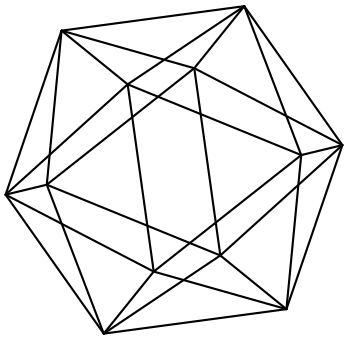
Max-Planck-Institut für Mathematik Bonn

Divisibility questions in commutative algebraic groups

by

Laura Paladino



Max-Planck-Institut für Mathematik
Preprint Series 2018 (44)

Divisibility questions in commutative algebraic groups

Laura Paladino

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

University of Calabria
Ponte Bucci, Cubo 30B
87036 Arcavacata di Rende
Italy

MPIM 18-44

Divisibility questions in commutative algebraic groups

Laura Paladino*

Abstract

Let k be a number field, let $\mathcal{A}$ be a commutative algebraic group defined over k and let p be a prime number. Let $\mathcal{A}[p]$ denote the p-torsion subgroup of $\mathcal{A}$. We give some sufficient conditions for the local-global divisibility by p in $\mathcal{A}$ and the triviality of the Tate-Shafarevich group $Ш(k, \mathcal{A}[p])$. When $\mathcal{A}$ is an abelian variety principally polarized, those conditions imply that the elements of the Tate-Shafarevich group $Ш(k, \mathcal{A})$ are divisible by p in the Weil-Châtelet group $H^1(k, \mathcal{A})$ and the local-global principle for divisibility by p holds in $H^r(k, \mathcal{A})$, for all $r \geq 0$.

1 Introduction

We consider two local-global problems, strongly related, that recently arose as generalizations of some classical questions. Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. Let $\bar{k}$ be the algebraic closure of k and let M_k be the set of places v of k. For every positive integer q, we denote by $\mathcal{A}[q]$ the q-torsion subgroup of $\mathcal{A}$ and by $k(\mathcal{A}[q])$ the number field obtained by adding to k the coordinates of the q-torsion points of $\mathcal{A}$. It is well-known that $\mathcal{A}[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, for some positive integer n depending only on $\mathcal{A}$. The Galois group $\mathrm{Gal}(k(\mathcal{A}[q])/k)$ is then isomorphic to the image of the representation of the absolute Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ in the general linear group $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$. The behaviour of $G := \mathrm{Gal}(k(\mathcal{A}[q])/k)$ is related to the answer to the following question, known as *Local-Global Divisibility Problem* in commutative algebraic groups.

Problem 1. *Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. Let $P \in \mathcal{A}(k)$ and let q be a positive integer. Assume that for all but finitely many valuations $v \in k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

*Partially supported by Istituto Nazionale di Alta Matematica F. Saveri with grant "Assegno di ricerca Ing. Giorgio Schirillo"; partially supported by Max Planck Institute for Mathematics in Bonn

This problem was stated in 2001 by Dvornicich and Zannier and its formulation was motivated by a particular case of the famous Hasse Principle on quadratic forms and by the Grunwald-Wang Theorem (see [15], [16] and [14]).

It is well-known that the vanishing of $H^1(G, \mathcal{A}[q])$ is a sufficient condition for the local-global dividibility by q (see [15]). Anyway, this condition is not necessary and the obstruction to the local-global principle for divisibility by q in $\mathcal{A}$ is given by a subgroup of $H^1(G, \mathcal{A}[q])$, denoted by $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ (see Section 2 for further details), that contains the Tate-Shafarevic group $Ш(k, \mathcal{A}[q])$ (up to isomorphism).

Clearly a solution to Problem 1 for all powers p^l of prime numbers p is sufficient to get an answer for all integers q, by the unique factorization in $\mathbb{Z}$ and Bézout's identity.

In the case of elliptic curves the problem has been widely studied since 2001. The answer is affirmative when q is a prime p (see [15] and [49]), for every k. For all powers 2^n, with $n \geq 2$ there are explicit counterexamples over $\mathbb{Q}$ (see [12], [16], [35]) and for 3^n, with $n \geq 2$ there are explicit counterexamples both over $\mathbb{Q}$ (see [12]) and over $\mathbb{Q}(\zeta_3)$ (see [35], [37]). For all powers of a prime $p \geq 5$ the answer is affirmative over $\mathbb{Q}$ (see [40]). Moreover if k does not contain the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where ζ_p is a p-th root of the unity, the local-global divisibility holds for all powers of every prime $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ (see [39]).

An aswer to the local-global divisibility by an odd prime number p in the algebraic tori, has been given in [21]. The answer is positive in every torus of dimension $n < 3(p-1)$ and negative when $n \geq 3(p-1)$.

These last result in particular shows that if $n \geq 3$, then even the local-global divisibility by p may fail. In addition for every $n \geq 6$ and $p \geq 3$, when $\mathcal{A}$ is an abelian variety, Katz in [27] produces counterexamples to the local-global disivibility by p when the question is restricted to torsion points of $\mathcal{A}$ (see also [18]). So we are sure that *the local-global divisibility by p does not hold in general.* This is also underlined by Dvornicich and Zannier in [15, §3], for $n \geq 3$. They construct some examples of subgroups of $\mathrm{GL}_n(q)$, with $n \in \{3, 4\}$, and show that the local-global divisibility by p fails in $\mathcal{A}$ over k if $\mathrm{Gal}(k(\mathcal{A}[p])/k)$ has a representation in $\mathrm{GL}_n(q)$, whose image is one of their examples (see also Subsection 3.2 for further details). Anyway, they have no evidence that their examples really realize representations of some Galois group $\mathrm{Gal}(k(\mathcal{A}[p])/k)$ and then the situation is not clear yet (see also [41]).

For abelian varieties, some sufficient conditions to have the local-global divisibility by

p^n, for every $n \geq 1$ appear in [19] and in [20]. Anyway, for a general abelian variety $\mathcal{A}$, one of the conditions is $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$. So the question about the divisibility by p remain in fact open, since, as stated above, the vanishing of $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$ widely assures the local-global divisibility by p. Let ζ_p be a p-th root of the unity. Only in the case of abelian varieties principally polarized and defined over number fields k linearly disjoint from $\mathbb{Q}(\zeta_p)$, the condition $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$ is replaced by some conditions concerning all the fields $k(P)$ generated by the coordinates of a point P, as P varies in $\mathcal{A}[p]$ (see [19, Theorem 3]).

In the end there are no criteria to establish the validity of the local-global divisibility by p in a general abelian variety, as well as in a general commutative algebraic group A.

Here we prove that, excluding some particular cases when p is small with respect to n, the strongest obstruction to the validity of the Hasse principle for divisibility by p is essentially the reducibility of $\mathcal{A}[p]$ as $\mathrm{Gal}(\bar{k}/k)$-module. In particular if $\mathcal{A}[p]$ is irreducible as a N-module, for every subnormal subgroup N of $\mathrm{Gal}(k(\mathcal{A}[p])/k)$, not contained in its center, then we get an affirmative answer for the divisibility by all $p > n$, for every n. We will call such a module a very strongly irreducible one, in accordance with the well-know definition of strongly irreducible module, that we are going to recall (see [4, Definition 1.1])

Definition 1.1. Let n, q be positive integers. A subgroup Γ of $\mathrm{GL}_n(q)$ is *strongly irreducible* if every normal subgroup $N \leq \Gamma$, not contained in the center $Z(\Gamma)$, is irreducible. We say that an irreducible Γ-module M is *strongly irreducible* if M is an irreducible N-module, for every normal subgroup $N \leq \Gamma$, not contained in the center $Z(\Gamma)$.

Here we state the definition of very strongly irreducibility, that concerns subnormal subgroups of Γ and not only normal subgroups of Γ.

Definition 1.2. Let n, q be positive integers. A subgroup Γ of $\mathrm{GL}_n(q)$ is *very strongly irreducible* if every subnormal subgroup N of Γ, not contained in the center $Z(\Gamma)$, is irreducible.
We say that an irreducible Γ-module M is *very strongly irreducible* if M is an irreducible N-module, for every subnormal subgroup $N \leq \Gamma$, not contained in the center $Z(\Gamma)$.

We prove the following statement.

Theorem 1.3. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, with $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Assume that $\mathcal{A}[p]$ is a very strongly irreducible G_k-module or a direct sum of very strongly irreducible G_k-modules and that we are in one of the following cases*

1) *$2 \leq n \leq 250$ and $p \geq \frac{n}{2} + 1$;*

2) *$n \geq 251$ and $p \geq n + 1$;*

then the local-global divisibility by p holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p]) = 0$.

