RESEARCH ARTICLE

Local–global divisibility on algebraic tori

Jessica Alessandrì[1] ⓘ | **Rocco Chirivì**[2] ⓘ | **Laura Paladino**[3] ⓘ

[1]Università degli Studi dell'Aquila, Coppito (AQ), Italy

[2]Università del Salento, Monteroni di Lecce (LE), Italy

[3]Università della Calabria, Rende (CS), Italy

Correspondence
Jessica Alessandrì, Università degli Studi dell'Aquila, Via Vetoio, Coppito 1 67100, Coppito (AQ), Italy.
Email:
jessica.alessandri@graduate.univaq.it

Abstract

We give a complete answer to the local–global divisibility problem for algebraic tori. In particular, we prove that given an odd prime p, if T is an algebraic torus of dimension $r < p - 1$ defined over a number field k, then the local–global divisibility by any power p^n holds for $T(k)$. We also show that this bound on the dimension is best possible, by providing a counterexample for every dimension $r \geqslant p - 1$. Finally, we prove that under certain hypotheses on the number field generated by the coordinates of the p^n-torsion points of T, the local–global divisibility still holds for tori of dimension less than $3(p - 1)$.

MSC 2020
11E72 (primary), 11G35, 14G05 (secondary)

1 | INTRODUCTION

Let k be a number field and let $\mathcal{G}$ be a commutative algebraic group defined over k. We denote by M_k the set of places of k and by k_v the completion of k at v. In 2001, Dvornicich and Zannier, motivated by a particular case of the Hasse principle for binary quadratic forms, stated the following problem, which is known as the *local–global divisibility problem* (see [9]).

Problem 1.1 (Dvornicich and Zannier [9]). Let q be a fixed positive integer. If we assume that the point $P \in \mathcal{G}(k)$ has the following property: for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$; can we conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$?

Clearly, it is sufficient to answer the problem when q is a power of a prime. The classical case of the multiplicative group $\mathcal{G} = \mathbb{G}_m$ has a complete answer: positive for q not divisible by

8 (see, e.g., [1, 9]) and negative for q divisible by 8 (see [21]). For a general commutative algebraic group, Dvornicich and Zannier gave in [9] a cohomological interpretation of the problem and sufficient conditions to answer the question (see also [10]). In particular, they showed that such an answer is linked to the triviality of a subgroup of $H^1(\mathrm{Gal}(k(\mathcal{G}[q])/k), \mathcal{G}[q])$, where $k(\mathcal{G}[q])$ is the field obtained by adjoining the coordinates of the q-torsion points of $\mathcal{G}$ to k, called the *first local cohomology group* (see Section 2 for further details).

By using these tools, it was possible to give criteria to answer the local–global divisibility problem for several algebraic groups. In the case of elliptic curves, the problem was long studied. The answer is affirmative for $q = 2, 3$ and for all powers $q = p^n$, with $p > C([k : \mathbb{Q}])$, where $C([k : \mathbb{Q}]) = 3$, if $k = \mathbb{Q}$, and $C([k : \mathbb{Q}]) = (3^{\frac{[k:\mathbb{Q}]}{2}} + 1)^2$, if $k \neq \mathbb{Q}$ (see the recent survey [8] for further details; see also [6]). Instead, for $q = p^n$, with $p = 2, 3$ and $n \geqslant 2$, there are known counterexamples over $\mathbb{Q}$ and over $\mathbb{Q}(\zeta_3)$ (when $p = 3$) [5, 16]. For each number field k linearly disjoint over $\mathbb{Q}$ (resp. over $\mathbb{Q}(\zeta_3)$) from the p^n-division field of $\mathcal{E}$ over $\mathbb{Q}$ (resp. over $\mathbb{Q}(\zeta_3)$), these counterexamples also give counterexamples in a finite extension of k (see Remark 3.5 for further details). While there are no explicit counterexamples for $p \geqslant 5$ over a number field k, in [18] necessary conditions on $\mathrm{Gal}(k(\mathcal{E}[p])/k)$ that have to be satisfied in order to have local–global divisibility by p^n for a prime $p \geqslant 5$ are given. In addition, for elliptic curves, an effective version of the hypotheses of Problem 1.1 is produced in [7]. For principally polarized abelian surfaces in [12], Gillibert and Ranieri proved sufficient conditions for the local–global divisibility by any prime power p^n, while in [13], they generalized these conditions in order to answer the case of GL_2-type varieties (see also [11]). Furthermore, in [17], the third author produced conditions for the local–global p-divisibility for a general commutative algebraic group. In the case of abelian varieties, the problem is also linked to a classical question posed by Cassels in 1962 on the p-divisibility of the Tate–Shafarevich group (see [2–4, 8]).

In this work, we focus on algebraic tori. As mentioned above, for the one-dimensional split torus $\mathbb{G}_m$, we have a complete answer. Notice that the negative answer for $q = 2^n$, with $n \geqslant 3$, implies that one can find counterexamples in every dimension, just by taking direct products of copies of $\mathbb{G}_m$. In [9], Dvornicich and Zannier proved that the local–global divisibility by a prime p holds for tori of dimension $r \leqslant \max\{3, 2(p-1)\}$, but fails for a torus of dimension $r = p^4 - p^2 + 1$. In this last case, they produced a k-rational point that is locally p-divisible for all but finitely many places $v \in M_k$, but not globally p-divisible. In [14], Illengo improved the condition $r \leqslant 2(p-1)$ given by Dvornicich and Zannier with the weaker one $r < 3(p-1)$. He also proved that this bound is best possible, by building an example with $r = 3(p-1)$ for which the local–global divisibility by p fails.

