ACTA ARITHMETICA
142.2 (2010)

On the problem of detecting linear dependence for products of abelian varieties and tori

by

Antonella Perucca (Lausanne)

1. Introduction. The *problem of detecting linear dependence* investigates whether the property for a rational point to belong to a subgroup obeys a local-global principle.

Question 1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$ and let Λ be a finitely generated subgroup of $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Does R belong to Λ?*

We answer this question affirmatively in three cases: if Λ is cyclic; if Λ is a free left $\operatorname{End}_K G$-submodule of $G(K)$; if Λ has a set of generators (as a group) which is a basis of a free left $\operatorname{End}_K G$-submodule of $G(K)$. In general, we prove that there exists an integer m (depending only on G, K and the rank of Λ) such that mR belongs to the left $\operatorname{End}_K G$-submodule of $G(K)$ generated by Λ.

The problem of detecting linear dependence for abelian varieties was first formulated by Gajda in 2002 in a letter to Ribet.

We now give the state of the art of the problem of detecting linear dependence for abelian varieties. Papers and preprints concerning this problem are: [16], [10], [2], [5], [1], [4], [7], [3], [6].

• Weston in [16] proved that if the abelian variety has commutative endomorphism ring then there exists a K-rational torsion point T such that $R+T$ belongs to Λ. Since the torsion of the Mordell–Weil group is finite, Weston basically solved the problem for abelian varieties with commutative endomorphism ring.

2010 *Mathematics Subject Classification*: Primary 11G10; Secondary 14L10, 14K15.
Key words and phrases: abelian varieties, tori, reductions, local-global principles, support problem.

• If the endomorphism ring of the abelian variety is not commutative, we are able to prove the following: there exists a non-zero integer m (depending only on G and K) such that mR belongs to the left $\operatorname{End}_K G$-submodule of $G(K)$ generated by Λ; see Theorem 6.

• We solve the problem of detecting linear dependence in the case where Λ is a free left $\operatorname{End}_K G$-submodule of $G(K)$ or if Λ has a set of generators (as a group) which is a basis of a free left $\operatorname{End}_K G$-submodule of $G(K)$. With an extra assumption on the point R (that R generates a free left $\operatorname{End}_K G$-submodule of $G(K)$), these two results are respectively proven by Gajda and Górnisiewicz in [5, Theorem B] and by Banaszak in [1, Theorem 1.1]. We remove the assumption on R in Theorem 6 and in Theorem 8 respectively.

• If Λ is cyclic, we solve the problem of detecting linear dependence. This result was only known for elliptic curves or under a condition satisfied if $\operatorname{End} G = \mathbb{Z}$ and the dimension of G is 2, 6 or odd. See [10, Theorem 3.3 and p. 120] by Kowalski.

• Gajda and Górnisiewicz in [5] use the theory of integrally semisimple Galois modules to study the problem of detecting linear dependence. This theory was completely developed by Larsen and Schoof in [11]. Gajda and Górnisiewicz prove the following result ([5, Theorem A]):

Let ℓ be a prime such that $T_\ell(G)$ is integrally semisimple, let $\hat{\Lambda}$ be a free $\operatorname{End}_K G \otimes \mathbb{Z}_\ell$-submodule of $G(K) \otimes \mathbb{Z}_\ell$ and let $\hat{R}$ in $G(K) \otimes \mathbb{Z}_\ell$ generate a free $\operatorname{End}_K G \otimes \mathbb{Z}_\ell$-submodule of $G(K) \otimes \mathbb{Z}_\ell$. Then $\hat{R}$ belongs to $\hat{\Lambda}$ if and only if for all but finitely many primes $\mathfrak{p}$ of K, $(\hat{R} \bmod \mathfrak{p})$ belongs to $(\hat{\Lambda} \bmod \mathfrak{p})$. If $\operatorname{End}_K G \otimes \mathbb{Q}_\ell$ is a division algebra and $\operatorname{End}_K G \otimes \mathbb{Z}_\ell$ is a maximal order, the condition on $\hat{\Lambda}$ can be replaced by the following: $\hat{\Lambda}$ is torsion-free over $\operatorname{End}_K G \otimes \mathbb{Z}_\ell$.

