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 Σ, 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 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

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

This argument motivates the following general definition.

Definition. — Let Γ be a group and let M be a Γ-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 Γ.

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_σ 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.

Proof of Proposition 2.1. — 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 $\mathrm{Aut}(\mathcal{A}[q])$. We observe that G is isomorphic to $\mathrm{Gal}(K/k)$.

We denote by Σ' the kernel of the representation of Σ in $\mathrm{Aut}(\mathcal{A}[q])$. By definition, Σ' acts trivially on $A[q]$, hence the restriction-inflation exact sequence [8, Prop. 4, Chap. IX, §6], takes the form

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

We claim that the middle arrow induces an isomorphism

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

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 (2.3) 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 (2.3) gives the verification. □

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

COROLLARY 2.3. — *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

$$H^1_{\mathrm{loc}}\big(\mathrm{Gal}(K/K), \mathcal{A}[q]\big) = 0.$$

By Proposition 2.1 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 $\mathrm{GL}_n(\mathbb{Z}/(q))$. In the following we shall identify $\mathcal{A}[q]$ with $(\mathbb{Z}/(q))^n$ and $\mathrm{Aut}(\mathcal{A}[q])$ with $\mathrm{GL}_n(\mathbb{Z}/(q))$.

EXAMPLE 2.4. — We can reinterpret in our language the case $\mathcal{A} = \mathbb{G}_m$ of Example 1.1 (see also [6, 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 2.1, 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 2.2 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 another remark:

PROPOSITION 2.5. — *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 [8, Thm. 4, Chap. IX, §2], the restriction

$$H^1\big(G, (\mathbb{Z}/(q))^n\big) \longrightarrow H^1\big(G_p, (\mathbb{Z}/(q))^n\big)$$

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 (2.3) relative to G, it satisfies them relative to any subgroup of G, and the conclusion follows. □

REMARK 2.6. — In the sequel we shall be primarily concerned with the calculation of $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(q))^n)$ in various special cases. We remark however that considering the whole G may be sometimes very useful. For example, it may be easily shown (using the restriction-inflation sequence) that, if G contains a nontrivial multiple of the identity matrix, then $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(q))^n) = 0$.

3. The case when $n = 2$, $q = p$ or $q = p^2$

When $n = 2$ and $q = p$, we have that $G = G_p$ is contained in the p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}/(p))$. Therefore 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 2.1 and 2.5 we deduce that our Problem has an affirmative answer. In particular, we obtain the following:

THEOREM 3.1. — *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 $E(k)$.*

When $q = p^2$, as we now assume, things are more involved. Let G_0 be the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}/(q)) \to \mathrm{GL}_2(\mathbb{Z}/(p))$. We formulate our result in terms of $H = G_p \cap G_0$. Note that H has a natural structure of $\mathbb{F}_p$-vector space.

PROPOSITION 3.2. — *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 $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p^2))^2) = 0$.

Proof. — We begin by looking at the group $H^1_{\mathrm{loc}}(H, (\mathbb{Z}/(p^2))^2)$. By definition, any element $\sigma \in H$ can be written as

$$\sigma = I + p\begin{pmatrix} x'_\sigma & t'_\sigma \\ w'_\sigma & y'_\sigma \end{pmatrix} \tag{3.1}$$

for some $x'_\sigma, t'_\sigma, w'_\sigma, y'_\sigma \in \mathbb{Z}/(p^2)$. Clearly (3.1) depends only on the residue classes mod p of $x'_\sigma, t'_\sigma, w'_\sigma, y'_\sigma$. If z' is an element of $\mathbb{Z}/(p^2)$, we shall denote throughout this section by z its residue class mod p.

It is easy to see that

$$\sigma \longmapsto \begin{pmatrix} x_\sigma & t_\sigma \\ w_\sigma & y_\sigma \end{pmatrix}$$

is an injective homomorphism $H \to (\mathbb{Z}/(p))^4$.

Let now $\{Z_\sigma, \sigma \in H\}$ be a 1-cocycle representing a class in $H^1_{\mathrm{loc}}(H, (\mathbb{Z}/(q))^2)$. By the local condition, $Z_\sigma \in \mathrm{Im}(\sigma - 1) \subset p(\mathbb{Z}/(q))^2$. Therefore we may write

$$Z_\sigma = pZ'_\sigma = p\begin{pmatrix} a'_\sigma \\ b'_\sigma \end{pmatrix}, \quad a'_\sigma, b'_\sigma \in \mathbb{Z}/(p^2).$$

Also, denoting again by a_σ and b_σ the classes of a'_σ and b'_σ mod p, by the cocycle condition we may verify that

$$\sigma \longmapsto \begin{pmatrix} a_\sigma \\ b_\sigma \end{pmatrix}$$

is a homomorphism of H to $(\mathbb{Z}/(p))^2$.

We recall without proof the following

LEMMA 3.3. — *Let V be a vector space and $\psi, \varphi_1, \ldots, \varphi_m \in V^*$. If*

$$\bigcap_{i=1}^{m} \ker \varphi_i \subset \ker \psi,$$

then $\psi \in \langle \varphi_1, \ldots, \varphi_m \rangle$.