In this work, we prove that the local–global divisibility by any odd power p^n, with $n \geqslant 1$, holds for an algebraic torus of dimension $r < p-1$. In particular, we prove that if $r < p-1$, then we have an affirmative answer to Problem 1.1, while for $r \geqslant p-1$, the local–global divisibility by p^n, with $n \geqslant 2$, is no longer assured. For the latter, we construct a counterexample of dimension $p - 1$ for which the local–global divisibility by every p^n with $n \geqslant 2$ does not hold. We remark that, starting from this construction, one can build a counterexample for every dimension $r \geqslant p-1$, by taking the product of the torus that we build in Lemma 3.1 with the split torus of dimension $r - (p-1)$. We summarize these results in the following theorem, that we prove in Section 3:

Theorem 1.2. *Let p be an odd prime.*

(a) *Let k be a number field and let T be a torus defined over k. If T has dimension less than $p-1$, then the local–global divisibility by p^n holds for $T(k)$, for every $n \geqslant 1$.*

(b) *For every $n \geqslant 2$ and for every $r \geqslant p - 1$, there exists a torus T defined over $k = \mathbb{Q}(\zeta_p)$ of dimension r and a finite extension L/k such that the local–global divisibility by p^n does not hold for $T(L)$.*

Nevertheless, under certain conditions on the base field k, satisfied, for example, by adjoining a primitive p^nth root of unity to k, we can say something more when $p - 1 \leqslant \dim(T) < 3(p - 1)$. Let $k(T[p^n])$ be the field obtained by adjoining the coordinates of the p^n-torsion points of T to k. In Section 4, we prove the following.

Theorem 1.3. *Let p be an odd prime and let $n \geqslant 1$ be an integer. Suppose that T is a torus defined over k with $p - 1 \leqslant \dim(T) < 3(p - 1)$ and p does not divide the degree $[k(T[p^n]) \cap k(\zeta_{p^n}) : k]$, where ζ_{p^n} is a p^nth root of unity. Then, the local–global divisibility by p^n holds for $T(k)$.*

We remark that, since the proof of this theorem is done by induction on the powers of p, we need the condition $\dim(T) < 3(p - 1)$ for the base of the induction.

2 │ PRELIMINARY RESULTS

As mentioned above, a useful method introduced by Dvornicich and Zannier in [9] in dealing with this problem is to translate it into cohomological terms. Let us recall some definitions and results.

Let $\mathcal{G}$ be a commutative algebraic group, defined over a number field k. Given a positive integer q, we denote by $\mathcal{G}[q]$ the set of q-torsion points of $\mathcal{G}(\overline{k})$. It is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^{\ell}$, for some ℓ depending only on $\mathcal{G}$ (see, e.g., [9, Section 2]).

Let $K := k(\mathcal{G}[q])$ be the number field generated by adjoining to k the coordinates of the q-torsion points of $\mathcal{G}$. It is a Galois extension of k and we denote by G its Galois group. Let Σ be the set of places v unramified in K and let $G_v = \mathrm{Gal}(K_w/k_v)$, where w is a place of K extending $v \in \Sigma$.

In [9], the authors introduce a subgroup of $\mathrm{H}^1(G, \mathcal{G}[q])$ called the *first local cohomology group*:

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{v \in \Sigma} \ker \left(\mathrm{H}^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} \mathrm{H}^1(G_v, \mathcal{G}[q]) \right). \tag{1}$$

By Čebotarev density theorem, the Galois groups G_v run over all cyclic subgroups of G, as v varies in Σ. Therefore, a cocycle $\{Z_\sigma\}_{\sigma \in G}$ in $\mathrm{H}^1(G, \mathcal{G}[q])$ is an element in $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ if and only if for every $\sigma \in G$, there exists $W_\sigma \in \mathcal{G}[q]$ such that $Z_\sigma = (\sigma - 1)W_\sigma$ (see [9] and [8] for further details). This justifies the following, more general, definition.

Definition 2.1 (Dvornicich and Zannier [9]). Let G be a group and let M be a G-module. We say that a cocycle $\{Z_g\}_{g \in G}$ of G with values in M *satisfies the local conditions* if there exist $W_g \in M$ such that $Z_g = (g - 1)W_g$ for all $g \in G$. We denote by $\mathrm{H}^1_{\mathrm{loc}}(G, M)$ the subgroup of $\mathrm{H}^1(G, M)$ of the classes of these cocycles.

As mentioned, it is sufficient to consider the case when q is a prime power, thus from now on, let $q = p^n$, for some prime number p and some positive integer n. By [9, Proposition 2.1], the triviality of the first local cohomology group gives a sufficient condition for an affirmative answer to Problem 1.1.

Proposition 2.2 (Dvornicich and Zannier [9]). *Assume that* $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{G}[q]) = 0$. *Let* $P \in \mathcal{G}(k)$ *be a rational point with the following property: for all but finitely many primes* v *of* k, *there exists* $D_v \in \mathcal{G}(k_v)$ *such that* $P = qD_v$. *Then there exists* $D \in \mathcal{G}(k)$ *such that* $P = qD$.

Furthermore, by [9, Theorem 2.5], it is enough to prove that $\mathrm{H}^1_{\mathrm{loc}}(G_p, \mathcal{G}[q]) = 0$ for a p-Sylow subgroup G_p of G. Moreover, the converse of Proposition 2.2 is also true over a finite extension of k, as the following theorem by Dvornicich and Zannier shows.

Theorem 2.3 [10, Theorem 3]. *Suppose that* $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ *is not trivial. Then there exists a number field* L *such that* $L \cap K = k$ *and a point* $P \in \mathcal{G}(L)$ *which is divisible by* q *in* $\mathcal{G}(L_w)$ *for all places* w *of* L *but is not divisible by* q *in* $\mathcal{G}(L)$.

We remark that if in (1), we take all valuations, instead of almost all, then we get a group isomorphic to the Tate–Shafarevich group $\Sha(k, \mathcal{G}[q])$. Thus, the vanishing of $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ implies the vanishing of $\Sha(k, \mathcal{G}[q])$, which is a sufficient condition to give an affirmative answer to the local–global divisibility problem in the case when v runs over all valuations of k (see, e.g., [5]).

Let us now introduce some notation for algebraic tori that we will use in the next sections. We adopt the same notation as in [9, Section 4]. Let T be an algebraic torus defined over a number field k, of dimension r. There exists an isomorphism of algebraic groups (defined over $\overline{k}$) $\phi : T \longrightarrow \mathbb{G}^r_m$. Let G_k be the absolute Galois group of k. For $\sigma \in G_k$, we denote by ϕ^σ the twist of ϕ by σ, that is, $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}$, and we consider the following map:

$$\psi : \quad G_k \quad \longrightarrow \quad \mathrm{Aut}(\mathbb{G}^r_m) \quad \simeq \mathrm{GL}_r(\mathbb{Z})$$
$$\sigma \quad \longmapsto \quad \phi \circ (\phi^\sigma)^{-1}.$$

Notice that ψ is a 1-cocycle, but since the action of G_k on $\mathrm{Aut}(\mathbb{G}^r_m)$ is trivial, ψ is actually a group homomorphism.

