Riv. Mat. Univ. Parma (7) **3*** (2004), 67-81

ROBERTO DVORNICICH and UMBERTO ZANNIER (*)

On the Hasse principle for the division of points in a commutative algebraic group (**)

Contents

1 - Introduction 67

2 - The cohomological interpretation 69

3 - Positive results 72

4 - Negative results 77

1 - Introduction

A very classical theorem (see [**1**], Thms 1 of Ch. IX and Ch. X) states, in particular, that if r is an odd positive integer and a is a non-zero rational number such that a is an r-th power modulo all but finitely many prime numbers p, then it is the r-th power of a rational number. On the contrary, for arbitrary r the result is not true: for example, 16 is an 8-th power in all $\mathbb{Q}_p$ with $p \neq 2$ but it is not the 8-th power of a rational number.

Now, taking r-th powers can be interpreted as multiplying by r in the algebraic group $\mathbb{G}_m$; this rephrasing motivates the following more general question:

(*) R. Dvornicich: Dipartimento di Matematica L. Tonelli, Università, Via Buonarroti 2, 56127 Pisa,Italy, e-mail: dvornic@dm.unipi.it; U. Zannier: Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy, e-mail: zannier@dimi.uniud.it

(**) Received November 7th 2004. AMS classification 14 G 05, 11 R 34, 14 G 25, 14 G 05.

for which algebraic groups $\mathcal{A}/k$ and natural numbers r, is the divisibility of a point P by r in $\mathcal{A}(k)$ equivalent to local r-divisibility almost everywhere?

The aim of this paper is to give an account of some cases where one can give an answer to this question, whether positive or negative. Most of the results we quote are contained in [**5**], [**6**], [**7**] and [**16**].

In order to formulate precisely our question and our results, we first introduce some notation.

In the sequel k denotes a number field with algebraic closure $\overline{k} = \overline{\mathbb{Q}}$. As usual we put $G_k := \mathrm{Gal}(\overline{k}/k)$. By a prime of k we mean a discrete valuation v of k. The completion (resp. residue field) at v will be denoted by k_v (resp. $k(v)$).

Let $\mathcal{A}$ be a commutative and connected algebraic group defined over k, supposed to be embedded in some projective or affine space. We shall write $\mathcal{A}$ additively and denote by O its origin (defined over k).

Let m be a positive integer and define $\mathcal{A}[m] := \{P \in \mathcal{A}(\overline{k}) \mid mP = O\}$. It follows from the classification of commutative algebraic groups in characteristic 0 (see for instance [**12**], Prop. 11, 12 of Ch. III, §2.7 and Cor. of Ch. VII, §2.7) that $\mathcal{A}[m] \cong (\mathbb{Z}/(m))^n$ for a certain integer $n = n_{\mathcal{A}}$ depending only on $\mathcal{A}$.

We shall be concerned with the following

Problem. *Let r be a positive integer and let $P \in \mathcal{A}(k)$. Suppose that for all but a finite number of primes v of k we have $P = rD_v$, for some $D_v \in k_v$. Can one conclude that there exists $D \in \mathcal{A}(k)$ such that $P = rD$?*

Example 1. The theorem mentioned at the beginning concerns the case $\mathcal{A} = \mathbb{G}_m$ of our problem. In [**1**] one can find a complete solution to this case. As mentioned, the answer is affirmative if r is odd, but more than this is true, and in particular one can always conclude that $2P$ is divisible by r in $\mathcal{A}(k)$. Letting $k = \mathbb{Q}$, $P = 16$, $r = 8$, one obtains the simplest example of a case where the answer to the problem is negative.

Remark 1. For almost all v we have that $\mathcal{A}$ has good reduction modulo v (whence the reduction is nonsingular) and that the point P is v-integral. In particular, for such a v, Hensel's lemma implies that the existence of D_v is equivalent to the fact that the reduction of P modulo v is divisible by r in $\mathcal{A}(k(v))$.

Also, the conclusion becomes trivial, in view of the Čebotarev theorem, if we assume that all r-th roots of P lie in k_v for almost all v.

The paper is organized as follows. In Section 2 we shall interpret the problem in cohomological terms, as is classical in the context; we shall introduce a certain cohomology group whose vanishing is sufficient for the local-global principle to

hold (see Propositions 1 and 2). This condition is possibly not necessary in the general case.

In Section 3 we shall give a number of examples where our *problem* has a positive answer. We shall start with general commutative algebraic groups $\mathcal{A}$ for which $n_{\mathcal{A}}$ is small; later on, we shall consider in some detail the cases when $\mathcal{A}$ is either an elliptic curve or an algebraic torus.

In Section 4 we shall give a number of examples where our *problem* has a negative answer. Again, we shall concentrate on the special cases when $\mathcal{A}$ is either an elliptic curve or an algebraic torus. Finally, we shall quote a result establishing to what extent the sufficient condition given in Proposition 1 is also necessary in order that our *problem* has a positive answer.