Recently, new results (yet unpublished) have been proven on the problem of detecting linear dependence for abelian varieties:

• There are counterexamples. Indeed, Question 1 has a negative answer already for powers of elliptic curves. See the preprints [7] by Jossen and the author and [3] by Banaszak and Krasoń.

• Question 1 has an affirmative answer for simple abelian varieties. This is proven by Jossen in his thesis ([6, Corollary 8.0.2]). By the Poincaré Reducibility Theorem, an abelian variety is isogenous to $A_1^{e_1} \times \cdots \times A_n^{e_n}$, where the A_i's are simple and non-isogenous abelian varieties. Banaszak and Krasoń [3, Theorem A] show that there exists a K-rational torsion point T such that $R+T$ belongs to Λ if the following condition is satisfied: for every $i = 1, \ldots, n$ the exponent e_i is at most the dimension of $H_1(A_i(\mathbb{C}); \mathbb{Q})$ as a vector space over $\operatorname{End}_{\bar{K}} A_i \otimes \mathbb{Q}$. Actually, R belongs to Λ because of the following result by Jossen.

• Let S be a subset of the primes of K of Dirichlet density 1. Consider the following subgroup of $G(K)$:

$$\tilde{\Lambda} = \{P \in G(K) : (P \bmod \mathfrak{p}) \in (\Lambda \bmod \mathfrak{p})\ \forall \mathfrak{p} \in S\}.$$

This group was first studied by Kowalski in [10]. Jossen [6, Theorem 8.0.1] proves (in the generality of semiabelian varieties) that the quotient $\tilde{\Lambda}/\Lambda$ is a finitely generated free abelian group.

In view of this result, Theorem 11 below can be extended to semiabelian varieties split up to isogeny. Because of Jossen's result, Theorem 6 actually proves that for semiabelian varieties split up to isogeny the following holds: the point R belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ. Consequently, Question 1 has an affirmative answer whenever Λ is a left $\mathrm{End}_K G$-submodule of $G(K)$. These last results are also independently proven by Jossen in [6].

Now we list further results on the problem of detecting linear dependence for commutative algebraic groups.

Schinzel [15, Theorem 2] answered Question 1 affirmatively for the multiplicative group. A generalization of Schinzel's result (Lemma 10 below for the multiplicative group where Λ is only required to be finitely generated) was proven by Khare in [8, Proposition 3]. Question 1 has a negative answer for tori. Indeed, Schinzel [15, p. 419] gave a counterexample for the product of two copies of the multiplicative group. See Example 9 below.

Kowalski [10] studied the problem of detecting linear dependence in the case where Λ is cyclic. In particular, he showed that the problem of detecting linear dependence has a negative answer whenever the additive group is embedded into G; see [10, Proposition 3.2].

Finally, a variant of the problem of detecting linear dependence was considered by Barańczuk in [4] for the multiplicative group and abelian varieties with endomorphism ring $\mathbb{Z}$.

2. Preliminaries. Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point of G and denote by G_R the smallest algebraic K-subgroup of G containing R. Write G_R^0 for the connected component of the identity of G_R and write n_R for the number of connected components of G_R. By [13, Proposition 5], G_R^0 is the product of an abelian variety and a torus defined over K.

We say that R is *independent* if R is non-zero and $G_R = G$. The point R is independent in G if and only if R is independent in $G \times_K \bar{K}$. Furthermore, R is independent in G if and only if R is non-zero and the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free. See [13, Section 2].