The isomorphism ϕ is defined over some number field, thus $\ker \psi$ has finite index in G_k and we can identify $\Delta := \psi(G_k)$ with a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$. We denote by L the field fixed by $\ker \psi$; it is a normal extension of k and $\Delta \simeq \mathrm{Gal}(L/k)$. The field L is also the splitting field of the torus T. Let $\zeta := \zeta_{p^n}$ be a primitive p^nth root of unity and let χ be the cyclotomic character

$$\chi : \quad G_k \quad \longrightarrow \quad (\mathbb{Z}/p^n\mathbb{Z})^\times$$
$$\sigma \quad \longmapsto \quad j_\sigma,$$

where j_σ is such that $\sigma(\zeta) = \zeta^{j_\sigma}$. Let $T[p^n]$ be the group of the p^n-torsion points of T. We have $T[p^n] = T(\overline{k})[p^n] \simeq \{(\zeta^{j_1}, \dots, \zeta^{j_r}) \in (\overline{k}^\times)^r \mid j_h \in \mathbb{Z}/p^n\mathbb{Z}\}$ and we fix the following isomorphism:

$$T[p^n] \quad \longrightarrow \quad (\mathbb{Z}/p^n\mathbb{Z})^r \tag{2}$$
$$(\zeta^{j_1}, \dots, \zeta^{j_r}) \quad \longmapsto \quad (j_1, \dots, j_r).$$

By this isomorphism, the natural action of G_k on $T[p^n]$ induces the following action on $(\mathbb{Z}/p^n\mathbb{Z})^r$: $\sigma \cdot v = j_\sigma \widetilde{\psi(\sigma)} v$ for all $v \in (\mathbb{Z}/p^n\mathbb{Z})^r$, where the tilde denotes the reduction mod p^n. Therefore,

we have the homomorphism

$$
\begin{array}{rcl}
\xi : & G_k & \longrightarrow & \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z}) \\
& \sigma & \longmapsto & j_\sigma \widetilde{\psi(\sigma)}.
\end{array}
\tag{3}
$$

It is easy to check that the field fixed by $\ker \xi$ is $K := k(T[p^n])$; thus, the image G of ξ in $\mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z})$ is a finite subgroup isomorphic to $G_k/\ker \xi \simeq \mathrm{Gal}(K/k)$. Let $G_{k(\zeta)}$ be the subgroup $\mathrm{Gal}(\overline{k}/k(\zeta))$ of G_k. We have $L = \overline{k}^{\ker \psi}$ and $K = \overline{k}^{\ker \xi}$, since $\ker \xi \supseteq \ker \psi \cap G_{k(\zeta)}$, we also get $K \subseteq L(\zeta)$. The kernel of the restriction of ξ to $G_{k(\zeta)}$ is contained both in $\ker \xi$ and in $\ker \widetilde{\psi}$. It follows that the image of $G_{k(\zeta)}$ via ξ is a normal subgroup G' of G, which is also a normal subgroup of the reduction $\widetilde{\Delta}$ modulo p^n of Δ. In particular, we have the following tower of extensions:
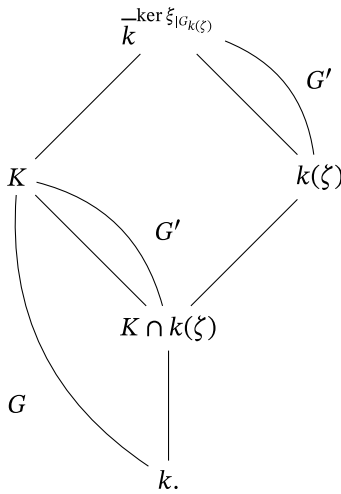
We have obtained that G and $\widetilde{\Delta}$ have a common normal subgroup G', with $[G : G'] \mid p^{n-1}(p-1)$ and $[\widetilde{\Delta} : G'] \mid p^{n-1}(p-1)$. In [9], the authors can easily conclude that G and $\widetilde{\Delta}$ also have the same p-Sylow subgroups (since in their situation both $[G : G']$ and $[\widetilde{\Delta} : G']$ are coprime with p), and thus, they reduce themselves to study only the p-Sylow subgroups in $\widetilde{\Delta}$. Instead, in our general setting for the divisibility by p^n problem, we have to distinguish two cases: either $p \mid [G : G']$ or $p \nmid [G : G']$.

The following theorem (see [19, Theorem 6.1.16]) will be a precious tool in proving part (a) of Theorem 1.2.

Theorem 2.4. *A subgroup of a quotient is a p-Sylow subgroup if and only if it is the image through the canonical projection homomorphism of a p-Sylow subgroup.*

In the proof of Theorem 1.3, we will also need the following well-known result (see p. 197 of [15]) whose proof we include for the reader's convenience (for a more general result, see [20]).

Lemma 2.5. *Let p be an odd prime and let $\pi : \mathrm{GL}_r(\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ be the reduction modulo p. Then π is injective on finite subgroups of $\mathrm{GL}_r(\mathbb{Z})$.*

Proof. It is enough to show that if $A \in \ker \pi$ and A has finite order m, then $A = \mathrm{Id}$. Suppose that instead, $A \neq \mathrm{Id}$. If $p \nmid m$, then write $A = 1 + p^k B$, with $k \geq 1$ and $B \in \mathrm{Mat}_r(\mathbb{Z})$ such that p does not divide at least one of the entries of B. We have

$$1 = A^m = \sum_{j=0}^{m} \binom{m}{j} p^{jk} B^j = 1 + mp^k B + \sum_{j=2}^{m} \binom{m}{j} p^{kj} B^j.$$

Thus, $mp^k B = -p^{k+1} C$, for some $C \in \mathrm{Mat}_r(\mathbb{Z})$ and so $mB = -pC$, which is a contradiction. On the other hand, if $p \mid m$, then $\overline{A} := A^{m/p}$ has order p and lies in $\ker \pi$. We have $\overline{A} = 1 + p^k \overline{B}$ with $k \geq 1$ and $\overline{B} \in \mathrm{Mat}_r(\mathbb{Z})$ such that p does not divide at least one of the entries of $\overline{B}$. We have

$$1 = \overline{A}^p = \sum_{j=0}^{p} \binom{p}{j} p^{jk} \overline{B}^j = 1 + p^{k+1} \overline{B} + \sum_{j=2}^{p-1} \binom{p}{j} p^{kj} \overline{B}^j + p^{pk} \overline{B}^p.$$

Since $p \neq 2$ and $k \geq 1$, we get $p^{k+1} \overline{B} = -p^{k+2} \overline{C}$, for some $\overline{C} \in \mathrm{Mat}_r(\mathbb{Z})$, so $B = -p\overline{C}$ and we have again a contradiction. $\square$

Finally, we state the following lemma by Illengo; this is a key result for the local–global divisibility in algebraic tori and we will use it in the proof of Theorem 1.2.