2 - The cohomological interpretation

First of all we note that, by Bezout's indentity, it is sufficient to study our *problem* in the case when r is a prime power. Let then $q = r = p^e$, where p is a prime and e is an integer and define $\mathcal{A}[q] \subset \mathcal{A}(\bar{k})$ to be the kernel of the multiplication by q map. This is a finite abelian p-group.

Let $K = k(\mathcal{A}[q])$ be the field generated over k by the points in $\mathcal{A}[q]$. Then K is a Galois extension of k.

Since the abelian group $\mathcal{A}[q]$ is isomorphic to $(\mathbb{Z}/(q))^n$, the absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$ acts as a subgroup of $GL_n(\mathbb{Z}/(q))$. We denote by G its image: observe that G is isomorphic to $\mathrm{Gal}(K/k)$.

Let $D \in \mathcal{A}(\bar{k})$ be any point satisfying $P = qD$ and let $L = k(D)$ be the number field generated by D over k. Then $F := LK \subset \overline{\boldsymbol{Q}}$ is normal over k, with Galois group Σ, say. For $\sigma \in \Sigma$ we have clearly

$$\sigma(D) = D + Z_\sigma, \tag{1}$$

for some $Z_\sigma \in \mathcal{A}[q]$. A quick computation gives the cocycle equation

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau), \tag{2}$$

for $\sigma, \tau \in \Sigma$. We let $\boldsymbol{c} : \sigma \mapsto Z_\sigma$ denote this cocycle and $[\boldsymbol{c}]$ its image in $H^1(\Sigma, \mathcal{A}[q])$.

Note that $[\boldsymbol{c}] = 0$ if and only if $P = qD'$ for some $D' \in \mathcal{A}(k)$.

Now let v be a prime of k, unramified in F and satisfying the assumptions of the problem. We may embed F in a finite extension F_w of k_v, corresponding to some prime w of F extending v. We have that $\mathrm{Gal}(F_w/k_v)$ is cyclic, generated by some Frobenius automorphism of v relative to F/k. By the basic assumption of the

problem, $P = qD_v$ for some $D_v \in \mathcal{A}(k_v)$. By the same argument as above, the restriction of $[\boldsymbol{c}]$ to $H^1(\mathrm{Gal}(F_w/k_v), \mathcal{A}[q])$ vanishes. We note that, by the Čebotarev theorem, $\mathrm{Gal}(F_w/k_v)$ varies over all cyclic subgroups of Σ as w runs over almost all primes of F. In other words, for each $\sigma \in \Sigma$ there exists $W_\sigma \in \mathcal{A}[q]$ such that

$$Z_\sigma = (\sigma - 1)\, W_\sigma. \tag{3}$$

This argument motivates the following general definition.

Definition 1. Let Γ be a group and let M be a Γ-module. We say that a cocycle $[\boldsymbol{c}] = [\{Z_\gamma\}] \in H^1(\Gamma, M)$ satisfies the *local conditions* if there exist $W_\gamma \in M$ such that $Z_\gamma = (\gamma - 1)W_\gamma$ for all $\gamma \in \Gamma$. We denote by $H^1_{\mathrm{loc}}(\Gamma, M)$ the subgroup of such cocycles. Equivalently, $H^1_{\mathrm{loc}}(\Gamma, M)$ is the intersection of the kernels of the restriction maps $H^1(\Gamma, M) \to H^1(C, M)$ as C varies over all cyclic subgroups of Γ.

Working with all valuations, instead of almost all, we would get the classical definition of the Selmer group. Modifications of the Selmer group, similar to our definition, appear in [**10**]. However, in order to render the paper self-contained, we prefer to keep our own notation. The next proposition can be obtained from rather well-known arguments (see for instance [**10**], Lemma 1.1 (ii)). It gives a sufficient condition for the *Problem* to have an affirmative answer.

Proposition 1. *Assume that* $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q]) = 0$. *Let* $P \in \mathcal{A}(k)$ *be a rational point with the following property: for all but finitely many primes* v *of* k, *there exists* $D_v \in \mathcal{A}(k_v)$ *such that* $P = qD_v$. *Then there exists* $D \in \mathcal{A}(k)$ *such that* $P = qD$.

Later in the paper we shall study the vanishing of the group $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q])$ in various special cases.

Remark 2. In some cases, Proposition 1 has a converse, namely: *Suppose that* $H^1(\mathrm{Gal}(K/k), \mathcal{A}(K)) = 0$, *but* $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q]) \neq 0$. *Then the Problem has a negative answer for some* $P \in \mathcal{A}(k)$.

In fact, the non-vanishing of $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q])$ gives a cocycle Z_σ satisfying (3) for $\sigma \in \mathrm{Gal}(K/k)$. Since $H^1(\mathrm{Gal}(K/k), \mathcal{A}(K)) = 0$, we have $Z_\sigma = \sigma(D) - D$ for some $D \in \mathcal{A}(F)$. Necessarily $P = qD \in \mathcal{A}(k)$ satisfies the assumptions, but not the conclusion of the Problem.