By the local conditions, there exist $\lambda_\sigma, \mu_\sigma \in k$ such that

$$a_\sigma = \lambda_\sigma x_\sigma + \mu_\sigma t_\sigma, \quad b_\sigma = \lambda_\sigma w_\sigma + \mu_\sigma y_\sigma.$$

The last equation implies $\ker w_\sigma \cap \ker y_\sigma \subset \ker b_\sigma$, whence, by Lemma 3.3, there exist $\tilde{\lambda}, \tilde{\mu} \in k$ such that

$$b_\sigma = \tilde{\lambda} w_\sigma + \tilde{\mu} y_\sigma$$

for all $\sigma \in H$. Subtracting the coboundary $(\sigma - 1)\begin{pmatrix} \tilde{\lambda} \\ \tilde{\mu} \end{pmatrix}$ and applying Lemma 3.3 again we may then assume

$$a_\sigma = \lambda x_\sigma + \mu t_\sigma, \quad b_\sigma = 0, \tag{3.2}$$

and the local conditions say that there exist $\lambda_\sigma, \mu_\sigma \in k$ such that

$$\begin{pmatrix} \lambda x_\sigma + \mu t_\sigma \\ 0 \end{pmatrix} = \begin{pmatrix} x_\sigma & t_\sigma \\ w_\sigma & y_\sigma \end{pmatrix} \begin{pmatrix} \lambda_\sigma \\ \mu_\sigma \end{pmatrix}. \tag{3.3}$$

We are now ready to prove that $H^1_{\mathrm{loc}}(H, (\mathbb{Z}/(p^2))^2) = 0$ in cases (i), (ii) and (iii).

- Case 1: $\dim H = 1$. — In this case H is cyclic and the result is trivial.

- Case 2: $\dim H = 3$. — The homomorphisms $x_\sigma, y_\sigma, w_\sigma, t_\sigma$ satisfy a single non-trivial linear relation of type

$$Ax_\sigma + Bt_\sigma + Cw_\sigma + Dy_\sigma = 0.$$

The cases when either $(A, B) = (0, 0)$ or $(C, D) = (0, 0)$ are dealt rather easily and we leave them to the reader.

Now suppose that (A, B) and (B, C) are both $\neq (0, 0)$, and so w_σ and y_σ are linearly independent. Considering the matrices of determinant zero, we have the system

$$Ax_\sigma + Bt_\sigma = -(Cw_\sigma + Dy_\sigma), \quad y_\sigma x_\sigma - w_\sigma t_\sigma = 0.$$

By elementary linear algebra, the local conditions are not satisfied if we can find a vector (w, y) such that

$$Aw + By \neq 0, \quad Cw + Dy \neq 0 \quad \text{and} \quad \lambda w + \mu y \neq 0.$$

A counting argument shows that this is always the case unless $(\lambda, \mu) = (0, 0)$ (the trivial cocycle) or $p = 2$ and (A, B), (C, D), (λ, μ) are all distinct. (This case gives in fact $H^1_{\mathrm{loc}}(H, (\mathbb{Z}/(4))^2) \neq 0$, as shown for instance by the case $(A, B) = (1, 0)$, $(C, D) = (0, 1)$ and $(\lambda, \mu) = (1, 1)$.)

- Case 3: $\dim H = 4$. — Choose σ such that $x_\sigma = w_\sigma = 1$, $t_\sigma = y_\sigma = 0$: with the notation of (3.2) and (3.3) we have $\lambda = \lambda_\sigma = 0$. Similarly, choosing σ such that $x_\sigma = w_\sigma = 0$, $t_\sigma = y_\sigma = 1$, we get $\mu = 0$ and so $a_\sigma = 0$ for all $\sigma \in H$.

Consider now the full group G_p and let H be the kernel of the reduction map. Then $\Gamma = G_p/H$ is cyclic, $\Gamma = \langle\bar\gamma\rangle$, and we may suppose

$$\tilde\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is a simple exercise to verify that, for $\dim H = 1$ and $p \neq 2, 3$, the group G_p is cyclic, so the conclusion is trivial. Hence we are left with the case $\dim H \geq 3$ (and $p \geq 3$ if $\dim H = 3$).

If $Z_\sigma = \begin{pmatrix} u'_\sigma \\ v'_\sigma \end{pmatrix}$ is a cocycle with values in $\mathbb{Z}/(p^2)$ such that $Z_\sigma = 0$ for all $\sigma \in H$, then $(h-1)Z_\sigma = 0$ for all $h \in H$, for all $\sigma \in G_p$ and, setting

$$h = I + p\Delta'_h = I + p\begin{pmatrix} x'_h & t'_h \\ w'_h & y'_h \end{pmatrix},$$

we have $p\Delta'_h Z_\sigma = 0$ for all $h \in H$, *i.e.*

$$\Delta_h \begin{pmatrix} u_\sigma \\ v_\sigma \end{pmatrix} = 0, \quad \forall h \in H,$$

where $\Delta_h, u_\sigma, v_\sigma$ denote the reduction of $\Delta'_h, u'_\sigma, v'_\sigma$ modulo p.