Lemma 2.6 [14, Lemma 4]. *Let p be a prime and let Γ be a p-group of matrices in $\mathrm{SL}_r(\mathbb{Q})$. If $r < p(p-1)$, then Γ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^b$, for some $b \leq r/(p-1)$.*

3 | PROOF OF THEOREM 1.2

In this section, we prove Theorem 1.2. With the notation as above, we show that:

(a) let p be an odd prime number and let $n \geq 1$ be an integer, then for every algebraic torus T of dimension $r < p - 1$, we have $\mathrm{H}^1_{\mathrm{loc}}(G_p, T[p^n]) = 0$, where G_p is a p-Sylow subgroup of G. Hence, by [9, Proposition 2.5], Problem 1.1 has affirmative answer;

(b) for every odd prime number p and every positive integer $n \geq 2$, there exists a torus T defined over $\mathbb{Q}(\zeta_p)$ of dimension $p - 1$ such that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \neq 0$. Thus, by Theorem 2.3, there exists a number field in which the local–global divisibility by p^n with $n \geq 2$ does not hold in T.

The counterexample in (b) shows that the bound on the dimension of T is best possible.

Since point (b) requires more effort, we start by showing a few results that we will use for its proof. The first step is building a torus such that G is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Lemma 3.1. *Let p be an odd prime and let $n \geq 2$. There exists an algebraic torus T of dimension $r = p - 1$ defined over $k = \mathbb{Q}(\zeta_p)$ such that G is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$. In particular, $G \subseteq \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z})$ is generated by*

$$\gamma_1 = \begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -1 \\ & & & 1 & -1 \end{pmatrix} \quad and \quad \gamma_2 = \begin{pmatrix} p+1 & & \\ & \ddots & \\ & & p+1 \end{pmatrix}.$$

Proof. Let L be a Kummer extension of k, such that $[L : k] = p$ and a prime other than p ramifies, for example, take $L = k(\sqrt[p]{2})$. Then, $L \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}$ and L/k is a cyclic extension of degree p. Let σ be a generator of $\mathrm{Gal}(L/k)$. Consider the split torus $\mathbb{G}_m = \mathbb{G}_{m,L}$ defined over L. We denote the group $\mathbb{G}_m[p^n]$ by $V \simeq \mathbb{Z}/p^n\mathbb{Z}$ using additive notation. The Galois action on V is given by the cyclotomic character $\chi : G_k \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $X = R_{L/k}\mathbb{G}_m$ be the Weil restriction of $\mathbb{G}_m$. It is an algebraic torus defined over k of dimension p, split over L. The group $X[p^n]$ of the p^n-torsion points of X is a free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank p and by properties of the Weil restriction, we have that

$$X[p^n] \simeq \prod_{j=0}^{p-1} V_j,$$

where V_j is an isomorphic copy of V, for every j. Let us choose a lifting $\overline{\sigma} \in G_k$ of σ. For every $\tau \in G_L = \mathrm{Gal}(\overline{k}/L)$ and $0 \leqslant h \leqslant p - 1$, the action of an element $\gamma = \tau\overline{\sigma}^h \in G_k$ on $X[p^n]$ is given by

$$\gamma \cdot (x_0, x_1 \dots, x_{p-1}) = \tau\overline{\sigma}^h \cdot (x_0, x_1 \dots, x_{p-1})$$

$$= \chi(\gamma)(x_{-h}, x_{-h+1}, \dots, x_{-h-1}), \tag{4}$$

where we are considering the indices of the coordinates modulo p.

Now let T be the norm 1 subtorus of X, that is, $T = R_{L/k}^{(1)}\mathbb{G}_m = \ker(R_{L/k}\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m)$, the kernel of the (generalized) norm map on X. It is an algebraic torus over k of dimension $r = p - 1$, split over L. We are going to show that $k(T[p^n]) = L(\zeta_{p^n})$.

Through the isomorphism (2) applied to $X[p^n]$, we can regard $T[p^n]$ as the submodule W of $X[p^n]$ of those vectors $(x_0, x_1 \dots, x_{p-1})$ such that the sum of all coordinates is equal to zero (we are using the additive notation here). The Galois action on $T[p^n]$ is given by $\xi : G_k \longrightarrow \mathrm{Aut(W)}$, that is, by the action on the points of $X[p^n]$ that lie in W (see (3)). We have that $k(T[p^n]) = \overline{k}^{\ker \xi}$. Thus, in order to determine this field, we need to find the elements of G_k that act trivially on W.

Since $p \geqslant 3$, by (4), we see that $\gamma = \tau\overline{\sigma}^h$ fixes every $(x_0, x_1 \dots, x_{p-1})$ in W if and only if $h = 0$ and $\chi(\gamma) = \chi(\tau) = 1$, that is, if and only if $\gamma \in G_L \cap G_{\mathbb{Q}(\zeta_{p^n})} = G_{L(\zeta_{p^n})}$. We therefore conclude that $k(T[p^n]) = L(\zeta_{p^n})$ as claimed.

