $m_{2,j,\lambda} := m_{1,j,\lambda} + 1$ and $m_{j,\lambda} := m_{2,j,\lambda} + 1$. Following the proof of Theorem 4.1 we also construct the constant M_4 which is clearly independent of j. We define the nonnegative integers $m_{0,j}, m_{3,j}, m_4$ with $l^{m_{0,j}} \parallel M_{0,j}$, $l^{m_{3,j}} \parallel M_{3,j}$ and $l^{m_4} \parallel M_4$. Put $m_{j,l} := \max_{\lambda \mid l} m_{j,\lambda}$ and $\epsilon_{j,l} := \max_{\lambda \mid l} \epsilon_{j,\lambda}$. Now, we choose the number $n_{j,l}$ in such a way that the image of the representation

$$\overline{\rho}_{l^{n_{j,l}+1}} : G_{L_{l^{n_{j,l}}}} \to GL_{\mathbb{Z}/l^{n_{j,l}+1}}(A[l^{n_{j,l}+1}])$$

contains a nontrivial homothety, $L_{l^{n_{j,l}}}\left(\frac{1}{l^{n_{j,l}}}\Gamma\right) \cap L_{l^{n_{j,l}+1}} = L_{l^{n_{j,l}}}$ and $n_{j,l} > \epsilon_{j,l} m_{0,j} + \epsilon_{j,l} m_4 + m_{j,l} + \epsilon_{j,l} m_{3,j}$. The last inequality guarantees that $\epsilon_{j,\lambda} n_{j,l} > \epsilon_{j,\lambda} m_{0,j} + \epsilon_{j,\lambda} m_4 + m_{j,\lambda} + \epsilon_{j,\lambda} m_{3,j}$. Eventually, we construct for each $1 \leq j \leq s$ and for each prime number $l \mid \pi_j(P)$ the number field

$$L_{j,l} := F\left(r(A)[l^{n_{j,l}+1}], \frac{1}{l^{n_{j,l}}} \boldsymbol{\Gamma}_j\right),$$

where $r(A)$ is the radical of A defined in Section 2. Observe that there are only a finite number of primes l considered above by the estimation of coefficients (6.3). By the Theorem of Lagarias and Odlyzko [LO, p. 416] there are effectively computable constants b_1 and b_2 such that every element $\sigma \in G(L_{j,l}/F)$ is equal to the Frobenius element $\mathrm{Fr}_v \in G(L_{j,l}/F)$ for a prime v of $\mathcal{O}_F$ such that $N_{F/\mathbb{Q}}(v) \leq b_1 d_{L_{j,l}}^{b_2}$. Now for every j such that $n_j = \pi_j(P) \neq 0$ let

$$S_{j,l}^{\mathrm{fin}} := \{v : N_{F/\mathbb{Q}}(v) \leq b_1 d_{L_{j,l}}^{b_2} \text{ and } v \text{ is of good reduction for } A\},$$
$$S_j^{\mathrm{fin}} := \bigcup_{l \mid n_j} S_{j,l}^{\mathrm{fin}}.$$

Then we define

$$S^{\mathrm{fin}} := \bigcup_{1 \leq j \leq s,\, n_j \neq 0} S_j^{\mathrm{fin}}.$$

It is enough to prove that for the set S^{fin} condition (2) implies (1). Indeed, if (1) does not hold then in the same way as in the proof of Theorem 4.1 there is $1 \leq j_0 \leq s$ such that $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some l and $\lambda \mid l$ such that $\lambda^{m_{1,j_0,\lambda}} \parallel n_{j_0}$ and $\lambda^{m_{2,j_0,\lambda}} \mid d_{j_0}$ for natural numbers $m_{1,j_0,\lambda} < m_{2,j_0,\lambda} = m_{1,j_0,\lambda} + 1$. As in the proof of Theorem 4.1 this leads to the investigation of a homomorphism π_{j_0} of $\mathbb{Z}$-modules and now the proof follows the lines of the proof of Theorem 4.1. Of course, the choice of the prime w in $\mathcal{O}_{F(r(A)[l^{n_{j_0,l}}])}$ is now done by virtue of Theorem 6.3. It is clear by the definition of $S_{j_0}^{\mathrm{fin}}$ that such a prime w can be chosen over a prime $v \in S_{j_0}^{\mathrm{fin}}$. Hence in the same way as in the proof of Theorem 4.1 we are led to a contradiction. ∎

Remark 6.5. The problem with an effective algorithm for finding S^{fin} comes from the lack of an effective algorithm for finding a $\mathbb{Z}$-basis of $A(F)/A(F)_{\mathrm{tor}}$. See [HS, pp. 457–465] for the explanation of obstructions to an effective algorithm for finding a $\mathbb{Z}$-basis of $A(F)/A(F)_{\mathrm{tor}}$.