Hilbert's Theorem 90 says that $H^1(\mathrm{Gal}(K/k), \mathcal{A}(K)) = 0$ is true in the case when $\mathcal{A} = \mathbb{G}_m$ of Example 1 above. In general, however, the analogue of Hilbert's theorem is false; in those cases there seems to be no obvious reason why the men-

tioned converse should nevertheless be true. We shall see in Section 4 how to partially overcome this difficulty.

Proof of Proposition 1. Let Σ be as at the beginning of this section. The arguments above show that $H^1_{\mathrm{loc}}(\Sigma, \mathcal{A}[q]) = 0$ implies the conclusion of the proposition. Hence we need only to show that we may replace the group $H^1_{\mathrm{loc}}(\Sigma, \mathcal{A}[q])$ by $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q])$.

Since $F \supset K$, the action of G_k on $\mathcal{A}[q]$ factors through Σ. Hence G_k and Σ have the same image G in $Aut(\mathcal{A}[q])$. We observe that G is isomorphic to $\mathrm{Gal}(K/k)$.

We denote by Σ' the kernel of the representation of Σ in $Aut(\mathcal{A}[q])$. By definition, Σ' acts trivially on $A[q]$, hence the restriction-inflation exact sequence ([**11**], Prop. 4, Ch. IX, §6) takes the form

$$0 \to H^1(G, \mathcal{A}[q]) \to H^1(\Sigma, \mathcal{A}[q]) \to H^1(\Sigma', \mathcal{A}[q]).$$

We claim that the middle arrow induces an isomorphism

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) \cong H^1_{\mathrm{loc}}(\Sigma, \mathcal{A}[q]).$$

To prove the claim note first that, since the inflation is injective, it induces trivially an injective map. On the other hand, take an element $[\{Z_\sigma\}]$ of $H^1_{\mathrm{loc}}(\Sigma, \mathcal{A}[q])$; it restricts to zero in $H^1(\Sigma', \mathcal{A}[q])$, as follows from (3) and the fact that Σ'_p acts trivially on $\mathcal{A}[q]$. By the exactness of the restriction-inflation sequence, $[\{Z_\sigma\}]$ comes from an element $[\{Y_\tau\}] \in H^1(G, \mathcal{A}[q])$, and now it suffices to check that it lies in $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$: in fact, we may choose $[\{Z_\sigma\}]$ such that $Y_\tau = Z_\sigma$ for each σ which projects to τ; with this choice equation (3) gives the verification. ■

In particular, we obtain the following corollary, which can also be easily proved directly.

Corollary 1. *Let $P \in \mathcal{A}(k)$ be a rational point such that for all but finitely many primes v of k, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$. Then $D \in \mathcal{A}(K)$ for all D such that $P = qD$.*

Proof. We may view P as a point in $\mathcal{A}(K)$. The assumptions imply, *a fortiori*, that for all but finitely many primes w of K there exists $D_w \in \mathcal{A}(K_w)$ such that $P = qD_w$. Since $\mathrm{Gal}(K/K)$ is trivial, we have $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/K), \mathcal{A}[q]) = 0$. By Proposition 1 there exists $D \in \mathcal{A}(K)$ such that $P = qD$. Finally, if $D' \in \mathcal{A}(\bar{k})$ also satisfies $P = qD'$, then $D' - D \in \mathcal{A}[q] \subset \mathcal{A}(K)$. ■

We have already observed that $\mathcal{A}[q] \cong (\mathbb{Z}/(q))^n$ and that Σ acts on $\mathcal{A}[q]$ as a subgroup of $GL_n(\mathbb{Z}/(q))$. In the following we shall identify $\mathcal{A}[q]$ with $(\mathbb{Z}/(q))^n$ and $\mathrm{Aut}(\mathcal{A}[q])$ with $GL_n(\mathbb{Z}/(q))$.

Example 2. We can reinterpret in our language the case $\mathcal{A} = \mathbb{G}_m$ of Example 1 (see also [**10**], formula (2.5), p.22). In this case $n_{\mathcal{A}} = 1$ and G is isomorphic to a subgroup of $(\mathbb{Z}/(q))^*$. If $q = p^a$ is an odd prime power, then G is cyclic, hence $H^1_{\mathrm{loc}}(G, \mathbb{Z}/(q)) = 0$ trivially. In virtue of Proposition 1, our *Problem* has an affirmative answer in this case. On the other hand, it is easy to verify that, for $k = \mathbb{Q}$ and $q = 8$, we have $H^1_{\mathrm{loc}}(\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}), \mathbb{Z}/(8)) \cong \mathbb{Z}/(2)$. Since $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*) = 0$ (Hilbert's Theorem 90), Remark 2 guarantees the existence of counterexamples to the conclusion of the Problem. An explicit one is given by taking 8-th roots of 16.