Note that $L \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta_p) = k$, so the extension $k(T[p^n])/k$ has Galois group $\mathrm{Gal}(k(T[p^n])/k)$ and

$$\mathrm{Gal}(k(T[p^n])/k) \ni \varphi \longmapsto (\varphi_{|L}, \varphi_{|k(\zeta_{p^n})}) \in \mathrm{Gal}(L/k) \times \mathrm{Gal}(k(\zeta_{p^n})/k) \tag{5}$$

is an isomorphism. Further, it is clear that the last group is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Let $\eta \in \mathrm{Gal}(k(\zeta_{p^n})/k)$ be the automorphism sending ζ_{p^n} to $\zeta_{p^n}^{p+1}$; the two elements σ and η are generators of $\mathrm{Gal}(L/k) \times \mathrm{Gal}(k(\zeta_{p^n})/k)$. As noticed in the previous section, the group $\mathrm{Gal}(k(T[p^n])/k)$ is isomorphic to $G = \xi(G_k) \subseteq \mathrm{GL}_{p-1}(\mathbb{Z}/p^n\mathbb{Z})$. So, we want to represent σ and η as matrices in $\mathrm{GL}_{p-1}(\mathbb{Z}/p^n\mathbb{Z})$. We can choose the lifting $\overline{\sigma} \in G_k$ of σ such that, when restricted to $k(T[p^n])$, it corresponds to the pair $(\sigma, 1)$ in the isomorphism (5); in particular, $\chi(\overline{\sigma}) = 1$. With respect to the basis $v = (1, -1, 0, \dots, 0, 0)$, $\overline{\sigma}(v)$, $\overline{\sigma}^2(v), \dots, \overline{\sigma}^{p-2}(v)$ of W, we can write the matrix

$\gamma_1 = \xi(\overline{\sigma})$ corresponding to σ, as

$$\gamma_1 = \begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -1 \\ & & & 1 & -1 \end{pmatrix}.$$

To conclude the proof, we observe that, with a similar reasoning, we can lift η to $\overline{\eta} \in G_k$ in such a way that, when restricted to $k(T[p^n])$, the element $\overline{\eta}$ corresponds to the pair $(1, \eta)$ and, clearly, $\chi(\overline{\eta}) = p + 1$. Hence, the action of $\overline{\eta}$ on W is just by multiplication by $p + 1$; so, if $\gamma_2 = \xi(\overline{\eta})$, we have

$$\gamma_2 = \begin{pmatrix} p + 1 & & \\ & \ddots & \\ & & p + 1 \end{pmatrix}.$$

□

Remark 3.2. In the proof, we have explicitly described the homomorphism ξ in (3) of Section 2 in the particular case where T is the norm torus.

Recall from (2) that $T[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, hence we have a natural identification of $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n])$ with $\mathrm{H}^1_{\mathrm{loc}}(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1})$ by inducing the action of G on $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ via the same isomorphism. In the following proposition, we show that these groups are nontrivial.

Proposition 3.3. *Let p be an odd prime and let $n \geqslant 2$. Consider the action of G on $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ induced by the isomorphism $T[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ of (2). There exists a (unique) extension of*

$$\gamma_1 \longmapsto v_1 = \begin{pmatrix} p^{n-2}(p-1) \\ 0 \\ \vdots \\ 0 \\ p^{n-2} \end{pmatrix}, \quad \gamma_2 \longmapsto v_2 = \begin{pmatrix} p^{n-1} \\ \vdots \\ p^{n-1} \\ 0 \end{pmatrix}$$

to a cocycle in $\mathrm{H}^1(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1})$ and it is a nontrivial element of $\mathrm{H}^1_{\mathrm{loc}}(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1})$.

Proof. To check that the assigned vectors define a cocycle, we have to prove that in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$

$$(1 + \gamma_1 + \cdots + \gamma_1^{p-1})v_1 = \underline{0}, \tag{6}$$

$$(1 + \gamma_2 + \cdots + \gamma_2^{p^{n-1}-1})v_2 = \underline{0}, \tag{7}$$

$$(1 - \gamma_2)v_1 + (\gamma_1 - 1)v_2 = \underline{0}, \tag{8}$$

where $\underline{0}$ is the vector with all coordinates equal to zero; indeed, these conditions must be true since $\gamma_1^p = \gamma_2^{p^{n-1}} = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1} = 1$ in G. A lifting of γ_1 to $\mathrm{GL}_{p-1}(\mathbb{Q})$ is the matrix γ_1 itself. It solves the

polynomial $x^p - 1$ and it is easy to see that 1 is not an eigenvalue. Thus, the minimal polynomial of γ_1 is $x^{p-1} + x^{p-2} + \cdots + x + 1$, and so, (6) holds. Using $\gamma_2 = (p+1)\mathrm{Id}$, we have that

$$(1 + \gamma_2 + \cdots + \gamma_2^{p-1})v_2 = (1 + (p+1) + \cdots + (p+1)^{p-1})v_2 \equiv \underline{0} \mod p^n.$$

Since $n \geq 2$, we can collect the factor $1 + \gamma_2 + \cdots + \gamma_2^{p-1}$ on the left-hand side of (7), and hence, (7) holds. For (8), some simple calculations lead to:

$$(1 - \gamma_2)v_1 + (\gamma_1 - 1)v_2 \equiv \begin{pmatrix} p^{n-1} \\ 0 \\ \vdots \\ 0 \\ -p^{n-1} \end{pmatrix} + \begin{pmatrix} -p^{n-1} \\ 0 \\ \vdots \\ 0 \\ p^{n-1} \end{pmatrix} \equiv \underline{0} \mod p^n.$$

Thus, we can extend v_1 and v_2 to a cocycle $Z = \{Z_\gamma\}_{\gamma \in G}$, with $Z_{\gamma_1} = v_1$ and $Z_{\gamma_2} = v_2$. We now prove that Z is not trivial. Suppose that it is a coboundary, then there exists $w \in (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that $v_1 = (\gamma_1 - 1)w$ and $v_2 = (\gamma_2 - 1)w$. We denote with $w^{(i)}$ the ith coordinate of w. From $v_2 = (\gamma_2 - 1)w$, we have $v_2 = pw$, so that $pw^{(p-1)} = 0$. On the other hand, from $v_1 = (\gamma_1 - 1)w$, we have

$$v_1 = \begin{pmatrix} p^{n-2}(p-1) \\ 0 \\ \vdots \\ 0 \\ p^{n-2} \end{pmatrix} = \begin{pmatrix} -1 & & & & -1 \\ 1 & -1 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & -1 & -1 \\ & & & 1 & -2 \end{pmatrix} \begin{pmatrix} w^{(1)} \\ w^{(2)} \\ \vdots \\ \vdots \\ w^{(p-1)} \end{pmatrix}. \tag{9}$$

Thus, we obtain the system

$$\begin{cases} -w^{(1)} - w^{(p-1)} = p^{n-2}(p-1) \\ w^{(1)} - w^{(2)} - w^{(p-1)} = 0 \\ \vdots \\ w^{(p-3)} - w^{(p-2)} - w^{(p-1)} = 0 \\ w^{(p-2)} - 2w^{(p-1)} = p^{n-2}. \end{cases} \tag{10}$$

By adding the equations in (10), we get $p^{n-1} = -pw^{(p-1)}$, in contradiction with $pw^{(p-1)} = 0$. Therefore, Z is not a trivial cocycle in $\mathrm{H}^1(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1})$.