The local conditions say that

$$\begin{pmatrix} u_\sigma \\ v_\sigma \end{pmatrix} = (\sigma - 1)\begin{pmatrix} \mu_\sigma \\ \nu_\sigma \end{pmatrix}$$

for some $\mu_\sigma, \nu_\sigma \in \mathbb{Z}/(p)$. If $\dim H \geq 3$, then $\det \Delta_h$ does not vanish identically on H, whence $u_\sigma = v_\sigma = 0$ for all σ; moreover, the local conditions (for $\sigma \notin H$) imply that $\nu_\sigma = 0$ for all σ, *i.e.*

$$\begin{pmatrix} u'_\sigma \\ v'_\sigma \end{pmatrix} = p\begin{pmatrix} a'_\sigma \\ b'_\sigma \end{pmatrix} = (\sigma - 1)\begin{pmatrix} \mu'_\sigma \\ p\beta'_\sigma \end{pmatrix}$$

for some $a'_\sigma, b'_\sigma, \mu'_\sigma, \beta'_\sigma \in \mathbb{Z}/(p^2)$. For $\sigma = \gamma^i h$ we have

$$p\begin{pmatrix} a'_\sigma \\ b'_\sigma \end{pmatrix} = (\gamma^i h - 1)\begin{pmatrix} \mu'_\sigma \\ p\beta'_\sigma \end{pmatrix}$$

and

$$\gamma^i h = \gamma^i(1 + p\Delta'_h) = \gamma^i + p\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x'_h & t'_h \\ w'_h & y'_h \end{pmatrix}.$$

Setting $\gamma^i - 1 = \begin{pmatrix} pr'_i & i + ps'_i \\ pt'_i & pv'_i \end{pmatrix}$, dividing by p and then reducing mod p, we get

$$\begin{pmatrix} a_\sigma \\ b_\sigma \end{pmatrix} = \begin{pmatrix} r_i\mu_\sigma + i\beta_\sigma + (x_h + iw_h)\mu_\sigma \\ (t_i + w_h)\mu_\sigma \end{pmatrix}.$$

Recalling that the last matrix must be independent of $h \in H$, we see that if w_h is not identically 0 on H, then $\mu_\sigma = 0$, $b_\sigma = 0$, $\sigma \mapsto a_\sigma$ is a homomorphism and

$$p\begin{pmatrix} a'_\sigma \\ 0 \end{pmatrix} = (\sigma - 1)\begin{pmatrix} 0 \\ pa'_\gamma \end{pmatrix}$$

for all $\sigma \in G_p$. Also, if w_h is identically zero but x_h is not, we get again $\mu_\sigma = 0$ and the same conclusion follows. □

EXAMPLE 3.4. — The condition $\dim H \neq 2$ in Proposition 3.2 (i) is necessary. In fact, let $x_\sigma = y_\sigma$, $t_\sigma = nw_\sigma$, with $(\frac{n}{p}) = -1$. Then

$$\sigma = I + p\Delta'_\sigma = I + p\begin{pmatrix} y'_\sigma & nw'_\sigma \\ w'_\sigma & y'_\sigma \end{pmatrix},$$

whence $\det \Delta_\sigma \neq 0$ if $(y_\sigma, w_\sigma) \neq (0,0)$ and the local conditions are satisfied. On the other hand, if

$$Z_\sigma = \begin{pmatrix} py'_\sigma \\ 0 \end{pmatrix},$$

then Z_σ is a cocycle but we cannot have

$$Z_\sigma = (\sigma - 1)\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix},$$

since $\alpha w_\sigma + \beta y_\sigma$ is not identically 0.

EXAMPLE 3.5. — In the case when $\dim H = 1$ the condition that $p \neq 2, 3$ is necessary, as shown by the following examples.

- If $p = 2$ let G_2 be the group generated by the matrices

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

and let Z_σ be the cocycle defined by $Z_\gamma = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $Z_h = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

- If $p = 3$ let G_3 be the group generated by the matrices

$$\gamma = \begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

and let Z_σ be the cocycle defined by $Z_\gamma = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$, $Z_h = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

REMARK 3.6. — For $n > 2$, we can have $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^n) \neq 0$ even in the case $q = p$. In fact, for $n = 3$, one can prove, with methods similar to those used in the proof of Proposition 3.2, that there is essentially one case for which

$H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^3) \neq 0$, namely the case when $p \neq 2$ and G_p is conjugate to a subgroup of $\mathrm{GL}_3(\mathbb{Z}/(p))$ of type

$$K_{p,\lambda} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & \lambda a \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_p \right\}, \quad \lambda \in \left(\mathbb{Z}/(p)\right)^*$$

for which it is easily seen that

$$Z_\sigma = \begin{pmatrix} \lambda a_\sigma^2 - b_\sigma \\ 0 \\ 0 \end{pmatrix}$$

satisfies the local conditions but is not a coboundary. If $p = 2$ (and necessarily $\lambda = 1$) the corresponding group $K_{2,1}$ turns out to be cyclic, so trivially $H^1_{\mathrm{loc}}(K_{2,1}, (\mathbb{Z}/(2))^3) = 0$ and hence $H^1_{\mathrm{loc}}(G_2, (\mathbb{Z}/(2))^3) = 0$ for any possible G_2. We shall use this remark when proving Theorem 4.1.

For $n > 3$ there are also several examples for which $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n)$ does not vanish: take for instance $n = 4$ and

$$G = \left\{ \begin{pmatrix} 1 & a & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_p \right\};$$

again the cocycle

$$Z_\sigma = \begin{pmatrix} b_\sigma \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

satisfies the local conditions but is not a coboundary.

4. The case of 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 [3, Chap. X.1.3]). As recalled in Example 1.1, 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 §5 that even this restriction does not imply an affirmative answer in general. We shall see that the answer is positive under certain conditions. The main result of this section is the following.