To simplify things further, we define G_p to be a Sylow p-subgroup of G. We have:

Proposition 2. *An element of $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(q))^n)$ is zero if and only if its restriction to $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(q))^n)$ is zero.*

Proof. By [**11**], Thm. 4, Ch. IX, §2, the restriction $H^1(G, (\mathbb{Z}/(q))^n) \to H^1(G_p, (\mathbb{Z}/(q))^n)$ is injective on the p-primary part of $H^1(G, (\mathbb{Z}/(q))^n)$, which is the whole group in the present case, since $(\mathbb{Z}/(q))^n$ is a p-group. On the other hand, if a cocycle satisfies the local conditions (3) relative to G, it satisfies them relative to any subgroup of G, and the conclusion follows. ∎

3 - Positive results

We start by considering general commutative algebraic groups $\mathcal{A}$ with $n_{\mathcal{A}} = n$. The main reference for general results of this kind is [**5**]. The case when $n = 2$ and $q = p$ is particularly simple: since $G = G_p$ is contained in the p-Sylow subgroup of $GL_2(\mathbb{Z}/(p))$, we have that the order of G_p divides p, whence G_p is cyclic and $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^2) = 0$. By Propositions 1 and 2 we deduce that our *problem* has an affirmative answer. In particular, we obtain the following (see [**5**] and [**16**]):

Theorem 1. *Let E be an elliptic curve defined over a number field k. If a point $P \in E(k)$ is divisible by p in almost all $E(k_v)$, then it is divisible by p in $E(k)$.*

Next, consider the case $n = 2$, $q = p^2$. Here the situation is more involved. Letting G_0 be the kernel of the reduction map $GL_2(\mathbb{Z}/(q)) \to GL_2(\mathbb{Z}/(p))$, we can

summarize our results in terms of $H = G_p \cap G_0$. Note that H has a natural structure of $\mathbb{F}_p$-vector space.

Proposition 3. *Suppose that either*
(i) $p \neq 2, 3$ *and* $\dim H \neq 2$, *or*
(ii) $p = 3$ *and* $\dim H \geq 3$, *or*
(iii) $p = 2$ *and* $\dim H = 4$.
Then $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p^2))^2) = 0$.

In all cases not covered by Proposition 3 one can actually have $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p^2))^2) \neq 0$; this remark will be the basis for the construction of an example where the answer to our *Problem* is negative (see Section 4, Theorem 5).

Considering now the case $n = 3$, we can have $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(q))^3) \neq 0$ even when $q = p$. However, one can prove that there is essentially one case for which $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^3) \neq 0$, and this occurs only for $p \neq 2$. We shall use in the proof of Theorem 4 the exceptionality of the prime 2 in this case, namely

Proposition 4. $H^1_{loc}(G_2, (\mathbb{Z}/(2))^3) = 0$ *for any possible* G_2.

On the other hand, more and more examples for which $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) \neq 0$ can be given for $n > 3$.

Now we restrict our consideration to special commutative groups. We consider first the important case of elliptic curves (see [**7**]).

Theorem 2. *Let* $\mathcal{E}/\mathbb{Q}$ *be an elliptic curve,* $P \in \mathcal{E}(\mathbb{Q})$ *be a point which is locally divisible by* p^n *in* $\mathcal{E}(\mathbb{Q}_v)$ *almost everywhere, where* p *is a prime number and* $n \geq 1$. *If*

$$p \notin S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

then P *is divisible by* p^n *in* $\mathcal{E}(\mathbb{Q})$.

Proof. **(Sketch)** Put $q = p^n$ and let $K = \mathbb{Q}(\mathcal{E}[q])$ be the field of q-torsion points on $\mathcal{E}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By Proposition 1 it will suffice to verify that $H^1_{\mathrm{loc}}(G, \mathcal{E}[q]) = 0$ for $p \notin S$; actually we shall show the stronger condition $H^1(G, \mathcal{E}[q]) = 0$.

As usual, we shall view $\mathcal{E}[q]$ as $(\mathbb{Z}/(q))^2$ and consequently we shall represent G as a subgroup of $GL_2(\mathbb{Z}/(q))$, denoted by the same symbol; also, as before, we denote by $G_0 \subset GL_2(\mathbb{F}_p))$ the reduction of G modulo p and by H_0 its image in $PGL_2(\mathbb{F}_p)$.

We recall at once that $\mathbb{Q}(\mathcal{E}[p])$, and *a fortiori* $\mathbb{Q}(\mathcal{E}[q])$, contains a primitive p-

th root of unity ζ (see [**14**], Cor. 8.1.1); the basic properties of the Weil pairing ([**14**], III.8) entail that the action of G on ζ is given by $g(\zeta) = \zeta^{\det g}$ for $g \in G$. In particular, $\det : G \to \mathbb{F}_p^*$ is surjective and hence $p-1$ divides the order of G_0.

To start with, we deal with the cases when G_0 contains a nontrivial multiple of the identity. By standard arguments in group theory, one sees that G itself must contain a nontrivial multiple of the identity. We are then reduced to a case covered by Sah's Theorem (see for instance [**9**], Ch. V, Thm. 5.1) and we get immediately $H^1(G, \mathcal{E}[q]) = 0$ in this case.