We are left to show that Z satisfies the local conditions. It is easy to see that the elements γ_2^h and $\gamma_1\gamma_2^h$, for $h = 0, 1, \ldots, p^{n-1} - 1$ are generators of all the cyclic subgroups of G. So, it is enough to show that there exist $W_{\gamma_2^h}$ and $W_{\gamma_1\gamma_2^h}$ in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that $Z_{\gamma_2^h} = (\gamma_2^h - 1)W_{\gamma_2^h}$ and $Z_{\gamma_1\gamma_2^h} = (\gamma_1\gamma_2^h - 1)W_{\gamma_1\gamma_2^h}$ for all $h \in \{0, 1, \ldots, p^{n-1} - 1\}$. First, since $\gamma_2 - 1 = p\mathrm{Id}$, we have that the image of $\gamma_2 - 1$ is the submodule M of $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ of vectors with each coordinate divisible by p. The vector v_2 satisfies this condition, so there exists $W_{\gamma_2} \in (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that $v_2 = Z_{\gamma_2} = (\gamma_2 - 1)W_{\gamma_2}$. Furthermore, since $Z_{\gamma_2^h} = (1 + \gamma_2 + \cdots + \gamma_2^{h-1})v_2$, we have that $Z_{\gamma_2^h}$ also lies in

M and $Z_{\gamma_2^h} = (\gamma_2^h - 1)W_{\gamma_2}$. Now we fix $h \in \{0, 1, \dots, p^{n-1} - 1\}$ and define

$$
V = \left\{ \begin{pmatrix} v^{(1)} \\ \vdots \\ v^{(p-1)} \end{pmatrix} \in (\mathbb{Z}/p^n\mathbb{Z})^{p-1} \;\middle|\; \sum_{j=1}^{p-1} v^{(j)} \equiv 0 \mod p \right\} \subseteq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}.
$$

We claim that the image of $\gamma_1\gamma_2^h - 1$ is equal to V. Since $\gamma_2^h = (p+1)^h \mathrm{Id} \equiv (1 + pl)\mathrm{Id} \mod p^n$ for some $l \in \mathbb{Z}/p^n\mathbb{Z}$, we can rewrite

$$
\gamma_1\gamma_2^h - 1 = (1 + pl)\gamma_1 - 1 = \begin{pmatrix} -1 & & & & -1-pl \\ 1+pl & -1 & & & -1-pl \\ & \ddots & \ddots & & \vdots \\ & & \ddots & -1 & -1-pl \\ & & & 1+pl & -2-pl \end{pmatrix},
$$

and thus, $\mathrm{Im}(\gamma_1\gamma_2^h - 1) \subseteq V$.

With easy calculations, one can check that the determinant of $\gamma_1\gamma_2^h - 1$ is equal to p modulo p^2. Take a lifting of $\gamma_1\gamma_2^h - 1$ to an integer matrix; this integer matrix has still determinant equal to p modulo p^2. Since $\mathbb{Z}$ is a principal ideal domain, we can consider its Smith normal form $\mathrm{diag}(\alpha_1, \alpha_2, \dots, \alpha_{p-1})$, and we get that $p \mid \alpha_{p-1}$ while $p^2 \nmid \alpha_{p-1}$ and $p \nmid \alpha_j$ for every $j = 1, \dots, p - 2$. Its projection $\mathrm{diag}(\widetilde{\alpha}_1, \widetilde{\alpha}_2, \dots, \widetilde{\alpha}_{p-1})$ modulo p^n is such that $\widetilde{\alpha}_j$ is invertible, for $j = 1, \dots, p-2$, and $\widetilde{\alpha}_{p-1} \neq 0$ is equal to 0 modulo p. Therefore, up to basis changes in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, the map $\gamma_1\gamma_2^h - 1$ is

$$
\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p \end{pmatrix}.
$$

It follows that $\mathrm{Im}(\gamma_1\gamma_2^h - 1)$ has index equal to p in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$. The submodule V has also index equal to p in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, and so, from the inclusions $\mathrm{Im}(\gamma_1\gamma_2^h - 1) \subseteq V \subseteq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, we get the equality $V = \mathrm{Im}(\gamma_1\gamma_2^h - 1)$. To conclude that Z satisfies the local conditions, it only remains to verify that $Z_{\gamma_1\gamma_2^h}$ lies in V. We have $Z_{\gamma_1\gamma_2^h} = v_1 + \gamma_1 Z_{\gamma_2^h}$, with $v_1 \in V$ and, as mentioned above, $Z_{\gamma_2^h} \in M$ (and also $\gamma_1 Z_{\gamma_2^h} \in M$). Since M is contained in V, we get that $Z_{\gamma_1\gamma_2^h} \in V$. $\qquad\square$

We conclude this section with the proof of Theorem 1.2.

Proof of Theorem 1.2. Let p be an odd prime.

(a) Let T be an algebraic torus of dimension $r < p - 1$ defined over a number field k and let $n \geqslant 1$ be an integer. With the notation of Section 2, since the inclusion $K \subseteq L(\zeta)$ holds, it is clear that G is isomorphic to the quotient $\mathrm{Gal}(L(\zeta)/k)/\mathrm{Gal}(L(\zeta)/K)$. Since p is an odd prime, any p-Sylow subgroup of the group $\Delta \simeq \mathrm{Gal}(L/k)$ is contained in $\mathrm{SL}_r(\mathbb{Q})$; hence by the condition $r < p - 1$ and Lemma 2.6, we have that Δ has no nontrivial p-Sylow subgroups. Since

$$
\mathrm{Gal}(L(\zeta)/k) \hookrightarrow \mathrm{Gal}(L/k) \times \mathrm{Gal}(k(\zeta)/k),
$$

we get that any p-Sylow subgroup of $\mathrm{Gal}(L(\zeta)/k)$ is isomorphic to a subgroup of $\mathrm{Gal}(k(\zeta)/k)$. The latter is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, and hence, it is cyclic. Thus, $\mathrm{Gal}(L(\zeta)/k)$ contains only one cyclic p-Sylow subgroup. Now let G_p be a p-Sylow subgroup of G. By Theorem 2.4, it is the image through the projection to the quotient of the p-Sylow subgroup of $\mathrm{Gal}(L(\zeta)/k)$, and hence, it is cyclic too and $\mathrm{H}^1_{\mathrm{loc}}(G_p, T[p^n])$ is trivial.