THEOREM 4.1. — *Let T be an algebraic k-torus of dimension*

$$n \leq \max\bigl(3, 2(p-1)\bigr).$$

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 $\mathrm{GL}_n(\mathbb{Z})$, with trivial action of $G_\mathbb{Q}$. Therefore $\sigma \mapsto \psi(\sigma)$ is a homomorphism $\psi : G_k \to \mathrm{GL}_n(\mathbb{Z})$. 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 $\mathrm{GL}_n(\mathbb{Z})$. 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 $(k, L, \text{conjugacy class of } \Delta \text{ in } \mathrm{GL}_n(\mathbb{Z}))$ defines a k-torus T up to k-isomorphism. (For a general account of this topic see for instance [4] or [11, Chap. 1, §3, Chap. 1, §3].)

Proof of Theorem 4.1. — The isomorphism ϕ shows that $T[p] \cong (\mathbb{Z}/(p))^n$ as 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

$$t^\sigma \longrightarrow \chi(\sigma)\psi(\sigma)v$$

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

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

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 §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 $\tilde{\Delta}'$ of $\tilde{\Delta}$. Both indices $[G : G']$ and $[\tilde{\Delta} : \tilde{\Delta}']$ divide $[k(\zeta_p) : k]$, and hence are coprime to p. It follows that G and $\tilde{\Delta}$ have the same p-Sylow subgroups.

By Propositions 2.1 and 2.5, it is sufficient to prove that

$$H^1_{\mathrm{loc}}\big(G_p, (\mathbb{Z}/(p))^n\big) = 0. \tag{4.1}$$

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

EXAMPLE 4.2. — Let F be a number field of degree n over $\mathbb{Q}$ and let $T = R_{F/\mathbb{Q}}\mathbb{G}_m$ be the n-dimensional $\mathbb{Q}$-torus obtained by restriction of scalars from F to $\mathbb{Q}$ (see [12, Chap. 1]). Then $G_{\mathbb{Q}}$ acts as permutation group on $G_{\mathbb{Q}}/G_F$ and this defines an n-dimensional permutation representation of $G_{\mathbb{Q}}$. It may be easily verified that its image is precisely Δ. The known case of $\mathcal{A} = \mathbb{G}_m$ (see Example 1.1) allows to treat this case. It is also possible however to show directly that, *e.g.* for $q = p$, $H^1_{\mathrm{loc}}(\Sigma_p, T[p]) = 0$.

By [1, Chap. 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) $\mathrm{ord}_p(\#\Delta_p) \leq \left[\dfrac{n}{p-1}\right] + \left[\dfrac{n}{p(p-1)}\right] + \cdots$.

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 $n \leq 3$, the result follows from §3; in fact, the only counterexample for $n = 3$ holds for $p \neq 2$ (see Remark 3.6).

Hence we assume from now on that $n = 2(p-1) \geq 4$, so $p \geq 3$ and $n < p(p-1)$. By (a) above we have $G_p \cong \Delta_p$ and, by (b), Δ_p has order $\leq p^2$. 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 representation of $(\mathbb{Z}/(p)) \times (\mathbb{Z}/(p))$ into $\mathrm{GL}_n(\mathbb{Z})$.

REMARK 4.3. — Although all such representations can be diagonalized over $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity, they may be non-conjugate in $\mathrm{GL}_n(\mathbb{Z}[\zeta_p])$, even if they are isomorphic over $\mathbb{Q}$. A fortiori, they may be non-conjugate in $\mathrm{GL}_n(\mathbb{Z})$. Therefore, in our analysis we must refine the classical theory of linear representations by introducing integrality conditions.

We give an example of the phenomenon just described. Take $p = 3$, $n = 4$ and put

$$\alpha = \begin{pmatrix} I & -I \\ 0 & A \end{pmatrix}, \quad \beta = \begin{pmatrix} A & I \\ 0 & I \end{pmatrix},$$

where $I = I_2$ and A is a matrix in $\mathrm{GL}_2(\mathbb{Z})$ such that $A^2 + A + I = 0$. It is readily verified that α, β generate a group G isomorphic to $(\mathbb{Z}/(3))^2$. On the other hand G cannot be put in diagonal form over $\mathbb{Z}[\zeta_3]$, for otherwise we would have $\alpha^2 + \alpha + I_4 \equiv 0 \pmod{(\zeta_3 - 1)}$, since every eigenvalue satisfies the same

congruence. This is however not the case: in fact, the right upper corner of $\alpha^2+\alpha+I_4$ is $-A-2I$; if this were divisible by ζ_3-1 then we would have $A\equiv I \pmod 3$. Since $A^3=I$, this would imply $A=I$.

In practice we shall write down all the representations of $(\mathbb{Z}/(p))^2$ in $GL_n(\mathbb{Z})$ up to equivalence in $GL_n(\mathbb{Z})$ and verify directly the triviality of the relevant H^1_{loc}. The method is probably capable to be generalized to some extent.

In the sequel we shall write Γ both for the mentioned subgroup $\Delta_p\subset \mathrm{GL}_n(\mathbb{Z})$ and for its reduction G_p modulo p.