LEMMA 2. *Let R be a K-rational point of G and let d be a non-zero integer. We have $G_{dR}^0 = G_R^0$. In particular, the dimension of G_{dR} equals the dimension of G_R and $G_{n_R R} = G_{n_R R}^0 = G_R^0$.*

Proof. Since G_R contains dR we have $G_{dR} \subseteq G_R$ and so $G_{dR}^0 \subseteq G_R^0$. Hence it suffices to prove that G_{dR}^0 and G_R^0 have the same dimension. Clearly, the dimension of G_{dR}^0 is less than or equal to the dimension of G_R^0. To prove the other inequality it suffices to show that multiplication by $[d]$ maps G_R into G_{dR}. This is true because $[d]^{-1}G_{dR}$ contains R. ∎

Denote by W the connected component of G_R containing R and let X be a torsion point in $G_R(\bar{K})$ such that $W = X + G_R^0$ (see [13, Lemma 1]). Clearly, $n_R X$ is the least positive multiple of X belonging to G_R^0 and the connected components of G_R are of the form $aX + G_R^0$ for $0 \leq a < n_R$. We can write $R = X + Z$ where Z is in $G_R^0(\bar{K})$. Since R and Z have a common multiple, from Lemma 2 it follows that Z is independent in G_R^0.

LEMMA 3. *Let L be a finite extension of K where X is defined. Then for all but finitely many primes $\mathfrak{q}$ of L the point $(n_R X \bmod \mathfrak{q})$ is the least positive multiple of $(X \bmod \mathfrak{q})$ belonging to $(G_R^0 \bmod \mathfrak{q})$.*

Proof. Denote by x the order of X. We may assume that the points in $G_R[x]$ are defined over L. Suppose that d is a positive integer smaller than n_R such that for infinitely many primes $\mathfrak{q}$ of L the point $(dX \bmod \mathfrak{p})$ belongs to $(G_R^0 \bmod \mathfrak{q})$. Up to excluding finitely many primes $\mathfrak{q}$, we may assume that the reduction modulo $\mathfrak{q}$ maps injectively $G_R[x]$ to $(G_R \bmod \mathfrak{q})[x]$. By [10, Lemma 4.4] we may also assume that the reduction modulo $\mathfrak{q}$ maps surjectively $G_R^0[x]$ onto $(G_R^0 \bmod \mathfrak{q})[x]$. Then for infinitely many primes $\mathfrak{q}$ the point $(dX \bmod \mathfrak{q})$ belongs to the reduction modulo $\mathfrak{q}$ of the finite group $G_R^0[x]$. We deduce that dX belongs to $G_R^0[x]$. We have a contradiction since $n_R X$ is the least positive multiple of X which belongs to G_R^0. ∎

LEMMA 4. *Let A and T be respectively an abelian variety and a torus defined over a number field K. Then $\mathrm{Hom}_{\bar{K}}(A,T) = \{0\}$ and $\mathrm{Hom}_{\bar{K}}(T,A) = \{0\}$.*

Proof. Since A is a complete variety and T is affine, there are no non-trivial morphisms from A to T. To prove the other equality, suppose that ϕ is a morphism from $\mathbb{G}_m$ to A. On the point sets, ϕ gives a homomorphism from a non-finitely generated to a finitely generated abelian group. Then the kernel of ϕ is not finite so it must be the whole $\mathbb{G}_m$. ∎

The following lemma in the case of abelian varieties was proven by Banaszak in [1, Step 2 of the proof of Theorem 1.1].

LEMMA 5. *Let G be the product of an abelian variety and a torus defined over a number field K. Let α be a $\bar{K}$-endomorphism of G. Suppose that there* *exists a prime number ℓ such that for every $n > 0$ and every torsion point T of G of order ℓ^n the point $\alpha(T)$ is a multiple of T. Then α is a scalar.*

Proof. Let R be a commutative ring with 1. Let F be a free finitely generated R-module. Suppose that s is an R-endomorphism of F sending every element to a multiple of itself. Then it can easily be seen that s is a scalar. Apply the previous assertion to $R = \mathbb{Z}/\ell^n\mathbb{Z}$, $F = G[\ell^n]$, taking for s the image of α in $\mathrm{End}_{\mathbb{Z}} G[\ell^n]$. We deduce that α acts as a scalar on $G[\ell^n]$. So for every $n > 0$ there exists an integer c_n such that α acts as the multiplication by $c_n \pmod{\ell^n}$ on $G[\ell^n]$. Since α commutes with multiplication by ℓ we deduce that $c_{n+1} \equiv c_n \pmod{\ell^n}$ for every n. This means that there exists c in $\mathbb{Z}_\ell$ such that $c \equiv c_n \pmod{\ell^n}$ for every n and that α acts on $T_\ell G$ as the multiplication by c.