There are evidences that the bounds for p appearing in **1)** and **2)** of Theorem 1.3 could be sharp in many cases (but not always, as we will see in Subsection 3.3, part *iii.*). At the end of the paper we will show a bound which is likely sharp in all cases (see Remark 3.11 and Theorem 3.12). We have not presented this bound in the statement of Theorem 1.3, with the aim of giving a simpler and more elegant bound for each n.

By the proof of Theorem 1.3, we will also deduce the following results.

Corollary 1.4. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, where $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Let $p \geq \frac{n}{2} + 1$. If the absolute Galois group G_k acts on $\mathcal{A}[p]$ as a subgroup of an extraspecial group, then $H^1(G, \mathcal{A}[p]) = 0$.*

Corollary 1.5. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, where $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Let $p > 2n + 2$. If the absolute Galois group G_k acts on $\mathcal{A}[p]$ as a subgroup of a group of Lie type in cross characteristic, then $H^1(G, \mathcal{A}[p]) = 0$.*

The triviality of $H^1(G, \mathcal{A}[p])$ is assured by a deep theorem proved by Nori (see [34, Theorem E]) in many cases, i. e. whenever G_k acts semisimply on $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$ and p is greater than a constant $c(n)$, depending only on n. Anyway the constant is not explicit. In our statement, in the cases when G_k acts on $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$ as a subgroup of $\mathrm{GL}_n(p)$ isomorphic to a subgroup of an almost simple group or an extraspecial group, we can respectively give explicit bounds $p > 2n + n$ and $p \geq n/2 + 1$ to get the triviality of that first cohomology group.

In the case when $\mathcal{A}$ is an abelian variety, with dual $\mathcal{A}^\vee$, the triviality of $Ш^1(k, \mathcal{A}[p]^\vee)$ implies $Ш(k, \mathcal{A}) \subseteq pH^r(k, \mathcal{A})$, for every positive integer r (see [13, Theorem 2.1]). When

$\mathcal{A}$ and $\mathcal{A}^\vee$ are isomorphic (for instance if $\mathcal{A}$ is principally polarized), then the vanishing of $Ш^1(k, \mathcal{A}[p])$ itself implies $Ш(k, \mathcal{A}) \subseteq pH^r(k, \mathcal{A})$, for all $r \geq 1$. Such an inclusion is a sufficient and necessary condition to have an affirmative answer to the following second and more general local-global problem.

Problem 2. *Let A be a commutative algebraic group defined over a number field k. Let q be a positive integer and let $\sigma \in H^r(k, \mathcal{A})$. Assume that for all $v \in M_k$ there exists $\tau_v \in H^r(k_v, \mathcal{A})$ such that $q\tau_v = \sigma$. Can we conclude that there exists $\tau \in H^r(k, \mathcal{A})$, such that $q\tau = \sigma$?*

Problem 2 was firstly considered by Cassels for $r = 1$ in the case when $\mathcal{A}$ is an elliptic curve $\mathcal{E}$ (see [5, Problem 1.3]). In particular Cassels questioned if the elements of the Tate-Shafarevich group $Ш(k, \mathcal{E})$ were divisible by p^l in the Weil-Châtelet group $H^1(k, \mathcal{E})$, for all l. Tate produced soon an affirmative answer for divisibility by p (see [6]).

Proposition 1.6 (Tate, 1962)**.** *Problem 2 has an affirmative answer when $r = 1$, $\mathcal{E}$ is an elliptic curve and $q = p$ is a prime number.*

The question for powers p^l, with $l \geq 2$ remained open for decades. The mentioned affirmative results to Problem 1 in elliptic curves imply an affirmative answer to Problem 2, since the proofs show the triviality of the corresponding Tate-Shafarevich group. So Cassels' question has an affirmative answer for all $p \geq 5$ in elliptic curves over $\mathbb{Q}$ and for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ in elliptic curves over k. On the contrary, for powers of $p \in \{2, 3\}$ the answer is negative by [12].

The problem was afterwards considered for abelian varieties by Bašmakov (see [2]) and lately by Çiperiani and Stix, who gave some sufficient conditions for a positive answer (see [9]). One of their conditions is again the vanishing of $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$, so in particular the question for divisibility by p is still open. In [12] Creutz also proved that for every prime p, there exists an abelian variety A defined over $\mathbb{Q}(\zeta_p)$ such that $Ш(k, A) \not\subseteq pH^1(k, A)$. Thus in abelian varieties of dimension strictly greater than 1, even the local-global divisibility by p may fail for Problem 2, as well as for Problem 1. As a consequence of Theorem 1.3, we have the following statement.

Corollary 1.7. *Let p be a prime number. Let $\mathcal{A}$ be an abelian variety principally polarized of dimension g. Assume that $\mathcal{A}[p]$ is a very strongly irreducible G_k-module or a direct sum of very strongly irreducible G_k-modules and we are in one of the following cases*

1) $1 \leq g \leq 125$, $p \geq \frac{n}{2} + 1$;

2) $g \geq 126$, $p \geq n + 1$;

then the local-global divisibility by p holds in $H^r(k, \mathcal{A})$, for all $r \geq 0$.

Corollary 1.7 can be considered a generalization of Tate's Proposition 1.6 to all commutative algebraic groups.

About the structure of this paper, a few preliminary known results in the theory of groups and in local-global divisibility are stated in next section. Then we proceed with the proof of Theorem 1.3. We firstly show the validity of the local-global divisibility by p and the triviality of $Ш(k, \mathcal{A}[p])$ in some particular cases, i. e., when it is a group extension with a cyclic group as a quotient (see Lemma 3.2) and when the image of the representation of G_k in $\mathrm{GL}_n(p)$ is the whole special linear group (see Lemma 3.5). Then we show that Theorem 1.3 holds for $n \in \{2, 3\}$. In the end we give a proof of Theorem 1.3 for a general n and we deduce Corollary 1.4 and Corollary 1.5.

2 Preliminary results

We recall some known results about local-global divisibility and about group theory, that will be useful in the following.

We keep the notation introduced in Section 1. Thus k denotes a number field and $\mathcal{A}$ denotes a commutative algebraic group, defined over k. From now on let $q := p^l$, where p is a prime number and l is a positive integer. As introduced before, the q-torsion subgroup of $\mathcal{A}$ will be denoted by $\mathcal{A}[q]$ and the number field generated over k by the coordinates of the points in $\mathcal{A}[q]$ will be denoted by $F := k(\mathcal{A}[q])$. The q-torsion subgroup $\mathcal{A}[q]$ of $\mathcal{A}$ is a G_k-module, where G_k denotes the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. We have $\mathcal{A}[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, for a certain n depending only on $\mathcal{A}$. Thus G_k acts over $\mathcal{A}[q]$ as a subgroup of $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$ isomorphic to $G = \mathrm{Gal}(k(\mathcal{A}[q])/k)$. We still denote by G the representation of G_k in $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$. If $q = p$ is a prime number, in particular $G \leq \mathrm{GL}_n(p)$. When $\mathcal{A}$ is an abelian variety of dimension g, we have $n = 2g$.

Let Σ be the subset of M_k containing all the places v of K, that are unramified in F. For every $v \in \Sigma$, we denote by G_v the Galois group $\mathrm{Gal}(F_w/k_v)$, where w is a place of F extending v. In [15] Dvornicich and Zannier proved that the answer to the local-global

question for divisibility by q of points in $\mathcal{A}(k)$ is linked to the behaviour of the following subgroup of $H^1(G, \mathcal{A}[q])$

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) := \bigcap_{v \in \Sigma} \ker(H^1(G, \mathcal{A}[q]) \xrightarrow{res_v} H^1(G_v, \mathcal{A}[q])), \tag{2.1}$$

where res_v, as usual, denotes the restriction map. By substituting M_k to Σ in (2.1), i. e. by letting v vary over all the valuations of k, we get the classical definition of the Tate-Shafarevich group $Ш^1(k, \mathcal{A}[q])$ (up to isomorphism)

$$Ш^1(k, \mathcal{A}[q]) := \bigcap_{v \in M_k} \ker(H^1(k, \mathcal{A}[q]) \xrightarrow{res_v} H^1(k_v, \mathcal{A}[q])).$$

In particular, the vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ assures the triviality of $Ш^1(k, \mathcal{A}[q])$, that is a sufficient condition to get an affirmative answer to Problem 2, for $r = 0$, and in many cases for all $r \geq 0$ (see [13, Theorem 2.1] and Section 2). Furthermore the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ is a sufficient condition for an affirmative answer to Problem 1 by [15, Proposition 2.1].
Owing to Čebotarev's Density Theorem, the group G_v varies over all cyclic subgroups of G as v varies in Σ, then in [15] Dvornicich and Zannier gave the following equivalent definition of $H^1_{\mathrm{loc}}(G, A[q])$.