To start with, we shall decompose our (faithful) action of Γ on $\mathbb{Q}^n$. Suppose that $\mathbb{Q}^n$ is equipped with a $\mathbb{Q}[\Gamma]$-module structure and suppose it is simple. Then, by Schur's Lemma (see for intance [5, Chap. XVII.1, Prop. 1.1]), the ring $\mathrm{End}_{\mathbb{Q}[\Gamma]}\mathbb{Q}^n$ is a division ring. On the other hand Γ is abelian, so this ring contains the image of $\mathbb{Q}[\Gamma]$ as a ring of endomorphism. If the representation of Γ on $\mathbb{Q}^m$ were faithful, we would have a contradiction: in fact the equation $X^p=1$ has $\geq p^2$ solutions in $\mathbb{Q}[\Gamma]$, which therefore cannot be a domain. Hence either the action of Γ on $\mathbb{Q}^m$ is trivial, and we have $m=1$, or it factors through a subgroup of order p. In this last case it corresponds to an irreducible representation of $\mathbb{Z}/(p)$ over $\mathbb{Q}$, which is either trivial or has dimension $p-1$ (corresponding to the irreducible factors of X^p-1 over $\mathbb{Q}$).

Therefore, since the action of $\mathbb{Q}[\Gamma]$ on $\mathbb{Q}^n$ is semisimple (see [7, Chap. 6.1, Prop. 9]) any representation of $\mathbb{Q}[\Gamma]$ in $\mathbb{Q}^n$ is either trivial, or may be decomposed as the sum of $p-1$ trivial 1-dimensional representations with a $(p-1)$-dimensional irreducible representation, or finally is the sum of two $(p-1)$-dimensional irreducible representations. Only the last possibility may come from a faithful action. In fact, otherwise the $(p-1)$-dimensional irreducible representation would be itself faithful. But we have proved just above that each simple representation cannot be faithful. Therefore we restrict to these last cases.

Let V be a $(p-1)$-dimensional subspace of $\mathbb{Q}^n$ stable by Γ. By [2, Chap. I.2.2, Cor. 3], we can find a $\mathbb{Q}$-basis $\{v_1,\dots,v_{p-1}\}$ of V such that

(i) $v_1,\dots,v_{p-1}\in\mathbb{Z}^n$;

(ii) $v_1,\dots,v_{p-1}$ may be extended to a basis $v_1,\dots,v_{p-1},w_1,\dots,w_{p-1}$ of $\mathbb{Z}^n$.

Expressing the matrices in Γ by means of this basis we may suppose that they have zeros in the lower $(p-1)\times(p-1)$ left corner. For $\sigma\in\Gamma$ we denote

$$\sigma=\begin{pmatrix}\omega_1(\sigma) & \omega_2(\sigma)\\ 0 & \omega_3(\sigma)\end{pmatrix},$$

where $\omega_i(\sigma)$ are $(p-1)\times(p-1)$ matrices over $\mathbb{Z}$. Observe that $\omega_1,\omega_3:\Gamma\to \mathrm{GL}_{p-1}(\mathbb{Z})$ are homomorphisms. Since $\sigma^p=1$ for each $\sigma\in\Gamma$, we see that either

$\sigma = 1$ or there exists at least one eigenvalue of σ different from 1. In fact, σ is diagonalizable (since it satisfies the separable equation $X^p - 1 = 0$).

In particular $\sigma \mapsto (\omega_1(\sigma), \omega_3(\sigma))$ is injective.

Also, $\ker \omega_i$ cannot be trivial for $i = 1$ or $i = 3$, since Γ cannot be embedded in $\mathrm{GL}_{p-1}(\mathbb{Z})$ (by the mentioned result in [1], *i.e.* (b) above). Hence Γ is generated by matrices α, β as follows:

$$\alpha = \begin{pmatrix} I & M \\ 0 & A \end{pmatrix} \qquad \beta = \begin{pmatrix} B & N \\ 0 & I \end{pmatrix},$$

for suitable integral $(p-1)\times(p-1)$ matrices A, B, M, N, with $A, B \in \mathrm{GL}_{p-1}(\mathbb{Z})$ (here I denotes the identity in $\mathrm{GL}_{p-1}(\mathbb{Z})$). Since neither α, nor β is the identity, both A and B have at least one eigenvalue distinct from 1, necessarily a primitive p-th root of 1. Therefore they must admit also the conjugate eigenvalues, which are $p-1$ in number. Hence they satisfy

$$\phi(A) = \phi(B) = 0, \quad \text{where } \phi(X) = X^{p-1} + \cdots + X + 1. \tag{4.2}$$

Since $\phi(X)$ is irreducible over $\mathbb{Q}$ necessarily it is the characteristic and minimal polynomial of both A, B.

We shall continue by proving that the minimal polynomial modulo p of both A and B is $\phi(X) \equiv (X-1)^{p-1} \pmod p$. Assume the contrary for A, say. Then $(A-I)^{p-2} \equiv 0 \pmod p$ and therefore $\det(A-I)^{p-2} \equiv 0 \pmod{p^{p-1}}$. In particular p^2 would divide $\det(A-I)$. On the other hand $\det(A-I) = \phi(1) = p$, since $\phi(X)$ is the characteristic polynomial of A.

We now let A, B act on $(\mathbb{Z}/(p))^{p-1}$ and look at their Jordan decomposition with respect to this action. By the above, we find that for $1 \le j \le p-2$,

$$\ker(A-I)^{p-j-1} = \mathrm{Im}(A-I)^j, \quad \ker(B-I)^{p-j-1} = \mathrm{Im}(B-I)^j. \tag{4.3}$$

Since α, β commute we readily get

$$(B-I)M + N(A-I) = 0. \tag{4.4}$$

Let now $\{Z_\sigma\}$ be a 1-cocycle with values in $(\mathbb{Z}/(p))^n$ representing a class in $H^1_{\mathrm{loc}}(\Gamma, (\mathbb{Z}/(p))^n)$, and write

$$Z_\sigma = (t_\sigma, \tilde{t}_\sigma), \quad t_\sigma, \tilde{t}_\sigma \in \big(\mathbb{Z}/(p)\big)^{p-1}.$$

By the local conditions, we may assume, subtracting a coboundary, that the restriction of Z to the subgroup H generated by α is zero. This automatically implies that Z_σ depends only on the class of σ modulo H. In particular $Z_{\alpha\beta} = Z_\beta$.