Write $G = A \times T$ where A is an abelian variety and T is a torus. By Lemma 4, α is the product $\alpha_A \times \alpha_T$ of an endomorphism of A and an endomorphism of T. It suffices to prove the following: if A (respectively T) is non-zero then c is an integer and α_A (respectively α_T) is the multiplication by c.

Suppose that A is non-zero. We know that α_A acts on $T_\ell A$ as the multiplication by c. By [12, Theorem 3, p. 176], c is an integer and α_A is the multiplication by c.

Suppose that T is non-zero. We reduce at once to the case where $T = \mathbb{G}_m^h$ for some $h \geq 1$. The endomorphism ring of $\mathbb{G}_m$ is $\mathbb{Z}$ hence we can identify the endomorphism ring of T with the ring of $h \times h$-matrices with integer coefficients. Since α_T acts on $T_\ell T$ as the multiplication by c, we deduce that α_T is a scalar matrix. Hence c is an integer and α_T is the multiplication by c. ∎

3. On a result by Gajda and Górnisiewicz. In this section we apply results on the support problem ([14]) to study the problem of detecting linear dependence. The second assertion of the following theorem was proven by Gajda and Górnisiewicz in [5, Theorem B] under the assumption that the point R generates a free left $\mathrm{End}_K G$-submodule of $G(K)$.

THEOREM 6. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point of G and let Λ be a finitely generated subgroup of $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists a non-zero integer m (depending only on G, K and the rank of Λ) such that mR belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ. Furthermore, if Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$ then R belongs to Λ.*

Remark that if G is an abelian variety, the integer m in Theorem 6 depends only on G and K since the rank of Λ is bounded by the rank of the Mordell–Weil group.

LEMMA 7. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point of G and let Λ be a finitely generated subgroup of $G(K)$. Fix a rational prime ℓ. Suppose that for all but finitely many primes $\mathfrak{p}$ of K there exists an integer $c_\mathfrak{p}$ coprime to ℓ such that $(c_\mathfrak{p} R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists a non-zero integer c such that cR belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ. One can take c such that $v_\ell(c) \leq v_\ell(m)$ where m is a non-zero integer depending only on G, K and the rank of Λ (hence not depending on ℓ). If Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$, one can take $m = 1$.*

Proof. Let $P_1, \dots, P_s$ generate Λ as a $\mathbb{Z}$-module. Consider G^s and its K-rational points $P = (P_1, \dots, P_s)$ and $Q = (R, 0, \dots, 0)$. We can apply [14, Main Theorem] to the points P and Q. Then there exist a K-endomorphism ϕ of G^s and a non-zero integer c such that $\phi(P) = cQ$. By [14, Proposition 10] one can take c such that $v_\ell(c) \leq v_\ell(m)$ where m depends only on G^s and K. In particular, cR belongs to $\mathrm{End}_K G \cdot \Lambda$. Since s depends only on G, K and the rank of Λ, the first assertion is proven. For the second assertion, let $P_1, \dots, P_s$ be a basis of Λ as a left $\mathrm{End}_K G$-module. Since P is independent, by [14, Proposition 9] one can take c coprime to ℓ. Consequently, one can take $m = 1$. ∎

Proof of Theorem 6. We apply Lemma 7 to every rational prime ℓ. Then for every ℓ there exists an integer c_ℓ such that $c_\ell R$ belongs to $\mathrm{End}_K G \cdot \Lambda$ and $v_\ell(c_\ell) \leq v_\ell(m)$, where m is a non-zero integer depending only on G, K and the rank of Λ. Since m is in the ideal of $\mathbb{Z}$ generated by the c_ℓ's, we deduce that mR belongs to $\mathrm{End}_K G \cdot \Lambda$. If Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$, one can take $m = 1$ in Lemma 7, hence R belongs to Λ. ∎

4. A refinement of a result by Banaszak. In this section we extend the result by Banaszak on the problem of detecting linear dependence ([1, Theorem 1.1]) from abelian varieties to products of abelian varieties and tori. Furthermore, by adapting Banaszak's proof we are able to remove his assumption on the point R (that R generates a free left $\mathrm{End}_K G$-submodule of $G(K)$).