Hence, from now on we shall assume that G_0 does not contain any scalar matrix of order $d > 1$, which implies that the natural map $G_0 \to PGL_2(\mathbb{F}_p)$ is injective, so $H_0 \cong G_0$.

We shall now use the classification of subgroups of $PGL_2(\mathbb{F}_p)$, to be found, e.g., in [**13**]. Suppose first that p divides the order of G_0. Then, by [**13**], Prop. 15, either G_0 contains $SL_2(\mathbb{F}_p)$ or it is contained in a Borel subgroup of $GL_2(\mathbb{F}_p)$; this last possibility means that G_0 can be put in triangular form with respect to some basis for $\mathbb{F}_p^2$.

Now, the first possibility yields that G_0 contains $-I$, which has order 2 (recall $p \neq 2$), a contradiction. The second possibility is also excluded for $p \notin S$; in fact, if G_0 can be put in (upper) triangular form, it stabilizes the subgroup generated by the column vector with coordinates $(1, 0)$; equivalently, the subgroup generated by the corresponding p-torsion point would be stable by the Galois action and thus rational. Now, a deep theorem of Mazur (see, e.g., [8], Thm. 2.2, p. 128) asserts that this cannot happen for $p \notin S$.

Therefore in the sequel we shall further assume that p does not divide $\#G_0$.

Note that we are assuming that $\#H_0 = \#G_0$ is coprime to p and we have observed that it is divisible by $p-1$. Hence, by [**13**], Prop. 16, $H_0 \cong G_0$ must be of one of the following types: (i) cyclic; (ii) dihedral; (iii) isomorphic to A_4, to A_5 or to S_5 (we denote by A_n (resp. S_n) the alternating (resp. symmetric) group on n elements). The rest of the proof consists in excluding, by group-theoretic arguments, all these cases for $p \notin S$.

Theorem 3. *Let k be a number field and let $\mathcal{E}/k$ be an elliptic curve. Then there exists $p_0 = p_0(\mathcal{E}, k)$ such that, if $p > p_0$ and $P \in \mathcal{E}(k)$ is a point locally divisible by p^n in $\mathcal{E}(k_v)$ almost everywhere, P is divisible by p^n in $\mathcal{E}(k)$.*

Proof. Let $q = p^n$, $K = k(\mathcal{E}[q])$ and $G = \mathrm{Gal}(K/k)$ and G_0 be the reduction of G modulo p (via the identification of G with a subgroup of $GL_2(\mathbb{Z}/(q))$. By the results of Serre [**13**], there exists $p_0 = p_0(\mathcal{E}, k)$ such that $G_0 = GL_2(\mathbb{Z}/(p)$ for $p > p_0$.

Then G_0 contains a nontrivial multiple of the identity and, by Sah's Theorem, $H^1(G, \mathcal{E}[q]) = 0$, which suffices. ■

The next special case we consider is the case of algebraic tori.

We recall that an algebraic k-torus of dimension n is a linear algebraic group, defined over k, which is isomorphic to $\mathbb{G}_m^n$ over $\bar{k}$ (see for instance [3], Ch. X.1.3). As recalled in Example 1, our *Problem* can have a negative answer already in the simplest case when the torus is isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$. For $q = p$ a prime, however, the answer in the case of $\mathbb{G}_m$ is positive. In this section we restrict our attention precisely to the case $q = p$. We shall see in Section 4 that even this restriction does not imply an affirmative answer in general; however, the answer is positive under certain conditions. The main result in the positive direction is the following.

Theorem 4. *Let T be an algebraic k-torus of dimension $n \leqslant \max(3, 2(p-1))$. Then if a point $P \in T(k)$ is divisible by p in almost all $T(k_v)$, then it is divisible by p in $T(k)$.*

Preliminary to the proof, we introduce some notation and outline some basic facts from the theory of algebraic tori.

Let $\phi : T \to \mathbb{G}_m^n$ be an isomorphism of algebraic groups defined over $\bar{k}$. For $\sigma \in G_k := \mathrm{Gal}(\bar{k}/k)$ we put

$$\psi(\sigma) := \phi \circ (\phi^\sigma)^{-1}.$$

Then $\psi(\sigma)$ is a 1-cocycle of G_k with values in the automorphism group of $\mathbb{G}_m^n$. Now this last group may be identified with $GL_n(\mathbb{Z})$, with trivial action of $G_{\mathbb{Q}}$. Therefore $\sigma \mapsto \psi(\sigma)$ is a homomorphism $\psi : G_k \to GL_n(\mathbb{Z})$. Since ϕ is defined over some number field, the kernel H of ψ has finite index in G_k and its image is a finite subgroup Δ of $GL_n(\mathbb{Z})$. We denote by L the fixed field of H; then L is a normal extension of k with Galois group $\mathrm{Gal}(L/k) \cong \Delta$. Moreover, ϕ is defined over L and L is the minimal splitting field for T, i.e. T becomes isomorphic to $\mathbb{G}_m^n$ over L. Conversely, the triple (k, L, conjugacy class of Δ in $GL_n(\mathbb{Z})$) defines a k-torus T up to k-isomorphism. (For a general account of this topic see for instance [4] or [**15**], Ch. 1, §3.)