By the local condition for β we deduce at once that $\tilde{t}_\beta = 0$. In fact the local condition applied to Z_β gives the existence of $u, v \in (\mathbb{Z}/(p))^{p-1}$ such that

$$Z_\beta = \begin{pmatrix} B-I & N \\ 0 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Therefore we find $\tilde{t}_{\alpha\beta} = \tilde{t}_\beta = 0$ and $t_{\alpha\beta} = t_\beta$.

The local condition applied to $Z_{\alpha\beta}$ gives the existence of $u, v \in (\mathbb{Z}/(p))^{p-1}$ such that

$$t_{\alpha\beta} = (B-I)u + (M+N)v, \quad 0 = (A-I)v. \tag{4.5}$$

By (4.3) we have $v = (A-I)^{p-2}w$ for some $w \in (\mathbb{Z}/(p))^{p-1}$. We use (4.4) and (4.5) to compute

$$\begin{aligned}(B-I)^{p-2}t_{\alpha\beta} &= (B-I)^{p-2}Mv + (B-I)^{p-2}Nv \\ &= -(B-I)^{p-3}N(A-I)v + (B-I)^{p-2}N(A-I)^{p-2}w \\ &= -(B-I)^{p-1}M(A-I)^{p-3}w = 0.\end{aligned}$$

Therefore, by (4.3) again, we have $t_{\alpha\beta} \in \mathrm{Im}(B-I)$. Since $t_\beta = t_{\alpha\beta}$ we obtain the existence of $s \in (\mathbb{Z}/(p))^{p-1}$ such that

$$t_\beta = (B-I)s.$$

Put finally $W := (s, 0) \in (\mathbb{Z}/(p))^n$. We see that

$$(\alpha - I)W = 0 = Z_\alpha, \quad (\beta - I)W = (t_\beta, 0) = Z_\beta.$$

Therefore the cocycle $Z_\sigma - (\sigma - I)W$ vanishes on a set of generators of Γ, whence always vanishes, proving that Z_σ vanishes in $H^1(\Gamma, (\mathbb{Z}/(p))^n)$. We have proved that $H^1_{\mathrm{loc}}(G_p, (\mathbb{Z}/(p))^n) = 0$ and the theorem. □

Remark 4.4. — What we have obtained depends heavily on the possibility of lifting G_p to a subgroup of integral matrices. In fact, take *e.g.* $p = 3$, $n = 4$: we have seen in §3 that for a subgroup $G \subset \mathrm{GL}_4(\mathbb{Z}/(3))$, $G \cong (\mathbb{Z}/(3))^2$, it is not always true that $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(3))^4) = 0$.

5. A counterexample

It is likely that the conclusion $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) = 0$ may be obtained under an assumption weaker than $n \leq 2(p-1)$, by arguments similar to those in the proof of Theorem 4.1.

However, for given p, some condition on n is necessary, as shown by the example detailed below, suggested by Colliot-Thélène. This example implies that $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n)$ can be nonzero for a suitable subgroup G of $\mathrm{GL}_n(\mathbb{Z})$, $G \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$, provided n is a sufficiently large integer (note that the case $G \cong (\mathbb{Z}/(p))^2$ is the most relevant in Theorem 4.1). The actual value of n in the example below is $n = p^4 - p^2 + 1$, so there is a range of uncertainty localized in $2p - 1 \leq n \leq p^4 - p^2$. It would be interesting to establish the best possible bound for n in order to have $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) = 0$ for such a G.

Actually, the example below will lead not only to $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n) \neq 0$ but to a counterexample to the conclusion of Theorem 4.1. In fact, we shall produce a k-rational point which is almost always locally p-divisible but not

globally. We are indebted to Colliot-Thélène and to the referee for predicting this sharper conclusion and for hinting how it could be reached.

EXAMPLE 5.1. — *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 $T(k)$.*

Let $G = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$ and consider the standard projective resolution of $\mathbb{Z}$ as a G-module (see [3, Chap. IV, §2])

$$\cdots \longrightarrow \mathbb{Z}[G \times G] \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0;$$

letting M be the kernel of the map $\mathbb{Z}[G \times G] \to \mathbb{Z}[G]$, we obtain an exact sequence

$$0 \to M \longrightarrow \mathbb{Z}[G \times G] \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0. \tag{5.1}$$

For a G-module X, let $X^0 = \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$; then we have a dual exact sequence

$$0 \to \mathbb{Z} \longrightarrow \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z}[G \times G] \xrightarrow{\beta} M^0 \to 0. \tag{5.2}$$

