*Bull. Soc. math. France*
**129** (3), 2001, p. 317–338

# LOCAL-GLOBAL DIVISIBILITY OF RATIONAL POINTS IN SOME COMMUTATIVE ALGEBRAIC GROUPS

BY ROBERTO DVORNICICH & UMBERTO ZANNIER

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 and in particular obtain an affirmative answer when $r$ is a prime and $\mathcal{A}$ is either an elliptic curve or a torus of small dimension with respect to $r$. Without restriction on the dimension of a torus, we produce an example showing that the answer can be negative even when $r$ is a prime.

RÉSUMÉ (*Divisibilité locale-globale des points rationnels en certains groupes algébriques commutatifs*)

Pour un groupe algébrique commutatif $\mathcal{A}$, défini sur un corps de nombres $k$, on se pose la question suivante : *étant donnés un entier $r$ strictement positif et un élément $P$ de $\mathcal{A}(k)$, on suppose que pour tout premier $v$ de $k$, à l'exception d'au plus d'un nombre fini, il existe un élément $D_v$ de $\mathcal{A}(k_v)$ avec $P = rD_v$. Peut-on en déduire l'existence d'un élément $D$ de $\mathcal{A}(k)$ tel que l'on ait $P = rD$ ?* Une réponse complète à cette question est bien connue dans le cas où $\mathcal{A}$ est le groupe multiplicatif $\mathbb{G}_m$. Nous étudions d'autres cas particuliers. Nous obtenons notamment une réponse affirmative dans le cas où $r$ est un nombre premier et où $\mathcal{A}$ est, soit une courbe elliptique, soit un tore de dimension petite par rapport à $r$. En outre, nous montrons par un exemple que, dans le cas où $\mathcal{A}$ est un tore de dimension arbitraire, la réponse peut être négative, même si $r$ est un nombre premier.

*Texte reçu le 8 novembre 1999, révisé le 11 mai 2000, accepté le 21 juillet 2000*

ROBERTO DVORNICICH, Diaprtimento di Matematica, Via F. Buonarroti 2, 56127 Pisa (Italy)
*E-mail :* dvornic@dm.unipi.it
UMBERTO ZANNIER, Istituto Universitario di Architettura D.C.A., S. Croce, 191 (Tolentini), 30135 Venezia (Italy) • *E-mail :* zannier@brezza.iuav.unive.it

2000 Mathematics Subject Classification. — 14G05.

Key words and phrases. — Rationality questions, rational points.

## 1. Introduction

A strong form of the Hasse principle for binary quadratic forms (over $\mathbb{Q}$) is the following: *if a quadratic form $aX^2 + bXY + cY^2 \in \mathbb{Q}[X, Y]$ of rank 2 represents 0 non-trivially over all but a finite number of completions $\mathbb{Q}_p$, then it represents 0 non-trivially over $\mathbb{Q}$.* This amounts to the fact that *if a rational number is a square modulo all but a finite number of primes, then it is a perfect square.* A generalization of this fact to higher powers $r$ and arbitrary number fields $k$ holds subject to certain assumptions (see Example 1.1 below). Now, taking $r$-th powers can be interpreted as multiplying by $r$ in the algebraic group $\mathbb{G}_m$; this rephrasement motivates the following more general question: *for which algebraic groups $\mathcal{A}/k$ and natural numbers $r$, the divisibility of a point $P$ by $r$ in $\mathcal{A}(k)$ is equivalent to local $r$-divisibility almost everywhere*?

In the present paper we shall investigate some instances of this question in the case of commutative algebraic groups. We shall show that there are cases in which the answer is positive (Theorem 3.1 and Theorem 4.1) and cases when it is negative (Example 2.4 and Example 5.1).

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

NOTATION. — In the sequel $k$ denotes a number field with algebraic closure $\bar{k} = \overline{\mathbb{Q}}$. As usual we put $G_k := \mathrm{Gal}(\bar{k}/k)$. 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

$$\mathcal{A}[m] := \big\{P \in \mathcal{A}(\bar{k}) \mid mP = O\big\}.$$

We have $\mathcal{A}[m] \cong (\mathbb{Z}/(m))^n$ for a certain integer $n = n_{\mathcal{A}}$ depending only on $\mathcal{A}$ (see the beginning of §2 for a sketch of the proof).

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 1.1. — In case $\mathcal{A} = \mathbb{G}_m$ a complete answer is provided by [AT, Thms 1 of Chap. IX and Chap. X]: the answer is affirmative *e.g.* if $r$ is odd; in any case one can conclude that $2P$ is divisible by $r$ in $\mathcal{A}(k)$. A counterexample to the case of general $r$ is given by $k = \mathbb{Q}$, $P = 16$, $r = 8$. See also Example 2.4 below for a direct verification of these facts.

REMARK 1.2. — 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 §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 2.1 and 2.5). This condition is possibly not necessary in the general case.