Definition 2.1. A cocycle $\{Z_\sigma\}_{\sigma \in G} \in H^1(G, \mathcal{A}[q])$ satisfies the *local conditions* if, for every $\sigma \in G$, there exists $A_\sigma \in \mathcal{A}[q]$ such that $Z_\sigma = (\sigma - 1)A_\sigma$. The subgroup of $H^1(G, \mathcal{A}[q])$ formed by all the cocycles satisfying the local conditions is called *first local cohomological group* of G with values in $\mathcal{A}[q]$ and it is denoted by $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$.

The description of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ given in Definition 2.1 is useful in proving its triviality and even in producing counterexamples to the local-global divisibility. We keep the notation $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ used in almost all previous papers about the topic, but it is worth to mention that in [42] Sansuc already treated similar modified Tate-Shafarevich groups as in (2.1) and introduced the notation $Ш^1_{M_k \setminus \Sigma}(k, \mathcal{A})$.

Remark 2.2. Observe that if G is cyclic, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) = 0$.

The vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ is strongly related to the behaviour of $H^1_{\mathrm{loc}}(G_p, \mathcal{A}[q])$, where G_p is the p-Sylow subgroup of G (see [15]).

Lemma 2.3 (Dvornicich, Zannier)**.** *Let G_p be a p-Sylow subgroup of A. An element of $H^1_{\mathrm{loc}}(\mathcal{A}, \mathcal{A}[q])$ is zero if and only if its restriction to $H^1_{\mathrm{loc}}(G_p, \mathcal{A}[q])$ is zero.*

In some cases, a quick way to show that both $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ and $H^1_{\mathrm{loc}}(G_p, \mathcal{A}[q])$ are trivial is the use of Sah's Theorem (see [30, Theorem 5.1]).

Lemma 2.4 (Sah's Theorem)**.** *Let G be a group and let M be a G-module. Let α be in the center of G. Then $H^1(G, M)$ is annihilated by the map $x \to \alpha x - x$ on M. In particular, if this map is an automorphism of M, then $H^1(G, M) = 0$.*

By Lemma 2.4, if G is a subgroup of $\mathrm{GL}_n(q)$ that contains a non-trivial scalar matrix, then $H^1(G, \mathbb{Z}/q\mathbb{Z}) = 0$. Thus, in particular, $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) = 0$ too.

Corollary 2.5. *Let $G \leq \mathrm{GL}_n(q)$, for some positive integers n and q. If $\lambda \cdot I_n \in G$, $\lambda \in \mathbb{F}_q^*$, is a nontrivial scalar matrix, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) = 0$.*

In our proofs of Theorem 1.3, a crucial tool is the use of Aschbacher's Theorem on the classification of maximal subgroups of $\mathrm{GL}_n(q)$ (see [1]). Aschbacher proved that the maximal subgroups of $\mathrm{GL}_n(q)$ could be divided into 9 specific classes $\mathcal{C}_i$, $1 \leq i \leq 9$. For a big n, it is a very hard open problem to find the maximal subgroups of $\mathrm{GL}_n(q)$ of type $\mathcal{C}_9$. We have an explicit list of such groups only for $n \leq 12$ (see [3]). On the contrary, the maximal subgroups of $\mathrm{GL}_n(q)$ of geometric type (i. e. of class $\mathcal{C}_i$, with $1 \leq i \leq 8$) have been described for every n (see [28]). We recall some notations in group theory and then we resume the description of the maximal subgroups of $\mathrm{GL}_n(q)$ of geometric type in the following Table 1 (see [28, Table 1.2.A, § 3.5 and § 4.6]).

Notation 1. Let n, l be positive integers, let p be a prime number and let $q = p^l$. We denote by $\mathbb{F}_q$ the finite field with q elements. Let ω_q be a primitive element of $\mathbb{F}_q^*$. We use the standard notations for the special linear group $\mathrm{SL}_n(q)$, the projective special linear group $\mathrm{PSL}_n(q)$, the unitary group $\mathrm{U}_n(q)$, the symplectic group $\mathrm{Sp}_n(q)$, the simmetric group S_n and the alternating group A_n. By C_n we denote a cyclic group of order n and by p^{1+2n} an extraspecial group of order p^{1+2n}. Furthermore, if n is odd or both n and q are even, then we denote by $\mathrm{O}_n(q)$ the orthogonal group and by $\mathrm{SO}_n(q)$ the special orthogonal group. If n is even and q is odd we denote by (see [3])

$\mathrm{GO}_n^+(q)$ the stabilizer of the non-degenerate symmetric bilinear antidiagonal form (1,...,1);

$\mathrm{SO}_n^+(q)$ the subgroup of $\mathrm{GO}_n^+(q)$ formed by the matrices with determinant 1;

$\mathrm{GO}_n^-(q)$ the stabilizer of non-degenerate symmetric bilinear form I_n, when $n \equiv 2(\mathrm{mod}\ 4)$ and $q \equiv 3(\mathrm{mod}\ 4)$ and the stabilizer of non-degenerate symmetric bilinear diagonal form $(\omega_q, 1, ..., 1)$, when $n \not\equiv 2(\mathrm{mod}\ 4)$ and $q \not\equiv 3(\mathrm{mod}\ 4)$;

$\mathrm{SO}_n^-(q)$ the subgroup of $\mathrm{GO}_n^-(q)$ formed by the matrices with determinant 1.

For n even and $\epsilon \in \{+, -\}$, we denote by $\Omega_n^\epsilon(q)$ the subgroup of index 2 of O_n^ϵ, obtained as the kernel of the spinor norm and by $P\Omega_n^\epsilon(q)$ the quotient $\Omega_n^\epsilon(q)/\{\pm\}$.

Notation 2. Let A, B be two groups. We denote by

$A \rtimes B$, the semidirect product of A with B (where $A \trianglelefteq A \rtimes B$);

$A \circ B$, the central product of A and B;

$A \wr B$, the wreath product of A and B;

$A.B$, a group Γ that is an extension of its normal subgroup A with the group B (then $B \simeq \Gamma/A$), in the case when we do not know if it is a split extension or not;

$A \cdot B$, a group Γ that is a non-split extension of its normal subgroup A with the group B (then $B \simeq \Gamma/A$);

$A : B$, a group Γ that is a split extension of its normal subgroup A with the group B (then $B \simeq \Gamma/A$ and $\Gamma \simeq A \rtimes B$).

type	description	structure
$\mathcal{C}_1$	stabilizers of totally singular or nonsingular subspaces	maximal parabolic group
$\mathcal{C}_2$	stabilizers of direct sum decompositions $V = \bigoplus_{i=1}^{r} V_i$, with each V_i of dimension t	$\mathrm{GL}_t(q) \wr S_r, n = rt$
$\mathcal{C}_3$	stabilizers of extension fields of $\mathbb{F}_q$ of prime index r	$\mathrm{GL}_t(q^r).C_r, n = rt, r$ prime
$\mathcal{C}_4$	stabilizers of tensor product decompositions $V = V_1 \otimes V_2$	$\mathrm{GL}_t(q) \circ \mathrm{GL}_r(q), n = rt$
$\mathcal{C}_5$	stabilizers of subfields of $\mathbb{F}_q$ of prime index r	$\mathrm{GL}_n(q_0)$, $q = q_0^r$, r prime
$\mathcal{C}_6$	normalizers of symplectic-type r-groups (r prime) in absolutely irreducible representations	$(C_{q-1} \circ r^{1+2t}).\mathrm{Sp}_{2t}(r)$, $n = r^t, r$ prime, $r \neq p$
$\mathcal{C}_7$	stabilizers of tensor product decompositions $V = \bigotimes_{i=1}^{t} V_i, \dim(V_i) = r$	$\underbrace{(\mathrm{GL}_r(q) \circ ... \circ \mathrm{GL}_r(q))}_{t}.S_t, n = r^t$
$\mathcal{C}_8$	classical subgroups	$\mathrm{Sp}_n(q)$, n even $\mathrm{O}_n^{\epsilon}(q)$, q odd $\mathrm{U}_n(q^{\frac{1}{2}})$, q a square

Table 1: Maximal subgroups of $\mathrm{GL}_n(q)$ of geometric types

Although we generally do not know explicitly the maximal subgroups of type $\mathcal{C}_9$, by Aschbacher's Theorem, we have such a characterization of them:

"if Γ is a maximal subgroup of $\mathrm{GL}_n(q)$ of class $\mathcal{C}_9$ and Z denotes its center, then for some nonabelian simple group T, the group $\Gamma/(\Gamma \cap Z)$ is almost simple with socle T; in this case the normal subgroup $(\Gamma Z).T$ acts absolutely irreducibly, preserves no nondegenerate classical form, is not a subfield group, and does not contain $\mathrm{SL}_n(q)$."