Proof. **(Sketch)** The isomorphism ϕ shows that $T[p] \cong (\mathbb{Z}/(p))^n$ is an abelian group. We now analyze the Galois action on $T[p]$. Let $\chi : G_k \to (\mathbb{Z}/(p))^*$ be the cyclotomic character defined by $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$ for a primitive p-th root of unity

ζ_p. It is easy to verify that G_k acts on $T[p]$ as

$$t^\sigma \to \chi(\sigma)\,\psi(\sigma)\,v$$

if $t \in T[p]$ corresponds to $v \in (\mathbb{Z}/(p))^n$. Therefore we have a homomorphism ξ: $G_k \to GL_n(\mathbb{Z}/(p))$ defined by

$$\xi : \sigma \mapsto \chi(\sigma)\ \widetilde{\psi(\sigma)},$$

where the tilde denotes the reduction mod p. The field $K = k(T[q])$ is precisely the fixed field of the kernel of ξ. Observe that this implies

$$K \subset L(\zeta_p).$$

(The last assertion can also be derived directly from the fact that ϕ is defined over L.)

As in Section 2, we denote by G the image of ξ. Restricting ξ to $G_{k(\zeta_p)}$ we have clearly $\chi(\sigma) = 1$, so the image of this restriction is a normal subgroup G' of G which is also a normal subgroup $\widetilde{\Delta}'$ of $\widetilde{\Delta}$. Both indices $[G : G']$ and $[\widetilde{\Delta} : \widetilde{\Delta}']$ divide $[k(\zeta_p) : k]$, and hence are coprime to p. It follows that G and $\widetilde{\Delta}$ have the same p-Sylow subgroups.

By Propositions 1 and 2, it is sufficient to prove that

$$H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^n) = 0\,. \tag{4}$$

By what we have just shown, this is the same as studying the vanishing of $H^1_{\mathrm{loc}}(\widetilde{\Delta}_p, (\mathbb{Z}/(p))^n)$, where $\widetilde{\Delta}_p$ is a p-Sylow subgroup of $\widetilde{\Delta}$. We also notice that the image of a p-Sylow subgroup of Δ under reduction mod p is a p-Sylow subgroup of $\widetilde{\Delta}$.

By [2], Ch. III, Exercise 7.6, we have that

(a) $G_p \cong \Delta_p$ except possibly for $p = 2$, where the kernel of the reduction has order at most 2.

(b) $\mathrm{ord}_p(\#\Delta_p) \leqslant \left[\dfrac{n}{p-1}\right] + \left[\dfrac{n}{p(p-1)}\right] + \dots$.

By condition (b) we see that G_p is necessarily cyclic whenever $n < 2(p-1)$, so the theorem follows in this case. Also, if $n \leqslant 3$, the result follows from Proposition 4.

Hence we assume from now on that $n = 2(p-1) \geqslant 4$, so $p \geqslant 3$ and $n < p(p-1)$. By (a) above we have $G_p \cong \Delta_p$ and, by (b), Δ_p has order $\leqslant p^2$. If Δ_p is cyclic the vanishing of the relevant H^1_{loc} is automatic and concludes the proof. Hence we may

suppose that $\Delta_p \cong G_p \cong (\mathbb{Z}/(p)) \times (\mathbb{Z}/(p))$. In particular Δ_p corresponds to a faithful representation of $(\mathbb{Z}/(p)) \times (\mathbb{Z}/(p))$ into $GL_n(\mathbb{Z})$.

For the rest of the proof we refer to [**5**]; essentially, it consists in classifying all faithful representations of $(\mathbb{Z}/(p))^2$ in $GL_n(\mathbb{Z})$ up to equivalence in $GL_n(\mathbb{Z})$ and verifying directly the triviality of the relevant H^1_{loc}. ■

Remark 3. The method of the proof can be probably generalized. For instance, in a paper not yet published, M. Illengo has announced that the conclusion of our Theorem 4 remains true under the weaker assumption $n < \max\{4, p(p-1)\}$.

4 - Negative results

This section is devoted to show situations in which our *problem* has a negative answer. The first example (see [**6**]) concerns elliptic curves, and arises from the analysis of the cases not covered by Proposition 3, where it can well happen that $H^1_{\text{loc}}(G_p, (\mathbb{Z}/(p^2))^2) \neq 0$. The example also shows that some restriction on the prime p in Theorem 2 is necessary.