THEOREM 8. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a finitely generated subgroup of $G(K)$ such that it has a set of generators (as a group) which is a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. Let R be a point in $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then R belongs to Λ.*

If $\mathrm{End}_K G = \mathbb{Z}$, the assumption on Λ is equivalent to saying that Λ contains no torsion points. In general, the condition implies that the left

$\mathrm{End}_K G$-module generated by Λ is free. The following example by Schinzel shows that the latter assumption is not sufficient.

EXAMPLE 9 (Schinzel, [15, p. 419]). A counterexample to Question 1 for $G = \mathbb{G}_m^2$ and $K = \mathbb{Q}$ is the following. Take the point $R = (1, 4)$ and take the group Λ generated by the points $P_1 = (2, 1)$, $P_2 = (3, 2)$, $P_3 = (1, 3)$. For every prime number $\mathfrak{p}$ the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. The point R belongs to the left $\mathrm{End}_K G$-module generated by Λ but does not belong to Λ. Notice that the left $\mathrm{End}_K G$-module generated by Λ is free and it is generated by P_2.

LEMMA 10. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a finitely generated subgroup of $G(K)$ such that it has a set of generators (as a group) which is a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. Let R be a point in $G(K)$. Fix a prime number ℓ. Suppose that for all but finitely many primes $\mathfrak{p}$ of K there exists an integer $c_\mathfrak{p}$ coprime to ℓ such that the point $(c_\mathfrak{p} R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists an integer c coprime to ℓ such that cR belongs to Λ.*

Proof. By Lemma 7 applied to $\mathrm{End}_K G \cdot \Lambda$, there exists an integer c coprime to ℓ such that cR belongs to $\mathrm{End}_K G \cdot \Lambda$. Let $\{P_1, \ldots, P_n\}$ be a set of generators for Λ which is a basis for $\mathrm{End}_K G \cdot \Lambda$. We can write

$$cR = \sum_{i=1}^{n} \phi_i P_i$$

for some ϕ_i in $\mathrm{End}_K G$. Without loss of generality it suffices to prove that ϕ_1 is the multiplication by an integer.

Suppose that ϕ_1 is not multiplication by an integer and apply Lemma 5 to ϕ_1. Then there exists a point T in $G[\ell^\infty]$ such that $\phi_1(T)$ is not a multiple of T. Let L be a finite extension of K where T is defined. The point $(P_1 - T, P_2, \ldots, P_n)$ is independent in G^n hence by [13, Proposition 12] there are infinitely many primes $\mathfrak{q}$ of L such that the following holds: $(P_i \bmod \mathfrak{q})$ has order coprime to ℓ for every $i \neq 1$ and $(P_1 - T \bmod \mathfrak{q})$ has order coprime to ℓ. By discarding finitely many primes $\mathfrak{q}$, we may assume the following: the order of $(T \bmod \mathfrak{q})$ equals the order of T; the point $(\phi_1(T) \bmod \mathfrak{q})$ is not a multiple of $(T \bmod \mathfrak{q})$ and in particular it is non-zero; $(c_\mathfrak{q} R \bmod \mathfrak{q})$ belongs to $(\Lambda \bmod \mathfrak{q})$ for some integer $c_\mathfrak{q}$ coprime to ℓ.