We will use this description in our proof of Theorem 1.3. Furthermore, for very small integers n there are a few subsequent and more explicit versions of Aschbacher's Theorem, that describe exactly the maximal subgroups of class $\mathcal{C}_9$. To prove Theorem 1.3 we will use the classification of the maximal subgroups of $\mathrm{SL}_n(q)$ appearing in [3], for $n \leq 12$.

From now on we will say that a subgroup G of $\mathrm{GL}_n(q)$ (respectively of $\mathrm{SL}_n(q)$) is of class $\mathcal{C}_i$ or of type $\mathcal{C}_i$, with $1 \leq i \leq 9$, if G is contained in a maximal subgroup of $\mathrm{GL}_n(q)$ (respectively of $\mathrm{SL}_n(q)$) of class $\mathcal{C}_i$.

3 Proof of Theorem 1.3

The proof of Theorem 1.3 follows by the proof of the next slightly more general statement, with the only difference in the hypotheses that we assume $G \leq \mathrm{GL}_n(p^m)$, for some

positive integer m (instead of simply $\mathrm{GL}_n(p)$). This more general assumption considering powers of p in lieu of p will be useful when G is of type $\mathcal{C}_3$ and it is isomorphic to a subgroup of $\mathrm{GL}_t(p^r).C_r$, with $n = tr$, for some prime number r.

Theorem 3.1. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Assume that $G = \mathrm{Gal}(k(\mathcal{A}[p])/k)$ is isomorphic to a subgroup of $\mathrm{GL}_n(p^m)$, for some positive integers n, m. If $\mathcal{A}[p]$ is a very strongly irreducible G-module or a direct sum of very strongly irreducible G-modules and we are in one of the following cases*

1) *$2 \leq n \leq 250$ and $p \geq \frac{n}{2} + 1$;*

2) *$n \geq 251$ and $p \geq n + 1$;*

then the local-global divisibility by p holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p]) = 0$.

When $n = 2$, $m = 1$ and $p \neq 2$, the conclusion of Theorem 3.1 follows immediately by Chevalley's Theorem on the classification of the commutative algebraic groups in characteristc 0 (see for example [43]), combined with the mentioned results in [15] and in [21]. Anyway, when $m > 1$, or $m = 1$, $p = 2$ and $\mathcal{A}$ an algebraic torus, there are no similar results in the literature, even for $n = 2$. Thus, we will give a proof for the more general case when $G \leq \mathrm{GL}_2(p^m)$, with $m \geq 1$, for $n = 2$ too. That will be a part of the base of the induction for the general case. In fact, for $n = 2$ we can prove a stronger result than Theorem 3.1, since it suffices to assume that $\mathcal{A}[p]$ is an irreducible G-module (or a direct sum of irreducible G-modules), as we will see in Subsection 3.1 (see Proposition 3.8).

We firstly prove a very useful lemma. In fact it covers many cases when G is isomorphic to a subgroup of $\mathrm{GL}_n(p^m)$ that is an extension of a group with trivial local cohomology by a cyclic group. Observe that here the hypothesis of irreducibility (and not very strongly irreducibility) is sufficient. Of course every statement proved for an irreducible G-module, holds for a very strongly irreducible G-module too (as well as for a strongly irreducible G-module).

Lemma 3.2. *Let p be a prime number and n, m positive integers. Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. Assume that $G = \mathrm{Gal}(k(\mathcal{A}[p])/k)$ acts*

irreducibly on $\mathcal{A}[p]$ as a subgroup of $\mathrm{GL}_n(p^m)$, which is an extension $S.Ct$, where t is a positive integer. If $H^1_{\mathrm{loc}}(S,\mathcal{A}[p])=0$, then $H^1_{\mathrm{loc}}(G,\mathcal{A}[p])=0$ too.

Proof. If S is trivial, then $G\simeq C_t$ is cyclic and $H^1_{\mathrm{loc}}(G,\mathcal{A}[p])=0$. Assume that S is a nontrivial normal subgroup of G. If S contains a nontrivial element of the center $Z(G)$, then by Sah's Theorem, we get $H^1_{\mathrm{loc}}(G,\mathcal{A}[p])=0$. So we may assume without loss of generality that $S\cap Z(G)$ is trivial. Let $C_t=\langle\mathfrak{f}\rangle$, where as usual $\langle\mathfrak{f}\rangle$ denotes the group generated by $\mathfrak{f}$. We have $G=S.\langle\mathfrak{f}\rangle$. We denote by $\mathfrak{f}$ both an element in the quotient C_t and a representative of it in G. Let $\{Z_g\}_{g\in G}$ represent a cocycle of $H^1_{\mathrm{loc}}(G,\mathcal{A}[p])$. Since $H^1_{\mathrm{loc}}(S,\mathcal{A}[p])=0$, then there exists $A\in\mathcal{A}[p]$ such that $Z_\sigma=(\sigma-1)A$, for all $\sigma\in S$. Furthermore, there exists $A_\mathfrak{f}\in\mathcal{A}[p]$ such that $Z_\mathfrak{f}=(\mathfrak{f}-1)A_\mathfrak{f}$. Being $\langle\mathfrak{f}\rangle$ cyclic, then $Z_\varphi=(\varphi-1)A_\mathfrak{f}$, for every $\varphi\in\langle\mathfrak{f}\rangle$. Since S is a normal subgroup of G, the automorphism $\mathfrak{f}$ acts on S by conjugation and $\mathfrak{f}\sigma\mathfrak{f}^{-1}=\tau$, with $\tau\in S$. In particular $\mathfrak{f}\sigma=\tau\mathfrak{f}$. Then

$$Z_{\mathfrak{f}\sigma\mathfrak{f}^{-1}}=Z_\mathfrak{f}+\mathfrak{f}Z_\sigma+\mathfrak{f}\sigma Z_{\mathfrak{f}^{-1}} \tag{3.1}$$

i. e.

$$(\tau-1)A=(\mathfrak{f}-1)A_\mathfrak{f}+\mathfrak{f}(\sigma-1)A+\mathfrak{f}\sigma(\mathfrak{f}^{-1}-1)A_\mathfrak{f}$$

$$\tau(A)-A=\mathfrak{f}(A_\mathfrak{f})-A_\mathfrak{f}+\tau\mathfrak{f}(A)-\mathfrak{f}(A)+\tau(A_\mathfrak{f})-\tau\mathfrak{f}(A_\mathfrak{f}).$$

We have

$$\tau(\mathfrak{f}-1)(A_\mathfrak{f}-A)=(\mathfrak{f}-1)(A_\mathfrak{f}-A).$$

By eventually changing σ with τ and $\mathfrak{f}$ with $\mathfrak{f}^{-1}$, one easily deduces that the p-torsion point $B:=(\mathfrak{f}-1)(A_\mathfrak{f}-A)$ is fixed by all $\sigma\in S$. In other words, if k^S denotes the subfield of $k(\mathcal{A}[p])$ fixed by S, then $B\in\mathcal{A}(k^S)$. If $B=0$, then $(\mathfrak{f}-1)A_\mathfrak{f}=(\mathfrak{f}-1)A$ and $H^1_{\mathrm{loc}}(G,\mathcal{A}[p])=0$. Suppose $B\neq 0$. Observe that for every element $\sigma\in S$ there exists $\sigma_i\in S$ such that $\sigma\mathfrak{f}^i=\mathfrak{f}^i\sigma_i$, for each positive integer i. Then all $\sigma\in S$ also fix $\mathfrak{f}^i(B)$, for every i:

$$\sigma(\mathfrak{f}^i(B))=\mathfrak{f}^i\sigma_i(B)=\mathfrak{f}^i(B).$$

By considering $\mathfrak{f}^i$ instead of f in (3.1), we get

$$\tau(\mathfrak{f}^i-1)(A_\mathfrak{f}-A)=(\mathfrak{f}^i-1)(A_\mathfrak{f}-A),$$

for all positive integers i. Assume that $t \geq n$. If $\mathfrak{f}^i(B) = \alpha B$, for some $1 \leq \alpha \leq p-1$ and $1 \leq i \leq t$, such that $\gcd(i,t) = 1$, we choose $\mathfrak{f}^i$ as a generator of $\langle \mathfrak{f} \rangle$. Consider a basis of $\mathcal{A}[p]$, where B is the first vector in the basis. Since every $\sigma \in S$ fixes B and $\mathfrak{f}^i(B) = \alpha B$, then the group G is reducible and we have a contraddiction with our assumptions. Then suppose that $\mathfrak{f}^i(B) \neq \alpha B$, for all $1 \leq i \leq p-1$. In particular B and $\mathfrak{f}(B)$ are linearly independent as vectors in $\mathcal{A}[p]$ and we can choose them as the first two elements of a basis of that vector space.