The exact sequence (5.2) can be split in the two parts

$$0 \to \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow N \to 0$$

and

$$0 \to N \longrightarrow \mathbb{Z}[G \times G] \longrightarrow M^0 \to 0$$

(here $N = I_G = \mathrm{Im}(\alpha) = \ker \beta$). It follows that there are isomorphisms

$$H^1(G, M^0) \cong H^2(G, N) \cong H^3(G, \mathbb{Z}),$$

$$H^1(C, M^0) \cong H^2(C, N) \cong H^3(C, \mathbb{Z})$$

for each cyclic subgroup $C \subset G$ (note that $\mathbb{Z}[G]$ and $\mathbb{Z}[G \times G]$ are both G- and C-free modules). By [10, Chap. I.4.4, Prop. 28], we have

$$H^3(G, \mathbb{Z}) \cong \mathbb{Z}/(p), \quad H^3(C, \mathbb{Z}) = 0,$$

whence

$$H^1(G, M^0) \cong \mathbb{Z}/(p), \quad H^1(C, M^0) = 0.$$

Next, consider the exact sequence

$$0 \to M^0 \xrightarrow{p} M^0 \xrightarrow{\pi} M^0/pM^0 \to 0.$$

We get a corresponding cohomology exact sequence

$$H^1(G, M^0) \xrightarrow{\bar{p}} H^1(G, M^0) \xrightarrow{\bar{\pi}} H^1(G, M^0/pM^0).$$

Since $H^1(G, M^0) \cong \mathbb{Z}/(p)$ is annihilated by the multiplication by p, $\mathrm{Im}(\bar{p}) = 0$ whence $\bar{\pi}$ is injective and

$$H^1(G, M^0/pM^0) \neq 0.$$

Finally consider the commutative diagram (see [8, Chap. VIII.2, Prop. 2])

$$\begin{array}{ccc} H^1(G,M^0) & \xrightarrow{\text{Res}} & \prod_C H^1(C,M^0)=0 \\ \downarrow \bar{\pi} & & \downarrow \bar{\pi} \\ H^1(G,M^0/pM^0) & \xrightarrow{\text{Res}} & \prod_C H^1(C,M^0/pM^0). \end{array}$$

Since $\bar{\pi}$ is injective, we get

$$0 \neq \mathrm{Im}(\bar{\pi}) \subset H^1_{\mathrm{loc}}(G,M^0/pM^0). \tag{5.3}$$

Because of the obvious isomorphisms as abelian groups, we may identify M^0 with $\mathbb{Z}^n$ and M^0/pM^0 with $(\mathbb{Z}/(p))^n$, where $n=p^4-p^2+1$. Also, the action of G on M^0 corresponds to a map $\psi : G \to \mathrm{GL}_n(\mathbb{Z})$.

For any choice of number fields $k \subset L$ such that $\mathrm{Gal}(L/k) \cong G$ we may define a k-torus T with splitting field L by giving the homomorphism ψ. If $k \supset \mathbb{Q}(\zeta_p)$, we have seen in Section 4 that the action of G on $T[p]$ corresponds to the action of G on M^0/pM^0, hence

$$H^1_{\mathrm{loc}}\big(G,T[p]\big) \neq 0,$$

which is the first result claimed. To complete the picture, we shall show that this leads to a counterexample to our local-global principle for p-divisibility.

Note that equation (5.3) not only shows that $H^1_{\mathrm{loc}}(G,M^0/pM^0) \neq 0$, but also that there is a non-trivial element $[\omega] \in H^1_{\mathrm{loc}}(G,M^0/pM^0)$ which is the image under $\bar{\pi}$ of an element $[\rho]$ of $H^1(G,M^0)$. In fact, $[\rho] \in H^1_{\mathrm{loc}}(G,M^0)$.

Let $\sigma \mapsto \rho_\sigma \in \mathbb{Z}^n \cong M^0$ be 1-cocycle representing $[\rho]$ and let $\sigma \mapsto \omega_\sigma \in (\mathbb{Z}/(p))^n$ be its reduction mod pM^0. Then, for $\sigma,\tau \in G$,

$$\rho_{\sigma\tau} = \rho_\sigma + \psi(\sigma)\rho_\tau \tag{5.4}$$

and

$$\begin{aligned} &\text{(i)} && \tilde{\rho}_\sigma = \omega_\sigma, \\ &\text{(ii)} && \omega_{\sigma\tau} = \omega_\sigma + \widetilde{\psi(\sigma)}\omega_\tau, \end{aligned} \tag{5.5}$$

where the tilde denotes reduction mod p.

Next, we sum (5.4) over $\tau \in G$ and we let $S = \sum_{\tau\in G} \rho_\tau$. We get

$$p^2\rho_\sigma = \big(1-\psi(\sigma)\big)S. \tag{5.6}$$

From now on, we find it convenient to use the isomorphism ϕ and view the abelian group $T(\bar{k})$ as $\mathbb{G}_m^n(\bar{k}) \cong \bar{k}^{*n}$. Correspondingly, we adopt the multiplicative notation in this final part of the paper.

However, the Galois action on $T(\bar{k})$, read in $\bar{k}^{*n}$, is not the usual one, but gets twisted by ψ. (In fact, in general, we have $T(F) \neq F^{*n}$ for an algebraic extension F of k.)