(b) Let $n \geqslant 2$ be an integer. As mentioned in the Introduction, it is enough to prove the statement for $r = p - 1$. By Lemma 3.1 and Proposition 3.3, there exists an algebraic torus defined over $k = \mathbb{Q}(\zeta_p)$ of dimension $p - 1$ such that $\mathrm{Gal}(k(T[p^n]/k)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ and $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \neq 0$. By Theorem 2.3, there exists a number field L such that $L \cap k(T[p^n]) = k$ and the local–global divisibility by p^n does not hold for $T(L)$. $\qquad\square$

Remark 3.4. The example built in Lemma 3.1 is defined over the number field $k = \mathbb{Q}(\zeta_p)$, but we can use it to construct an example over $\mathbb{Q}$ of dimension $(p-1)^2$. Indeed, let $\widetilde{T} = R_{k/\mathbb{Q}}(T)$ be the Weil restriction of T. It has dimension $\dim(\widetilde{T}) = [k : \mathbb{Q}] \dim(T) = (p-1)^2$ and for every number field F containing k, we have $\widetilde{T}(F) = R_{k/\mathbb{Q}}(T)(F) \simeq T(F)^{p-1}$. In particular, if $P \in T(F)$ is a point such that the local–global divisibility fails, we have the failure of the local–global divisibility also for the corresponding point on $\widetilde{T}(F)$ (given by $p - 1$ copies of P).

Remark 3.5. Let T be a torus defined over a number field k, with nontrivial $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k(T[p^n])/k), T[p^n])$. If L is a finite extension of k linearly disjoint from $k(T[p^n])$ over k, then

$$\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(L(T[p^n])/L), T[p^n]) \simeq \mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k(T[p^n])/k), T[p^n])$$

is nontrivial too. Thus, by Theorem 2.3, we have a counterexample over a finite extension of L. In this way, we have counterexamples over infinitely many number fields; in particular, this applies to $k = \mathbb{Q}$. Moreover, this argument works not only for tori, but for every commutative algebraic group.

4 | PROOF OF THEOREM 1.3

We are going to prove Theorem 1.3. In the following proof, we will show that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) = 0$; in particular, this proves that the local–global divisibility by p^n holds.

Proof of Theorem 1.3. We proceed by induction on $n \geqslant 1$ proving that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) = 0$. The base of the induction $n = 1$ is proven in [14]. Thus, suppose $n \geqslant 2$ and $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^m]) = 0$, for every $m \leqslant n - 1$. With the notation of Section 2, let $F = K \cap k(\zeta)$. We have that $[F : k] = [G : G']$, thus it is coprime with p by the assumptions of the theorem. Therefore, the p-Sylow subgroups of G are contained in G', hence in $\widetilde{\Delta}$. For any $j = 1, \ldots, n - 1$, using the same construction as in Section 2, we can define a group $G^{(j)} \subseteq \mathrm{GL}_r(\mathbb{Z}/p^j\mathbb{Z})$ that is isomorphic to $\mathrm{Gal}(k(T[p^j])/k)$. Let $\pi_j : \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p^j\mathbb{Z})$ be the reduction modulo p^j and let $H^{(j)}$ be the intersection of G with $\ker \pi_j$. It is easy to prove that $G^{(j)} = \pi_j(G) \simeq \mathrm{Gal}(k(T[p^j])/k)$ and $H^{(j)} \simeq \mathrm{Gal}(K/k(T[p^j]))$. We claim that $H^{(1)}$ is trivial. Every $h \in H^{(1)}$ can be written as $h = 1 + pA$, for some $A \in \mathrm{Mat}_r(\mathbb{Z}/p^n\mathbb{Z})$, so we have $h^{p^{n-1}} \equiv \mathrm{Id} \mod p^n$. Hence, the subgroup $H^{(1)}$ is a p-group, and thus, it is contained in a p-Sylow subgroup G_p of G. Since every p-Sylow subgroup of G is contained in G', we have that $H^{(1)}$ is contained in a p-Sylow subgroup G'_p of G' too. Thus, $H^{(1)} \subseteq \widetilde{\Delta}_p$,

where $\widetilde{\Delta}_p$ is a p-Sylow subgroup of $\widetilde{\Delta}$. Let $H \subset \mathrm{GL}_r(\mathbb{Z})$ be a subgroup of Δ such that its image via the reduction modulo p^n is $H^{(1)}$. Consider $\pi : \mathrm{GL}_r(\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ the reduction modulo p. We have that H is contained in $\ker(\pi) \cap \Delta$. So, by using Lemma 2.5, we find that H and, consequently, $H^{(1)}$ are trivial. Our claim is proved, and we get that also every $H^{(j)}$ is trivial since they are all contained in $H^{(1)}$. Therefore, $G \simeq G^{(n-1)} \simeq \cdots \simeq G^{(1)}$ via the relative projections.