Suppose that $B, \mathfrak{f}(B)$ and $\mathfrak{f}^2(B)$ are not linearly independent, i. e. $\mathfrak{f}^2(B) = \alpha_0 B + \alpha_1 \mathfrak{f}(B)$, for some $\alpha_0, \alpha_1 \in \mathbb{F}_p$. Then the matrix that represents $\mathfrak{f}$ in $\mathrm{GL}_n(p^l)$ is of the form

$$\begin{pmatrix} 0 & \alpha_0 & * & ... & * \\ 1 & \alpha_1 & * & ... & * \\ 0 & 0 & * & ... & * \\ & & \vdots & & \\ 0 & 0 & * & ... & * \end{pmatrix}.$$

Since every $\sigma \in S$ fixes B and $\mathfrak{f}(B)$, then G is reducible, a contraddition. Thus we may assume that $B, \mathfrak{f}(B)$ and $\mathfrak{f}^2(B)$ are linearly independent. In a similar way, we get that $B, \mathfrak{f}(B), \mathfrak{f}^2(B), ..., \mathfrak{f}^{n-1}(B)$ are linearly independent (recall that we are assuming $t \geq n$). Therefore we can choose the basis $\{B, \mathfrak{f}(B), \mathfrak{f}^2(B), ..., \mathfrak{f}^{n-1}(B)\}$, for $\mathcal{A}[p]$. We have that every $\sigma \in S$ fixes all the p-torsion points of $\mathcal{A}[p]$, a contraddiction with S being nontrivial. Thus $B = 0$ and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Now suppose $t < n$. As above we may assume that $B, \mathfrak{f}(B), \mathfrak{f}^2(B), ..., \mathfrak{f}^{t-1}(B)$ are linearly independent. Moreover $\mathfrak{f}^t(B) = B$. We have that $\mathfrak{f}$ has the following form, with respect to such a basis $\{B, \mathfrak{f}(B), \mathfrak{f}^2(B), ..., \mathfrak{f}^{t-1}(B)\}$ (recall that $t < n$)

$$\mathfrak{g} = \left(\begin{array}{ccc|c|ccc} 0 & ... & 0 & 1 & * & ... & * \\ \hline & & & 0 & * & ... & * \\ & I_{t-1} & & \vdots & \vdots & & \vdots \\ & & & 0 & * & ... & * \\ \hline 0 & ... & 0 & 0 & * & ... & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & ... & 0 & 0 & * & ... & * \end{array}\right). \tag{3.2}$$

Since $\sigma \in S$ fixes every $\mathfrak{f}^i(B)$, then G acts reducibly on $\mathcal{A}[p]$ and we have a contraddiction. Therefore $B = 0$, implying $(\mathfrak{f}-1)A = (\mathfrak{f}-1)A_{\mathfrak{f}}$, i. e. $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. □

With the same arguments used in the proof of Lemma 3.2, we can also prove the following statements.

Corollary 3.3. *Let p be a prime number and let n, m be positive integers. Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. Assume that $G = \mathrm{Gal}(k(\mathcal{A}[p])/k)$ is isomorphic to a subgroup of $\mathrm{GL}_n(p^m)$ that is an extension $S.J$, where S acts irreducibly on $\mathcal{A}[p]$. If $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$.*

Proof. Let $\{Z_g\}_{g\in G}$ represent a cocycle of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$. Since $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, then there exists $A \in \mathcal{A}[p]$ such that $Z_\sigma = (\sigma - 1)A$, for all $\sigma \in S$. Choose an element $\mathfrak{f} \in J$. We still denote by $\mathfrak{f}$ one of its representatives in G. There exists $A_\mathfrak{f} \in \mathcal{A}[p]$, such that $Z_\mathfrak{f} = (\mathfrak{f} - 1)A_\mathfrak{f}$. Let $B := (\mathfrak{f} - 1)(A_\mathfrak{f} - A)$. By considering the subgroup of J generated by $\mathfrak{f}$ and repeating the argument used in Lemma 3.2, every $\sigma \in S$ fixes B. If $B \neq 0$, then we have a contraddiction with S acting irreducibly on $\mathcal{A}[p]$. Thus $B = 0$, i. e. $Z_\mathfrak{f} = (\mathfrak{f} - 1)(A_\mathfrak{f}) = (\mathfrak{f} - 1)A$, implying $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. □

Corollary 3.4. *Let p be a prime number and let n, m be positive integers. Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k. Assume that $G = \mathrm{Gal}(k(\mathcal{A}[p])/k)$ is isomorphic to a subgroup of $\mathrm{GL}_n(p^m)$ that is an extension $S.J$. If $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$ and $H^1_{\mathrm{loc}}(J, \mathcal{A}[p]) = 0$, and there exist $\rho \in S$ and $\omega \in J$ such that $\rho - 1$ and $\omega - 1$ are invertible, then $H^1_{\mathrm{loc}}(J, \mathcal{A}[p]) = 0$.*

Proof. Let $\{Z_g\}_{g\in G}$ represent a cocycle of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$. Since $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, then there exists $A \in \mathcal{A}[p]$ such that $Z_\sigma = (\sigma - 1)A$, for all $\sigma \in S$. Moreover, there exists $W \in \mathcal{A}[p]$ such that $Z_\tau = (\tau - 1)W$, for all $\tau \in J$. By the same argument used in the proof of Lemma 3.2, the point $B := (\omega - 1)(W - A) \in \mathcal{A}[p]$ is fixed by every $\sigma \in S$. In particular B lies in $\bigcap_{\sigma\in S} \ker(\sigma - 1)$. Since $\ker \rho = 0$, then $B = 0$, implying $(\omega - 1)(W - A) = 0$. The kernel of $\omega - 1$ is trivial too by hyphotesis and then $W = A$.

□

The next remark, will allow us to deal with subgroups of $\mathrm{SL}_n(p^m)$, instead of $\mathrm{GL}_n(p^m)$.

Remark 3.5. Let G be a subgroup of $\mathrm{GL}_n(p^m)$ and let $\widetilde{G} := G \cap \mathrm{SL}_n(p^m)$. Since $|\mathrm{GL}_n(p^m)| = (p^m - 1)|\mathrm{SL}_n(p^m)|$, then the p-Sylow subgroup of $\mathrm{GL}_n(p^m)$ coincides with the p-Sylow subgroup of $\mathrm{SL}_n(p^m)$. By Lemma 2.3, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^m]) = 0$ if and only if $H^1_{\mathrm{loc}}(\widetilde{G}, \mathcal{A}[p^m]) = 0$. Moreover $\mathrm{SL}_n(p^m)$ is a normal subgroup of $\mathrm{GL}_n(p^m)$ and then, if

$\mathcal{A}[p]$ is a very strongly irreducible G-module, then $\mathcal{A}[p]$ is a very strongly irreducible $\widetilde{G}$-module too. Therefore from now on we assume $G \leq \mathrm{SL}_n(p^m)$, without loss of generality.

Observe that when $\mathcal{A}[p]$ is an irreducible G-module, the vanishing of $H^1_{\mathrm{loc}}(\widetilde{G}, \mathcal{A}[p^m])$ implies the vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^m])$ by Lemma 3.2 too. In fact $\mathrm{GL}_n(p^m)$ is an extension of $\mathrm{SL}_n(p^m)$ by a cyclic group.

We are going to prove that if G is the whole special linear group $\mathrm{SL}_n(p^m)$ (for some m), then the local-global divisibility holds in $\mathcal{A}$.