To be precise, let $P = (x_1, \dots, x_n) \in \bar{k}^{*n}$ and let $\sigma \in G_k$. Viewing P as an element of $T(\bar{k})$, we have

$$P^\sigma = (\sigma(x_1) \dots, \sigma(x_n))^{\psi(\sigma)},$$

where, for a matrix $M = (m_{ij}) \in M_n(\mathbb{Z})$, we put

$$(y_1, \dots, y_n)^M = \Big(\prod_{i=1}^n y_j^{m_{1j}}, \dots, \prod_{i=1}^n y_j^{m_{nj}} \Big). \tag{5.7}$$

The proof of this formula is a straightforward application of the definitions. For later purpose, we also define, for a vector $\mathbf{m} = (m_1, \dots, m_n)$,

$$(y_1, \dots, y_n)^{\mathbf{m}} = y_1^{m_1} \cdots y_n^{m_n}.$$

Before using equation (5.6), we make a definite choice of the fields k and L. We let $k = \mathbb{Q}(\zeta_{p^3})$, L' be a normal extension of $\mathbb{Q}$ with Galois group G and linearly disjoint from k, and $L = L'k$. Note that L' can be obtained, for instance, as a suitable subfield of $\mathbb{Q}(\zeta_{q_1 q_2})$, where q_1, q_2 are distinct primes congruent to 1 mod p.

Let $\gamma \in k$ be a primitive p^3-th root of unity and let $\zeta = \gamma^{p^2}$. Let also

$$Q = (\zeta, \dots, \zeta) \in T[p].$$

Consider the map $\sigma \mapsto Z_\sigma := Q^{\rho_\sigma}$, where ρ_σ is the cocycle with values in $\mathbb{Z}^n \cong M^0$ defined above. Recall that the reduction mod p, $\{\omega_\sigma\}$, of $\{\rho_\sigma\}$ is a non-trivial cocycle in $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(p))^n$. One immediately verifies that

(i) $\sigma \mapsto Z_\sigma$ is a 1-cocycle with values in $T[p]$;

(ii) $\sigma \mapsto Z_\sigma$ represents a non-trivial class in $H^1_{\mathrm{loc}}(G, T[p])$.

By the definition of γ, we have

$$Q = R^{p^2}, \quad R = (\gamma, \dots, \gamma).$$

In view of (5.6) we have

$$Z_\sigma = R^{p^2 \rho_\sigma} = R^{(1-\psi(\sigma))S}.$$

Moreover, since $\sigma(\gamma) = \gamma$ for all $\sigma \in G$, (5.7) yields

$$Z_\sigma = D/D^\sigma, \quad \text{where } D = R^S.$$

It follows that the point $P = D^p$ is almost always locally p-divisible, but not globally. Note that, although $D \in k^{*n}$, D does not lie in $T(k)$ but only in $T(L)$. On the contrary, $P = D^p \in T(k)$.

In the example just given, the torus and the point P are defined over a number field k. We can get a similar example with a torus and a point defined over $\mathbb{Q}$ at the cost of increasing the dimension. For this purpose, we consider

the torus obtained by restriction of scalars $\tilde{T} = R_{k/\mathbb{Q}}(T)$ (see [11, Chap. 1, §3.12, Ex. 18]). Then $\tilde{T}$ is defined over $\mathbb{Q}$,

$$\dim \tilde{T} = p^2(p-1)\dim T = p^2(p-1)(p^4-p^2+1),$$

and there is a bijection between $T(k)$ and $\tilde{T}(\mathbb{Q})$.

The point $\tilde{P} \in \tilde{T}(\mathbb{Q})$ corresponding to $P \in T(k)$ has the desired properties.

REMARK 5.2. — Throughout the paper we have worked with the condition that a point P be divisible in $\mathcal{A}(k_v)$ for almost all v. However, sometimes the Hasse principle holds only under the stronger assumption that the local conditions are satisfied for all v. We can ask what happens in our situation, and in particular in Example 5.1, by imposing this stronger assumption.

We contend that examples like 5.1 exist even with the stronger assumption. In fact, the whole machinery continues to work whenever all the local Galois groups $\mathrm{Gal}(L_w/k_v)$ are cyclic. This is automatically true for the non-ramified primes v. For the ramified ones (in our example, the primes dividing q_1q_2), it may be shown that this condition is guaranteed by the following:

$$q_1 \equiv 1 \bmod p \text{ and } q_2 \text{ splits completely in } \mathbb{Q}(\zeta_{pq_1}, \sqrt[p]{q_1}).$$

Here are some numerical examples of choices of (p, q_1, q_2) that satisfy this condition:

$$(2,5,11),\ (3,7,337),\ (5,151,22651).$$

For every given p, the existence of infinitely many pairs (q_1, q_2) such that (p, q_1, q_2) satisfies the condition is an easy consequence of well-known results in algebraic number theory.

BIBLIOGRAPHY

[1] BOURBAKI (N.) – *Groupes et algèbres de Lie*, ch. 2 et 3, Hermann, Paris, 1972.

[2] CASSELS (J.W.S.) – *An introduction to the geometry of numbers*, 2nd ed., Springer Verlag, 1971.

[3] CASSELS (J.W.S.) & FRÖHLICH (A.), eds. – *Algebraic Number Theory*, Academic Press, 1967.

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

[5] LANG (S.) – *Algebra*, 3rd ed., Addison-Wesley, 1993.

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

[7] SERRE (J.-P.) – *Représentations linéaires des groupes finis*, Hermann, Paris, 1967.

[8] _____, *Local Fields*, Springer Verlag, 1979.
[9] _____, *Algebraic Groups and Class Fields*, Springer Verlag, 1988.
[10] _____, *Cohomologie galoisienne*, 5th ed., Lecture Notes in Math., vol. 5, Springer Verlag, 1994.
[11] Voskresenskiĭ (V.E.) – *Algebraic groups and their birational invariants*, AMS Transl. Math. Monographs, vol. 179, Amer. Math. Soc., 1998.
[12] Weil (A.) – *Adèles and algebraic groups*, Birkhäuser, 1982.