Theorem 5. *There exist elliptic curves $\mathcal{E}$ defined over $\mathbb{Q}$ and points $P \in \mathcal{E}(\mathbb{Q})$ such that $P \in 4\,\mathcal{E}(\mathbb{Q}_v)$ for almost all $v \in M_{\mathbb{Q}}$ but $P \notin 4\,\mathcal{E}(\mathbb{Q})$.*

Proof. **(Skecth)** Since for an elliptic curve $\mathcal{E}$ the group $\mathcal{E}[4](\bar{k})$ is isomorphic to $(\mathbb{Z}/(4))^2$, we identify $G := \text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}$ with a subgroup of $GL_2(\mathbb{Z}/(4))$. First of all we want G to be a group for which $H^1_{\text{loc}}(G, (\mathbb{Z}/(4))^2) \neq 0$. Choosing G as

$$G = \left\{ I + 2\begin{pmatrix} x & y \\ x+y & x+y \end{pmatrix} \,\middle|\, x, y \in \mathbb{Z}/(4) \right\}$$

$$= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \right\},$$

it is straightforward to verify that a nonzero element in $H^1_{\text{loc}}(G, (\mathbb{Z}/(4))^2)$ is given by the cocycle

$$Z_\sigma = \begin{pmatrix} 2y \\ 0 \end{pmatrix}, \qquad \text{for } \sigma = \sigma(x, y) = I + 2\begin{pmatrix} x & y \\ x+y & x+y \end{pmatrix}. \tag{5}$$

Starting from these data, we seek an elliptic curve $\mathcal{E}/\mathbb{Q}$ and a point $P \in \mathcal{E}(\mathbb{Q})$ with

the following properties. Let $K = \mathbb{Q}(\mathcal{E}[4])$; we first require that the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $(\mathbb{Z}/(4))^2$ corresponds to G with respect to some basis for $\mathcal{E}[4]$ over $\mathbb{Z}/(4)$, so that in particular $[K : \mathbb{Q}] = 4$. Then we require that, for some point $D \in \mathcal{E}(K)$ with $4D = P$, the cocycle $D^\sigma - D \in \mathcal{E}[4]$ corresponds to Z_σ (with respect to the same basis for $\mathcal{E}[4]$), namely

$$Z_\sigma = D^\sigma - D \,. \tag{6}$$

We first note that the above conditions and (5) yield $D^{\sigma(1,0)} = D$. Thus we seek $D \in \mathcal{E}(k)$, where $k \subset K$ is the fixed field of $\sigma(1, 0)$. We have $[k : \mathbb{Q}] = 2$.

Now, for simplicity, we work with curves $\mathcal{E}$ having a Weierstrass equation of the form

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$ are distinct rationals which satisfy $\alpha + \beta + \gamma = 0$, and we impose that the conjugate D' of D over $\mathbb{Q}$ satisfies $D' = D + (\alpha, 0)$ (the sum being the usual sum of points in an elliptic curve). Then we find that our conditions imply that actually $k = \mathbb{Q}(\sqrt{-1})$, $\gamma - \alpha$ and $(\alpha - \beta)(\beta - \gamma)$ are (nonzero) rational squares and that $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha - \beta})$.

Now, these arithmetical conditions on α, β, γ correspond to rational points on a certain rational curve. It is easy to parametrize it: setting $\gamma - \alpha = \xi^2$, $\alpha - \beta = (\beta - \gamma)\,\eta^2$ and combining these equations with $\alpha + \beta + \gamma = 0$, we obtain

$$\alpha = -\frac{\xi^2(1 + 2\eta^2)}{3(1 + \eta^2)}\,, \quad \beta = -\frac{\xi^2(1 - \eta^2)}{3(1 + \eta^2)}\,, \quad \gamma = \frac{\xi^2(2 + \eta^2)}{3(1 + \eta^2)}\,. \tag{7}$$

From this parametrization, however, we have to discard the points corresponding to $\xi\eta = 0$ (for which α, β, γ are not distinct) and to $1 + \eta^2$ a rational square (for which $[K : \mathbb{Q}] = 2$).

Also, given α, β, γ, we can parametrize the points $D = (u_0 + u_1\sqrt{-1}, v_0 + v_1\sqrt{-1})$ suitable for us. Namely, setting $2u_0 = -t^2 - \alpha$, $2u_1 = s$, the suitable choices for D correspond to the rational points on the (s, t)-plane curve of genus 1 defined by

$$-s^2 = t^4 + 6\alpha t^2 + (\beta - \gamma)^2. \tag{8}$$

■

Remark 4. It is not hard to recognize that the curve (8) has rational points for infinitely many values of (ξ, η), with $\xi\eta \neq 0$ and $1 + \eta^2$ not a rational square, giving rise to non-isomorphic curves. We give two examples:

(a) $\xi = 5,\ \eta = 2,\ s = 8,\ t = 1$. This gives the point

$$D = (7 + 4\sqrt{-1},\ -4 + 22\sqrt{-1}), \qquad P = \left(\frac{1561}{12^2},\ \frac{19459}{12^3} \right)$$

on the elliptic curve

$$y^2 = (x + 15)(x - 5)(x - 10).$$

(b) $\xi = 65,\ \eta = 8,\ s = 112,\ t = 1$. This gives the point

$$D = (1397 + 56\sqrt{-1},\ -56 + 4192\sqrt{-1}), \quad P = \left(\frac{5086347841}{1848^2},\ -\frac{35496193060511}{1848^3} \right)$$

on the elliptic curve

$$y^2 = (x + 2795)(x - 1365)(x - 1430).$$

It is to be remarked that in this example the point $P = 4D$ is divisible by 4 in $\mathbb{Q}_p$ for *all* primes p but it is not divisible by 4 in $\mathbb{Q}$.