Lemma 3.6. *If $G = \mathrm{SL}_n(p^m)$, for some positive integer m, then $H^1_{loc}(G, \mathcal{A}[p]) = 0$.*

Proof. Let $q = p^m$. If $n = 2$ (more generally if n is even), then G contains $-I$ and, by Lemma 2.5, we have the conclusion. Assume that $n = 3$. By lemma 2.3, it suffices to prove that $H^1_{\mathrm{loc}}(G_p, \mathcal{A}[p]) = 0$, for a p-Sylow subgroup G_p of G. Let G_p be the subgroup of $G = \mathrm{SL}_3(q)$ consisting of all the upper triangular matrices of the form

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

We denote by G_1 the subset of G_p formed by the matrices

$$\begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with $\alpha \in \mathbb{F}_p$. By G_2 we denote the subset of G_p formed by the matrices

$$\begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix},$$

with $\beta, \gamma \in \mathbb{F}_p$. Observe that G_p is generated by the elements of G_1 and the elements of G_2. In fact

$$\begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \beta - \alpha\gamma \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}.$$

We are going to prove that both $H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p])$ and $H^1_{\mathrm{loc}}(G_2, \mathcal{A}[p])$ are trivial. Then we will be able to glueing the local cohomologies and showing $H^1_{\mathrm{loc}}(G_p, \mathcal{A}[p]) = 0$.

1. The triviality of $H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p])$.

The additive group of the finite field $\mathbb{F}_{p^m}$, with p^m elements, is isomorphic to the vector space $V = (\mathbb{F}_p)^m$. Let $\alpha_1, \alpha_2, ...\alpha_m$ be a basis of V. Observe that G_1 is generated by the matrices

$$\sigma_i = \begin{pmatrix} 1 & \alpha_i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $1 \leq i \leq m$. If $\sigma \in G_1$, then

$$\sigma = \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

with $\alpha = \lambda_{\sigma,1}\alpha_1 + \lambda_{\sigma,2}\alpha_2 + ... + \lambda_{\sigma,m}\alpha_m$, for some $\lambda_{\sigma,1}, ..., \lambda_{\sigma,m} \in \mathbb{Z}/p\mathbb{Z}$. Therefore $\sigma = \sigma_1^{\lambda_{\sigma,1}} \cdot \sigma_2^{\lambda_{\sigma,2}} \cdot ... \cdot \sigma_m^{\lambda_{\sigma,m}}$. For some $\tau \in G_1$, suppose that there exists $A \in \mathcal{A}[p]$ such that $(\sigma - 1)A = Z_\sigma$ and $(\tau - 1)A = Z_\tau$. Then

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau) = (\sigma - 1)A + \sigma((\tau - 1)A) = \sigma(A) - A + \sigma\tau(A) - \sigma(A) = (\sigma\tau - 1)A.$$

Thus, to prove that there exists $A \in \mathcal{A}[p]$ such that $(\sigma - 1)A = Z_\sigma$, for all $\sigma \in G_1$, it suffices to prove that $(\sigma_i - 1)A = Z_{\sigma_i}$, for every $1 \leq i \leq m$. Assume that $Z_{\sigma_i} = (x_{\sigma_i}, y_{\sigma_i}, z_{\sigma_i})$ represents a cocyle in $H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p])$. Since Z_{σ_i} satisfies the local conditions as in Definition 2.1, then there exists $A_i = (\tilde{x_{\sigma_i}}, \tilde{y_{\sigma_i}}, \tilde{z_{\sigma_i}}) \in \mathcal{A}[p]$ such that $(\sigma_i - 1)A_i = Z_{\sigma_i}$, i. e.

$$\begin{pmatrix} 0 & \alpha_i & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \tilde{x_{\sigma_i}} \\ \tilde{y_{\sigma_i}} \\ \tilde{z_{\sigma_i}} \end{pmatrix} = \begin{pmatrix} x_{\sigma_i} \\ y_{\sigma_i} \\ z_{\sigma_i} \end{pmatrix}. \tag{3.3}$$

By equation (3.3), we deduce that $y_{\sigma_i} = z_{\sigma_i} = 0$ and $\alpha_{\sigma_i}\tilde{y_{\sigma_i}} = x_{\sigma_i}$. Thus, without loss of generality we may choose $A_i = (0, \tilde{y_{\sigma_i}}, 0)$, for every $1 \leq i \leq m$. Let $j \in \{1, ..., m\}$. We have

$$\begin{cases} \alpha_{\sigma_i}\tilde{y_{\sigma_i}} = x_{\sigma_i} \\ \alpha_{\sigma_j}\tilde{y_{\sigma_j}} = x_{\sigma_j} \end{cases} \tag{3.4}$$

In a similar way $y_\sigma = z_\sigma = 0$, for all $\sigma \in G_1$. Observe that

$$Z_{\sigma\tau} = \begin{pmatrix} x_\sigma \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 & \alpha_\sigma & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_\tau \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_\sigma \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} x_\tau \\ 0 \\ 0 \end{pmatrix} = Z_\sigma + Z_\tau.$$

Then, because of $y_\sigma = z_\sigma = 0$, the equality $Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau)$ is simply $Z_{\sigma\tau} = Z_\sigma + Z_\tau$, for all $\sigma, \tau \in G_1$. In particular $x_{\sigma\tau} = x_\sigma + x_\tau$ and then, by equation (3.4), we get $x_{\sigma_i\sigma_j} = x_{\sigma_i} + x_{\sigma_j} = \alpha_{\sigma_i}\tilde{y_{\sigma_i}} + \alpha_{\sigma_j}\tilde{y_{\sigma_j}}$.

On the other hand

$$\sigma_i\sigma_j = \begin{pmatrix} 1 & \alpha_{\sigma_i} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha_{\sigma_j} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_{\sigma_i} + \alpha_{\sigma_j} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

implying $x_{\sigma_i\sigma_j} = (\alpha_{\sigma_i} + \alpha_{\sigma_j})\tilde{y_{\sigma_i\sigma_j}}$. Then

$$(\alpha_{\sigma_i} + \alpha_{\sigma_j})\tilde{y_{\sigma_i\sigma_j}} = \tilde{y_{\sigma_i}}\alpha_{\sigma_i} + \tilde{y_{\sigma_j}}\alpha_{\sigma_j},$$

i. e.,

$$(\tilde{y_{\sigma_i\sigma_j}} - \tilde{y_{\sigma_i}})\alpha_{\sigma_i} + (\tilde{y_{\sigma_i\sigma_j}} - \tilde{y_{\sigma_j}})\alpha_{\sigma_j} = 0.$$

Since α_i and α_j are elements of a basis of V, then $\tilde{y_{\sigma_i\sigma_j}} = \tilde{y_{\sigma_i}}$ and $\tilde{y_{\sigma_i\sigma_j}} = \tilde{y_{\sigma_j}}$, implying $\tilde{y_{\sigma_i}} = \tilde{y_{\sigma_j}}$. We have $A_i = A_j$ and then $H^1_{\text{loc}}(G_1, \mathcal{A}[p]) = 0$.

2. The triviality of $H^1_{\text{loc}}(G_2, \mathcal{A}[p])$.

The group G_2 is generated by the matrices of the form

$$\sigma = \begin{pmatrix} 1 & 0 & \alpha_i \\ 0 & 1 & \alpha_j \\ 0 & 0 & 1 \end{pmatrix}, \tag{3.5}$$

where $i, j \in \{1, ..., m\}$ and $\alpha_1, ..., \alpha_m$ form a basis of the vector space V as above. Assume that $Z_\sigma = (x_\sigma, y_\sigma, z_\sigma)$ represents a cocyle in $H^1_{\text{loc}}(G_1, \mathcal{A}[p])$. Then, for every $\sigma \in G_2$, there exists $A_\sigma = (\tilde{x_\sigma}, \tilde{y_\sigma}, \tilde{z_\sigma}) \in \mathcal{A}[p]$ such that $(\sigma - 1)A_\sigma = Z_\sigma$, i. e.

$$\begin{pmatrix} 0 & 0 & \alpha_i \\ 0 & 0 & \alpha_j \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \tilde{x_\sigma} \\ \tilde{y_\sigma} \\ \tilde{z_\sigma} \end{pmatrix} = \begin{pmatrix} x_\sigma \\ y_\sigma \\ z_\sigma \end{pmatrix}. \tag{3.6}$$

By equation (3.6), we deduce that $z_\sigma = 0$ and

$$\begin{cases} \alpha_i\tilde{z_\sigma} = x_\sigma \\ \alpha_j\tilde{z_\sigma} = y_\sigma \end{cases} \tag{3.7}$$