Remark 6.6. For a given abelian variety A/F, in general, there is no finite set S^{fin} of primes of good reduction, depending only on A, such that for any $P \in A(F)$ and any subgroup $\Lambda \in A(F)$ the condition $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{\mathrm{fin}}$ implies $P \in \Lambda + A(F)_{\mathrm{tor}}$. Indeed, take any simple abelian variety A with $\mathrm{End}_{\overline{F}}(A) = \mathbb{Z}$ and with the rank of $A(F)$ over $\mathbb{Z}$ at least 2. Take two nontorsion points $P', Q' \in A(F)$, linearly independent over $\mathbb{Z}$. For any natural number M consider the finite set S_M of primes v of $\mathcal{O}_F$ of good reduction for A/F which are over rational primes $p \leq M$. Take a natural number n divisible by $\prod_{v \in S_M} |A_v(k_v)|$. Taking $P := nP'$ and $\Lambda := n\mathbb{Z}Q'$ we observe that $r_v(P) = 0 = r_v(\Lambda)$ for all $v \in S_M$ but by construction $P \notin \Lambda + A(F)_{\mathrm{tor}}$.

Acknowledgements. The authors would like to thank A. Schinzel for pointing out the very interesting example in his paper [Sch] on page 419. The authors would like to thank K. Rubin for pointing out important properties of CM elliptic curves used in Section 5 of this paper and for a number of important suggestions. The authors were partially supported by the NCN (grant no. NN 201 607 440).

References

[B] G. Banaszak, *On a Hasse principle for Mordell–Weil groups*, C. R. Math. Acad. Sci. Paris 347 (2009), 709–714.

[BGK1] G. Banaszak, W. Gajda and P. Krasoń, *Support problem for the intermediate Jacobians of l-adic representations*, J. Number Theory 100 (2003), 133–168.

[BGK2] —, —, —, *Detecting linear dependence by reduction maps*, ibid. 115 (2005), 322–342.

[BGK3] —, —, —, *On reduction map for étale K-theory of curves*, Homology Homotopy Appl. 7 (2005), 1–10.

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

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

[BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergeb. Math. Grenzgeb. 21, Springer, Berlin, 1990.

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

[De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg 14 (1941), 197–272.

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

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

[HS] M. Hindry and J. H. Silverman, *Diophantine Geometry. An Introduction*, Grad. Texts in Math. 201, Springer, Berlin, 2000.

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

[JP] P. Jossen and A. Perucca, *A counterexample to the local-global principle of linear dependence for abelian varieties*, C. R. Math. Acad. Sci. Paris 348 (2010), 9–10.

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

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

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

[Ko] E. Kowalski, *Some local-global applications of Kummer theory*, Manuscripta Math. 111 (2003), 105–139.

[La] S. Lang, *Complex Multiplication*, Grundlehren Math. Wiss. 255, Springer, 1983.

[LO] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: Algebraic Number Fields: L-functions and Galois Properties (Durham, 1975), Academic Press, London, 1977, 409–464.

[Pe1] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. Number Theory 129 (2009), 469–476.

[Pe2] —, *On the problem of detecting linear dependence for products of abelian varieties and tori*, Acta Arith. 142 (2010), 119–128.

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

[Re] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

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

[RS] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. 39 (2002), 455–474.

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

[Se] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. I.H.E.S. 54 (1981), 123–201.

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

[Sil1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[Sil2] —, *The theory of height functions*, in: Arithmetic Geometry, G. Cornell and J. H. Silverman (eds.), Springer, 1986, 151–166.

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

Grzegorz Banaszak
Department of Mathematics
Adam Mickiewicz University
61-614 Poznań, Poland
E-mail: banaszak@amu.edu.pl

Piotr Krasoń
Department of Mathematics
University of Szczecin
70-453 Szczecin, Poland
E-mail: krason@wmf.univ.szczecin.pl

Received on 22.5.2009
and in revised form on 25.9.2011 (6036)