Fix $\mathfrak{q}$ as above. We know that there exists an integer m coprime to ℓ such that $(mP_i \bmod \mathfrak{q}) = 0$ for every $i \neq 1$ and $(m(P_1 - T) \bmod \mathfrak{q}) = 0$. Then we have

$$(mc_\mathfrak{q} cR \bmod \mathfrak{q}) = (mc_\mathfrak{q} \phi_1(P_1) \bmod \mathfrak{q}) = (mc_\mathfrak{q} \phi_1(T) \bmod \mathfrak{q}).$$

Since $v_\ell(mc_\mathfrak{q}) = 0$, we deduce that the point $(mc_\mathfrak{q} cR \bmod \mathfrak{q})$ has order a power of ℓ and it is not a multiple of $(T \bmod \mathfrak{q})$. Then $(mc_{\mathfrak{q}}cR \bmod \mathfrak{q})$ does not belong to $\sum_{i=1}^{n} \mathbb{Z}(P_i \bmod \mathfrak{q})$. Consequently, $(c_{\mathfrak{q}}R \bmod \mathfrak{q})$ does not belong to $(\Lambda \bmod \mathfrak{q})$ and we have a contradiction. ∎

Proof of Theorem 8. We can apply Lemma 10 to every rational prime ℓ. Then for every ℓ there exists an integer c_ℓ coprime to ℓ such that $c_\ell R$ belongs to Λ. Since 1 is contained in the ideal of $\mathbb{Z}$ generated by the c_ℓ's, we deduce that R belongs to Λ. ∎

5. On a result by Kowalski. Kowalski [10] studied the problem of detecting linear dependence for commutative algebraic groups in the case where Λ is cyclic. The following theorem was proven for elliptic curves in [10, Theorem 3.3]. Kowalski also described in [10, p. 120] how to apply the results by Khare and Prasad [9] to this problem.

THEOREM 11. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a cyclic subgroup of $G(K)$. Let R be a K-rational point of G. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then R belongs to Λ.*

LEMMA 12. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be an infinite cyclic subgroup of $G(K)$. Let T be a K-rational torsion point of G. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(T \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then T is zero.*

Proof. Suppose that T is non-zero. Then T can be uniquely written as a sum of torsion points whose orders are prime powers. These torsion points are multiples of T. Consequently, we reduce at once to the case where the order of T is the power of a prime number ℓ.

Let $\Lambda = \mathbb{Z}P$ for a point P of infinite order. The algebraic subgroup G_P of G generated by P has dimension at least 1. In Section 2 we saw the following: $P = X + Z$ for some point Z in $G_P^0(\bar{K})$ and some torsion point X in $G_P(\bar{K})$; the point Z is independent in G_P^0; $n_P X$ is the least multiple of X which belongs to G_P^0; G_P^0 is the product of an abelian variety and a torus defined over K.

Let c be the ℓ-adic valuation of the order of X. Let L be a finite extension of K where X, Z, $G[\ell^{2c}]$ are defined and such that $n_P X$ has n_P-roots in $G_P^0(L)$. Notice that for all but finitely many primes $\mathfrak{q}$ of L the point $(T \bmod \mathfrak{q})$ belongs to $(\mathbb{Z}P \bmod \mathfrak{q})$.

By [13, Proposition 12], there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z \bmod \mathfrak{q})$ is coprime to ℓ. Then for infinitely many primes $\mathfrak{q}$ the point $(T \bmod \mathfrak{q})$ lies in the finite group generated by $(X \bmod \mathfrak{q})$. We deduce that $T = aX$ for some non-zero integer a.

Let T_0 be a point in G_P^0 of order ℓ^{2c}. By [13, Proposition 11], there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z - T_0 \bmod \mathfrak{q})$ is coprime to ℓ. We deduce that for infinitely many primes $\mathfrak{q}$ the point $(T \bmod \mathfrak{q})$ lies in the finite group generated by $(T_0 + X \bmod \mathfrak{q})$. Then $T = b(T_0 + X)$ for some non-zero integer b.

Since $aX = b(T_0 + X)$ and because the order of T_0 is ℓ^{2c} we deduce that $v_\ell(b) \geq c$. Consequently, T is the sum of bT_0 and a torsion point of order coprime to ℓ. Then T is a multiple of T_0 and in particular it belongs to G_P^0.