In §3 we shall consider in some detail the case $n = 2$ and make just a few remarks on the case of other small values of $n$; in particular, the local-global principle for $p$-divisibility in elliptic curves will follow in a very simple way (see Theorem 3.1). On the other hand, we shall also give simple examples where the relevant cohomology group is nonzero.

In §4 we shall consider the case when $\mathcal{A}$ is a torus, namely it becomes isomorphic to $\mathbb{G}_m^n$ over $\bar{k}$. The classical result recalled here as Example 2.4 shows that the answer is negative for general $r$ even when $\mathcal{A}$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$. We shall study in detail the case when $r$ is prime. It will turn out rather easily that, when $r = p$ and $n < 2(p-1)$, the Problem has an affirmative answer. With more substantial work, also the case $n = 2(p-1)$ will follow (see Theorem 4.1).

It is perhaps possible to improve further on the bound $n \leq 2(p-1)$, but certainly Theorem 4.1 does not hold without restrictions on $n$. In §5 we shall describe in detail an example suggested by J.-L. Colliot-Thélène (see Example 5.1). We shall explicitly construct a torus in which our Problem has a negative answer for $r = p$.

*Acknowledgements.* — We wish to thank Professor J.-L. Colliot-Thélène for valuable remarks, in particular for pointing out the example described in §5 below. We are indebted to the referee for helping us in clarifying the consequences of such example, as well as for his detailed report.

A substantial part of this paper was written when the authors were guests of the Institute for Advanced Study, Princeton. We thank the School of Mathematics of the Institute and the James D. Wolfensohn Foundation for their hospitality and support.

## 2. The cohomological interpretation

For the reader's convenience, we start this section with a sketch of the proof that $\mathcal{A}[m] \cong (\mathbb{Z}/(m))^n$ for a certain integer $n = n_{\mathcal{A}}$ depending only on $\mathcal{A}$. It follows from the classification of commutative algebraic groups in characteristic 0 (see for instance [9, Prop. 11, 12 of Chap. III, §2.7 and Cor. of Chap. VII, §2.7]) that there exists an exact sequence

$$0 \to \mathbb{G}_a^r \times \mathbb{G}_m^s \longrightarrow \mathcal{A} \longrightarrow \mathcal{B} \to 0,$$

where $\mathcal{B}$ is an abelian variety. It is a straightforward consequence of the commutativity of $\mathcal{A}$ and the divisibility of $\mathbb{G}_a^r \times \mathbb{G}_m^s$ that this leads to an exact sequence

$$0 \to (\mathbb{G}_a^r \times \mathbb{G}_m^s)[m] \longrightarrow \mathcal{A}[m] \longrightarrow \mathcal{B}[m] \to 0.$$

Now $(\mathbb{G}_a^r \times \mathbb{G}_m^s)[m] \cong (\mathbb{Z}/(m))^s$ and $\mathcal{B}[m] \cong (\mathbb{Z}/(m))^{2t}$, where $t$ is the dimension of $\mathcal{B}$. Therefore the abelian group $\mathcal{A}[m]$ has order $m^{s+2t}$ and can be generated by $\leq s + 2t$ elements. Since $\mathcal{A}[m]$ has exponent $m$, the result follows from the theory of finite abelian groups.

Coming back to our Problem, first of all we note that it is sufficient to analyze 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 normal over $k$.

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 $\mathrm{GL}_n(\mathbb{Z}/(q))$. 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 $F := LK \subset \bar{\mathbb{Q}}$ is normal over $k$, with Galois group $\Sigma$, say. For $\sigma \in \Sigma$ we have clearly

$$\sigma(D) = D + Z_\sigma, \tag{2.1}$$

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

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau), \tag{2.2}$$

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

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

Let now $v$ 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 $[\mathbf{c}]$ 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 $\Sigma$ 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

$$Z_\sigma = (\sigma - 1)W_\sigma. \tag{2.3}$$

This argument motivates the following general definition.

Definition. — Let $\Gamma$ be a group and let $M$ be a $\Gamma$-module. We say that a cocycle $[\mathbf{c}] = [\{Z_\gamma\}] \in H^1(\Gamma, M)$ 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 $\Gamma$.

Working with all valuations, instead of almost all, we would get the classical definition of the Shafarevic group. Modified Shafarevich groups, similar to our definition, appear in [6]. 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 [6, Lemma 1.1 (ii)],). It gives a sufficient condition for the Problem to have an affirmative answer.

Proposition 2.1. — *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 $H^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{A}[q])$ in various special cases.

Remark 2.2. — In some cases, Proposition 2.1 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 $Z_\sigma$ satisfying (2.3) 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 1.1 above. In general however the analogue of Hilbert's theorem is false; in those cases there seems to be no obvious reason why the mentioned converse should nevertheless be true. In §5 we shall give a different instance of the converse implication.