Furthermore, without loss of generality, we may assume that $\tilde{x_\sigma} = \tilde{y_\sigma} = 0$, i. e. $A_\sigma = (0, 0, \tilde{z_\sigma})$. Because of $z_\sigma = 0$, in a similar way as above we have that the equality $Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau)$ is simply $Z_{\sigma\tau} = Z_\sigma + Z_\tau$, for all $\tau \in G_2$. Let

$$\tau = \begin{pmatrix} 1 & 0 & \alpha_h \\ 0 & 1 & \alpha_s \\ 0 & 0 & 1 \end{pmatrix},$$

for some $h, s \in \{1, ..., m\}$. Therefore $x_{\sigma\tau} = x_\sigma + x_\tau = \tilde{z_\sigma}\alpha_i + \tilde{z_\tau}\alpha_h$. On the other hand, as for the matrices of G_1, the entry $x_{\sigma\tau}$ is equal to $(\alpha_i + \alpha_h)\tilde{z_{\sigma\tau}}$. Then

$$(\alpha_i + \alpha_h)\tilde{z_{\sigma\tau}} = \tilde{z_\sigma}\alpha_i + \tilde{z_\tau}\alpha_h.$$

Likewise we get

$$(\alpha_j + \alpha_s)\tilde{z_{\sigma\tau}} = \tilde{z_\sigma}\alpha_j + \tilde{z_\tau}\alpha_s.$$

We have the system of equations

$$\begin{cases} \alpha_i(\tilde{z_\sigma} - \tilde{z_{\sigma\tau}}) + \alpha_h(\tilde{z_\tau} - \tilde{z_{\sigma\tau}}) = 0 \\ \alpha_j(\tilde{z_\sigma} - \tilde{z_{\sigma\tau}}) + \alpha_s(\tilde{z_\tau} - \tilde{z_{\sigma\tau}}) = 0 \end{cases} \tag{3.8}$$

Since α_i, α_j, α_h, α_s are elements of a basis of V, then $\tilde{z_{\sigma\tau}} = \tilde{z_\sigma}$ and $\tilde{z_{\sigma_i\tau}} = \tilde{z_\tau}$, implying $\tilde{z_\sigma} = \tilde{z_\tau}$. Since the matrices of the form (3.5) generate G_2, as i, j vary between 1 and m, then we can conclude that there exists $R \in \mathcal{A}[p]$ such that $(\sigma - 1)R = Z_\sigma$, for all $\sigma \in G_2$. Therefore $H^1_{\text{loc}}(G_2, \mathcal{A}[p]) = 0$.

3. The glueing of the cohomologies

By equation (3.6), without loss of generality, we can choose $A_1 = (0, a, 0)$ and $R = (0, 0, b)$, for some $a, b \in \mathbb{F}_p$. Let $W = (0, a, b)$. We have $(\sigma - 1)W = Z_\sigma$, for every $\sigma \in G_1$ and $(\tau - 1)W = Z_\tau$, for every $\tau \in G_2$. Observe that, for every $\sigma \in G_1$ and $\tau \in G_2$, the cocycle equation implies

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau) = (\sigma - 1)W + \sigma(\tau - 1)W = (\sigma\tau - 1)W.$$

Because of G_1 and G_2 generating G, we get the conclusion.

When $n > 3$

Let $n > 3$. Let G_p be the p-Sylow subgroup of $\mathrm{GL}_n(p^m)$ formed by all the upper triangular matrices. Observe that G_p is generated by the matrices

$$\begin{pmatrix} 1 & * & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \vdots \\ & & & \ddots & 1 & 0 \\ 0 & \dots & & \dots & 0 & 1 \end{pmatrix}; \dots; \begin{pmatrix} 1 & 0 & \dots & 0 & * & 0 \\ 0 & 1 & & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \\ & & \ddots & \ddots & * & \vdots \\ \vdots & & & 0 & 1 & 0 \\ 0 & \dots & & \dots & 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & & \dots & 0 & * \\ 0 & 1 & \ddots & & \vdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ & & & \ddots & 0 & \vdots \\ \vdots & & & \ddots & 1 & * \\ 0 & \dots & & \dots & 0 & 1 \end{pmatrix},$$

with the entries $*$ varying in $\mathbb{F}_p$. For $2 \leq i \leq n$, let M_i be the subgroup of G_p formed by the identity and the matrices with some nonzero entries only in the ith column. By induction, the same techniques used to prove the triviality of $H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p])$ and $H^1_{\mathrm{loc}}(G_2, \mathcal{A}[p])$ as above, show that there exists $W_i = (0, ..., 0, a_i, 0, ..., 0)$, depending only on i, such that $(\sigma - 1)W_i = Z_\sigma$, for all $\sigma \in G_i$. Let $W = (0, a_2, ..., a_i, ..., a_n)$. Then $(\sigma - 1)W = Z_\sigma$, for all $\sigma \in G$.

□

From now on we will assume, without loss of generality, that G is a proper subgroup of $\mathrm{SL}_n(p^m)$.

For $n \in \{2, 3\}$ we give a proof Theorem 3.1 based on a case by case analysis of the possible maximal subgroups of $\mathrm{SL}_n(p^m)$. Then we proceed with the proof of Theorem 1.3 for a general n.

3.1 The case when $n = 2$

In this section we consider algebraic groups $\mathcal{A}$ such that G is isomorphic to a subgroup of $\mathrm{GL}_2(p^m)$, for some positive integer m. In particular this is the case when $\mathcal{A}[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. As stated above if $m = 1$ and $p \neq 2$, then the conclusion of Theorem 3.1 follows immediately by Chevalley's Theorem on the classification of the commutative algebraic groups in characteristc 0 (see for example [43]), combined with the mentioned results in [15] and [21]. Anyway, when $m > 1$, or $m = 1$, $p = 2$ and $\mathcal{A}$ an algebraic torus, there are no similar results in the literature. Thus, here we give a proof for the more

general case when $G \leq \mathrm{GL}_2(p^m)$, with $m \geq 1$. We use the classification of the maximal subgroups of $\mathrm{SL}_2(q)$ appearing in [3], for $q = p^m$, that we partially recall in the next lemma.

Lemma 3.7. *Let $q = p^m$, where p is a prime number and m is a positive integer. The maximal subgroups of $\mathrm{SL}_2(q)$ of type $\mathcal{C}_i$, with $2 \leq i \leq 9$ are*

(a) *a subgroup of type $\mathcal{C}_2$, the generalized quaternion group $Q_{2(q-1)}$ of order $2(q-1)$, with q odd, $q \neq 5$;*

(b) *a subgroup of type $\mathcal{C}_2$, the dihedral group $D_{2(q-1)}$ of order $2(q-1)$, with q even;*

(c) *a subgroup of type $\mathcal{C}_3$, the generalized quaternion group $Q_{2(q+1)}$, of order $2(q+1)$, for q odd;*

(d) *a subgroup of type $\mathcal{C}_3$, the dihedral group $D_{2(q+1)}$ of order $2(q+1)$, for q even;*

(e) *a subgroup of type $\mathcal{C}_5$, the group $\mathrm{SL}_2(q_0).C_2$, with $q = q_0^2$;*

(f) *subgroup of type $\mathcal{C}_5$, the group $\mathrm{SL}_2(q_0)$, with $q = q_0^r$, for q odd, r an odd prime;*

(g) *subgroup of type $\mathcal{C}_5$, the group $\mathrm{SL}_2(q_0)$, with $q = q_0^r$, for q even, $q_0 \neq 2$, r prime;*

(h) *a group of type $\mathcal{C}_6$, the group $2^{1+2}.S_3$, for $q = p \equiv \pm 1 \pmod 8$;*

(i) *a group of type $\mathcal{C}_6$, the group $2^{1+2} : C_3$, for $q = p \equiv \pm 3, 5, \pm 11, \pm 13, \pm 19 \pmod{40}$;*

(j) *a group of type $\mathcal{C}_9$, the group $C_2^{\cdot}A_5$, $q = p \equiv \pm 1 \pmod{10}$ or $q = p^2$, with $p \equiv \pm 3 \pmod{10}$.*

In fact, for $n = 2$ we are going to prove the following stronger result than Theorem 3.1, with the assumption that $\mathcal{A}[p]$ is an irreducible G-module or a direct sum of irreducible G-modules.