The second example concerns algebraic tori.

In the proof of Theorem 4 we obtained the conclusion $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) = 0$ under the assumption $n \leqslant 2(p-1)$. As remarked, this assumption can be relaxed, but for given p some condition on n is necessary. The following theorem, obtained with the substantial advice of Colliot-Thélène, shows not only that one can have $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) \neq 0$, but that the answer to our *problem* for algebraic tori and $r = p$ can be negative. The proof is too technical to be even sketched here; the interested reader can find the details in [**5**].

Theorem 6. *There exists a torus T over a number field k and a point P in $T(k)$ such that P is p-divisible in $T(k_v)$ for almost all v, but not p-divisible in $T(k)$.*

Remark 5. In the proof of Theorem 6 given in [**5**], an explicit example of a torus for which the answer to our *problem* is negative is given. In this example, the torus is defined over a certain number field k and has dimension $n = p^4 - p^2 + 1$; at the cost of increasing the dimension, one can obtain examples of tori T defined over $\mathbb{Q}$ and can also satisfy the stronger requirement that there exists a point $P \in T(\mathbb{Q})$ which is divisible by p over *all* local fields $\mathbb{Q}_\ell$ but not over $\mathbb{Q}$. However, we do not know what is the minimum values of n (in terms of p) for which such examples exist.

Finally, we quote a very recent and still unpublished result (see [7]) which settles almost completely the problem raised in Remark 2, namely, to what extent the condition given in Theorem 1 is also necessary in order that our *problem* has a positive answer.

Theorem 7. *Let $K = k(\mathcal{A}[q])$ and let Z be a cocycle of G with values in $\mathcal{A}[q]$ representing a nontrivial element of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$. Then there exists a number field L such that $L \cap K = k$ and a point $P \in \mathcal{A}(L)$ which is divisible by q in $\mathcal{A}(L_w)$ for all places w of L but is not divisible by q in $\mathcal{A}(L)$.*

Using Theorem 7, results such as Theorem 6 can be reobtained more simply (although less explicitly), just by exhibiting a case where the relevant group H^1_{loc} is non-trivial.

References

[1] E. ARTIN and J. TATE, *Class field theory*, Benjamin, New York-Amsterdam 1968.

[2] N. BOURBAKI , *Groupes et algèbres de Lie*, Chap. 2 et 3, Hermann, Paris 1972.

[3] J. W.S. CASSELS and A. FRÖHLICH (ED.), *Algebraic Number Theory*, Academic Press, London 1967.

[4] J.-L. COLLIOT-THÉLÈNE and J.-J. SANSUC., *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. **10** (1977), 175-229.

[5] R. DVORNICICH and U. ZANNIER, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), 317-338.

[6] R. DVORNICICH and U. ZANNIER, *An analogue for elliptic curves of the Grunwald-Wang example*, C.R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.

[7] R. DVORNICICH and U. ZANNIER, *On a local-global principle for the divisibility of a rational point by a positive integer*, submitted.

[8] S. LANG, *Number Theory III*, Encyclopaedia of Mathematical Sciences, EMS **60**, Springer-Verlag, Berlin 1991.

[9] S. LANG, *Elliptic Curves: Diophantine Analysis*, Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag Berlin-New York 1978.

[10] J.-J. SANSUC, *Groupe de Brauer et arithmétique des groupes linéaires sur un corps de nombres*, J. reine angew. Math. **327** (1981), 12-80.

[11] J.-P. SERRE, *Local Fields*, Springer Verlag, New York-Berlin 1979.

[12] J.-P. SERRE, *Algebraic groups and class fields*, Springer Verlag, New York 1988.

[13] J.-P. SERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[14] J. H. SILVERMAN, *The arithmetic of elliptic curves*, Springer-Verlag GTM **106**, 1986.

[15] V. E. VOSKRESENSKIĬ, *Algebraic groups and their birational invariants*, AMS Transl. of Mathematical Monographs **179** (1998).

[16] S. WONG, *Power residues on Abelian varieties*, Manuscripta Math. **102** (2000), 129-137.

Abstract

Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. We consider the following question: Let r be a positive integer and let $P \in \mathcal{A}(k)$. Suppose that for all but a finite number of primes v of k we have $P = rD_v$, for some $D_v \in \mathcal{A}(k_v)$. Can one conclude that there exists $D \in \mathcal{A}(k)$ such that $P = rD$? A complete answer for the case of the multiplicative group $\mathbb{G}_m$ is classical. We study other instances, mainly concerning elliptic curves and algebraic tori, obtaining results in both directions: namely, we have families of examples for which the answer is positive and families of examples for which the answer is negative.

* * *