Consider the following short exact sequence:

$$1 \longrightarrow T[p] \overset{\iota}{\longrightarrow} T[p^n] \overset{\varepsilon}{\longrightarrow} T[p^{n-1}] \longrightarrow 1,$$

where ι is the inclusion and ε is the p-power map (here we are using the multiplicative notation for $T[p]$, $T[p^{n-1}]$, and $T[p^n]$). The group G acts on $T[p^n]$ and, via the projections, on $T[p]$ and $T[p^{n-1}]$, and by these actions, the above short exact sequence is a sequence of G-modules. Thus, we have the following long exact sequence:

$$1 \to T[p]^G \to T[p^n]^G \to T[p^{n-1}]^G \to \mathrm{H}^1(G, T[p]) \to \mathrm{H}^1(G, T[p^n]) \to \mathrm{H}^1(G, T[p^{n-1}]) \to \ldots$$

Let C be a cyclic subgroup of G and for $i = 1, n-1, n$ let res_i be the restriction $\mathrm{H}^1(G, T[p^i]) \longrightarrow \mathrm{H}^1(C, T[p^i])$. We have the following diagram with exact rows:

$$
\begin{array}{ccccc}
\ker(\mathrm{res}_1) & \longrightarrow & \ker(\mathrm{res}_n) & \longrightarrow & \ker(\mathrm{res}_{n-1}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(G, T[p]) & \longrightarrow & \mathrm{H}^1(G, T[p^n]) & \longrightarrow & \mathrm{H}^1(G, T[p^{n-1}]) \\
\downarrow {\scriptstyle \mathrm{res}_1} & & \downarrow {\scriptstyle \mathrm{res}_n} & & \downarrow {\scriptstyle \mathrm{res}_{n-1}} \\
\mathrm{H}^1(C, T[p]) & \longrightarrow & \mathrm{H}^1(C, T[p^n]) & \longrightarrow & \mathrm{H}^1(C, T[p^{n-1}])
\end{array}
$$

where the central row is given by the long exact sequence above, the lower row is obtained from the same exact sequence by restriction to the subgroup C, whereas the upper one is induced by the commutativity of the diagram given by the last two rows. Since the group G is isomorphic to $G^{(1)}$ and to $G^{(n-1)}$, we have that the cyclic subgroups of $G^{(1)}$ and $G^{(n-1)}$ are the images of the projections of the cyclic subgroups of G. Therefore, by taking the intersection over all the cyclic subgroups of G, from the first row of the diagram, we have the exact sequence

$$\mathrm{H}^1_{\mathrm{loc}}(G, T[p]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^{n-1}]).$$

Since by inductive hypothesis $\mathrm{H}^1_{\mathrm{loc}}(G, T[p]) = \mathrm{H}^1_{\mathrm{loc}}(G, T[p^{n-1}]) = 0$, we also have $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) = 0$. □

Remark 4.1. We remark that in Lemma 3.1, we have $k = \mathbb{Q}(\zeta_p)$ and $F := k(T[p^n]) \cap k(\zeta_{p^n}) = k(\zeta_{p^n})$, so $[F : k] = [k(\zeta_{p^n}) : k] = [\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}(\zeta_p)] = p^{n-1}$. Moreover, we notice that the automorphism η in the proof of Lemma 3.1 is a generator of the subgroup $H^{(1)} \simeq \mathrm{Gal}(k(T[p^n])/k(T[p]))$, defined in the proof of Theorem 1.3 above. In particular, for the torus defined in Lemma 3.1, we have that $H^{(1)}$ is not trivial.

Remark 4.2. Notice that it is always possible to construct an algebraic torus T, not split over k, that satisfies the conditions of Theorem 1.3. An example is obtained by taking a number field k that contains a p^nth root of unity, any finite extension L/k of degree d, with $p - 1 \leqslant d < 3(p - 1)$, and considering $T = R_{L/k}\mathbb{G}_{m,L}$, the Weil restriction of the split torus $\mathbb{G}_{m,L}$ over L. The torus T is defined over k, it is split over L and it has dimension d. Thus, $F = K \cap k(\zeta)$ is equal to k and the hypotheses of the theorem are satisfied.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Jessica Alessandrì https://orcid.org/0000-0002-1543-7307
Rocco Chirivì https://orcid.org/0000-0002-6268-2858
Laura Paladino https://orcid.org/0000-0003-4758-9775

REFERENCES

1. E. Artin and J. T. Tate, *Class field theory*, Benjamin, Reading, MA, 1967.
2. J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.
3. M. Çiperiani and J. Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: on a question of Cassels*, J. Reine Angew. Math. **700** (2015), 175–207.
4. B. Creutz, *Locally trivial torsors that are not Weil–Châtelet divisible*, Bull. London Math. Soc. **45** (2013), 935–941.
5. B. Creutz, *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett. **23** (2016), no. 2, 377–387.
6. B. Creutz and S. Lu, *The local-global principle for divisibility in CM elliptic curves*, J. Number Theory **250** (2023), 139–154.
7. R. Dvornicich and L. Paladino, *On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility*, Int. J. Number Theory **18** (2022), no. 7, 1567–1590.
8. R. Dvornicich and L. Paladino, *Local-global questions for divisibility in commutative algebraic groups*, Eur. J. Math. **8** (2022), 599–628.
9. R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), 317–338.
10. R. Dvornicich and U. Zannier, *On a local-global principle for the divisibility of a rational point by a positive integer*, Bull. London Math. Soc. **39** (2007), 27–34.

11. F. Gillibert and G. Ranieri, *On the local-global divisibility of torsion points on elliptic curves and GL₂-type varieties*, J. Number Theory **174** (2017), 202–220.

12. F. Gillibert and G. Ranieri, *On the local-global divisibility over abelian varieties*, Ann. Inst. Fourier **68** (2018), no. 2, 847–873.

13. F. Gillibert and G. Ranieri, *On local-global divisibility over GL₂-type varieties*, Acta Arith. **193** (2020), no. 4, 339–354.

14. M. Illengo, *Cohomology of integer matrices and local-global divisibility on the torus*, J. Théor. des Nombres de Bordeaux **20** (2008), 327–334.

15. H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. reine angew. Math. **101** (1887), no. 3, 196–202.

16. L. Paladino, *On counterexamples to local-global divisibility in commutative algebraic groups*, Acta Arith. **148** (2011), no. 1, 21–29.

17. L. Paladino, *Divisibility questions in commutative algebraic groups*, J. Number Theory **205** (2019), 210–245.

18. G. Ranieri, *Counterexamples to the local–global divisibility over elliptic curves*, Ann. Mat. Pura Appl. **197** (2018), 1215–1225.

19. W. R. Scott, *Group theory*, Dover, New York, 1987.

20. J.-P. Serre, *Rigidité du foncteur de Jacobi d'échelon $n \geqslant 3$*, Séminaire Henri Cartan, Exposé 17 (Appendice), 1960–61.

21. E. Trost, *Zur theorie des Potenzreste*, Nieuw Arch. Wiskd. **18** (1934), 58–61.