Let T_1 be a point in $G_P^0(L)$ such that $n_P T_1 = -n_P X$. By [13, Proposition 11], there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z - T_1 \bmod \mathfrak{q})$ is coprime to ℓ. Up to discarding finitely many primes $\mathfrak{q}$, we may assume that $(T \bmod \mathfrak{q})$ belongs to $(\mathbb{Z}P \bmod \mathfrak{q})$ and that the order of $(T \bmod \mathfrak{q})$ equals the order of T. Again up to discarding finitely many primes $\mathfrak{q}$, by Lemma 3 we may assume that $(n_P X \bmod \mathfrak{q})$ is the least multiple of $(X \bmod \mathfrak{q})$ belonging to $(G_P^0 \bmod \mathfrak{q})$. Consequently, the intersection of $(G_P^0 \bmod \mathfrak{q})$ and $(\mathbb{Z}P \bmod \mathfrak{q})$ is $(\mathbb{Z}n_P P \bmod \mathfrak{q})$. Then $(T \bmod \mathfrak{q})$ belongs to $(\mathbb{Z}n_P P \bmod \mathfrak{q})$.

Fix a prime $\mathfrak{q}$ as above and denote by r the order of $(Z - T_1 \bmod \mathfrak{q})$. We have

$$\begin{aligned}(rn_P P \bmod \mathfrak{q}) &= (rn_P Z + rn_P X \bmod \mathfrak{q}) = (rn_P T_1 + rn_P X \bmod \mathfrak{q}) \\ &= (0 \bmod \mathfrak{q}).\end{aligned}$$

Since r is coprime to ℓ, it follows that $(\mathbb{Z}n_P P \bmod \mathfrak{q})$ has no ℓ-torsion and in particular it does not contain $(T \bmod \mathfrak{q})$. We have a contradiction. ∎

Proof of Theorem 11. If Λ is finite then there exists an element P' in Λ such that for infinitely many primes $\mathfrak{p}$ of K we have $(R \bmod \mathfrak{p}) = (P' \bmod \mathfrak{p})$. Hence $R = P'$ and the statement is proven. We may then assume that $\Lambda = \mathbb{Z}P$ for a point P of infinite order.

We first prove that the statement holds in the case where the algebraic group G_P generated by P is connected. In this case, G_P is the product of an abelian variety and a torus ([13, Proposition 5]). By [10, Lemma 4.2], we may assume that $G_P = G$. So we may assume that P is independent in G and we conclude by applying Theorem 8.

In general, let n_P be the number of connected components of G_P. Notice that the points $n_P P$ and $n_P R$ still satisfy the hypotheses of the theorem and that $G_{n_P P}$ is connected by Lemma 2. Therefore we know (by the special case above) that $n_P R = g n_P P$ for some integer g. Since R and P are rational points, we deduce that $R = gP + T$ for some rational torsion point T. Since $R - T$ belongs to Λ, for all but finitely many primes $\mathfrak{p}$ of K the point $(T \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. By applying Lemma 12 we deduce that $T = 0$ hence R belongs to Λ. ∎

Acknowledgements. I thank Emmanuel Kowalski and René Schoof for helpful discussions.

References

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

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

[3] G. Banaszak and P. Krasoń, *On arithmetic in Mordell–Weil groups*, preprint, arXiv: 0904.2848v2, 2009.

[4] S. Barańczuk, *On a generalization of the support problem of Erdős and its analogues for abelian varieties and K-theory*, J. Pure Appl. Algebra 214 (2010), 380–384.

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

[6] P. Jossen, *On the arithmetic of* 1*-motives*, Ph.D. thesis, Central European Univ. Budapest, 2009.

[7] 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.

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

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

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

[11] M. Larsen and R. Schoof, *Whitehead's lemma and Galois cohomology of abelian varieties*, http://mlarsen.math.indiana.edu/∼larsen/unpublished.html, 2004.

[12] D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math. 5, Oxford Univ. Press, London, 1970.

[13] 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.

[14] —, *Two variants of the support problem for products of abelian varieties and tori*, ibid., 1883–1892.

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

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

Antonella Perucca
Section de Mathématiques
École Polytechnique Fédérale de Lausanne
Station 8
CH-1015 Lausanne, Switzerland
E-mail: antonella.perucca@epfl.ch

Received on 14.11.2008
and in revised form on 19.8.2009 (5861)