Proposition 3.8. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Assume that $G = \mathrm{Gal}(k(\mathcal{A}[p])/k)$ is isomorphic to a subgroup of $\mathrm{GL}_2(p^m)$, for some positive integer m. If $\mathcal{A}[p]$ is an irreducible G_k-module or a direct sum of irreducible G_k-modules, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p]) = 0$.*

Proof. As already noticed in [39], for every group Γ and every direct sum of two Γ-modules M_1 and M_2, one has $H^1_{\mathrm{loc}}(\Gamma, M_1 \times M_2) \simeq H^1_{\mathrm{loc}}(\Gamma, M_1) \bigoplus H^1_{\mathrm{loc}}(\Gamma, M_2)$. Thus $H^1_{\mathrm{loc}}(G, .)$ is an additive functor and it suffices to prove the statement when $\mathcal{A}[p]$ is an irreducible G_k-module, to get an answer even in the case when $\mathcal{A}[p]$ is a direct sum of irreducible G_k-modules. Thus, we may assume without loss of generality that G is not of type $\mathcal{C}_1$ and it is isomorphic to one of the subgroups of $\mathrm{SL}_2(p^m)$ listed in Lemma 3.7. In cases **(a)** (resp. **(c)**), G is a subgroup of the generalized quaternion group $Q_{2(q-1)}$ (resp. $Q_{2(q+1)}$). The group $Q_{2(q-1)}$ (resp. $Q_{2(q+1)}$) is an extension $C_2.C_{q-1}$ (resp. $C_2.C_{q+1}$) of a cyclic group of order 2, with a cyclic group of order $q-1$ (resp. $q+1$). Then G is cyclic or it is an extension of two cyclic groups. Since the local cohomology of a cyclic group is trivial, then by Lemma 3.2, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. In cases **(b)**, **(d)**, **(h)**, **(i)** and **(j)**, for every $p \geq 2$, the p-Sylow subgroup of G is either trivial or cyclic (recall that cases **(h)**, **(i)** and **(j)** may occur only if $p \neq 2$). By Lemma 2.3, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Suppose that we are in case **(e)**. For every $p > 2$, the p-Sylow subgroup G_p of G is a subgroup of $\mathrm{SL}_2(q_0)$, where $q = q_0^2$. Thus, without loss of generality, we may assume that G is a subgroup of $\mathrm{SL}_2(q_0)$. If $G = \mathrm{SL}_2(q_0)$, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, by Lemma 3.6. Assume that G is a proper subgroup of $\mathrm{SL}_2(q_0)$. If G is still of type C_5, then G is isomorphic to a subgroup of $\mathrm{SL}_2(q_1)$, where $q_0 = q_1^2$. Again, if $G = \mathrm{SL}_2(q_1)$, then by Lemma 3.6, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. We may assume that G is a proper subgroup of $\mathrm{SL}_2(q_1)$ and so on. Since m is finite, at a certain point we will find that either G is of type $\mathcal{C}_i$, with $i \neq 5$, or G is trivial. If G is of type $\mathcal{C}_i$, with $i \neq 5$, because of our assumption that G is very strongly irreducible, then G is isomorphic to one of the subgroups listed in cases **(a)**, **(b)**, **(c)**, **(d)**, **(h)**, **(i)** and **(j)**. Thus $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, as above. If G is trivial, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$ too. The same arguments, combined with Lemma 3.2 (recall that we are assuming that $\mathcal{A}[p]$ is irreducible), give $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for $p = 2$ too. Cases **(f)** and **(g)** are similar to case **(e)**, being G_p a subgroup of $\mathrm{SL}_2(q_0)$, with $q = q_0^r$, with r a prime. □

In particular we have proved Theorem 3.1 for $n = 2$.

3.2 The case when $n = 3$

In this section we consider algebraic groups $\mathcal{A}$ such that $\mathcal{A}[p] \cong (\mathbb{Z}/p\mathbb{Z})^3$. As mentioned in the Introduction, in [15] Dvornicich and Zannier underline that the answer in this case is not obvious. In fact, they show an example in which $H^1_{\mathrm{loc}}(\Gamma, \mathbb{Z}/p\mathbb{Z}) \neq 0$, where Γ is a

subgroup of the p-Sylow subgroup of $\mathrm{GL}_3(p)$ of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & \lambda a \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b \in \mathbb{Z}/p\mathbb{Z}, \lambda \in \mathbb{Z}/p\mathbb{Z}^*.$$

Anyway, they have no evidence that this group is really the p-Sylow subgroup of a Galois group $\mathrm{Gal}(k(\mathcal{A}[p])/k, \mathcal{A}[p])$. Even in the case when Γ would be the p-Sylow subgroup of a certain Galois group $\mathrm{Gal}(k(\mathcal{A}[p])/k, \mathcal{A}[p])$, we could get no information about the algebraic group $\mathcal{A}$ for which the local-global divisibility fails. Here we prove Theorem 3.1 for $n = 3$.

We use the classification of the maximal subgroups of $\mathrm{SL}_3(q)$ and of $\mathrm{SU}_3(q)$ appearing in [3].

Lemma 3.9. *Let $q = p^m$, where p is a prime number and m is a positive integer. Let $d := \gcd(q-1, 3)$. The maximal subgroups of $\mathrm{SL}_3(q)$ of type $\mathcal{C}_i$, with $3 \leq i \leq 9$ are*

(a) *a group of type $\mathcal{C}_2$, the group $C_{q-1}^2 : S_3$, for $q \geq 5$;*

(b) *a group of type $\mathcal{C}_3$, the group $C_h : C_3$, where $h = q^2 + q + 1$;*

(c) *a group of type $\mathcal{C}_5$, the group $\mathrm{SL}_3(q_0).C_s$, where $s := \gcd\left(\frac{q-1}{p-1}, 3\right)$ and $q = q_0^r$, r prime.*

(d) *a group of type $\mathcal{C}_6$, the group $3_+^{1+2} : Q_8.C_s$, where $s = \frac{\gcd(q-1,9)}{3}$, $q = p \equiv 1 \pmod 3$ and the extraspecial group 3_+^{1+2} is the p-Sylow subgroup of $\mathrm{GL}_3(p)$;*

(e) *a group of type $\mathcal{C}_8$, the group $\mathrm{SO}_3(q) \times C_d$, with q odd;*

(f) *a group of type $\mathcal{C}_8$, the group $\mathrm{SU}_3(q_0) \times C_t$, where $t := \gcd(p-1, 3)$ and $q = q_0^2$;*

(g) *a group of type $\mathcal{C}_9$, the group $\mathrm{PSL}_2(7) \times C_d$, for $q = p \equiv 1, 2, 4 \pmod 7, q \neq 2$;*

(h) *a group of type $\mathcal{C}_9$, the group $C_3 \cdot A_6$, of order $9 \cdot 5!$, for $q = p \equiv 1, 4 \pmod{15}$ or $q = p^2$, with $p \equiv 2, 3 \pmod 5, p \neq 3$.*

Lemma 3.10. *Let $q = p^m$, where p is a prime number and m is a positive integer. Let $d := \gcd(q-1, 3)$. The maximal subgroups of $\mathrm{SU}_3(q)$ of type $\mathcal{C}_i$, with $3 \leq i \leq 9$ are*

(e.1) *a group of type $\mathcal{C}_2$, the group $C_{q-1}^2 : S_3$, for $q \geq 5$;*

(e.2) *a group of type $\mathcal{C}_3$, the group $C_h : C_3$, where $h = q^2 + q + 1$, $q \neq 3$;*

(e.3) *a group of type $\mathcal{C}_5$, the group $\mathrm{SU}_3(q_0).C_s$, where $s := \gcd\left(\frac{q+1}{q+1}, 3\right)$ and $q = q_0^r$, r prime;*

(e.4) *a group of type $\mathcal{C}_8$, the group $\mathrm{SO}_3(q) \times C_d$, q odd and $q \geq 7$;*

(e.5) *a group of type $\mathcal{C}_6$, the group $3_+^{1+2} : Q_8.C_s$, where $s = \frac{\gcd(q+1,9)}{3}$, the extraspecial group 3_+^{1+2} is the p-Sylow subgroup of $\mathrm{GL}_3(p)$, $q = 5$ or $q = p \equiv 2 \pmod 3$ and $q \geq 11$;*

(e.6) *a group of type $\mathcal{C}_9$, the group $\mathrm{PSL}_2(7) \times C_d$, $q = p \equiv 3, 5, 6 \pmod 7$;*

(e.7) *a group of type $\mathcal{C}_9$, the group $C_3 \cdot A_6$, for $q = p \equiv 11, 14 \pmod{15}$;*

(e.8) *a group of type $\mathcal{C}_9$, the group $C_3 \cdot A_6 C_2$, (where here C_2 is a known specific quotient of A_6), for $q = p = 5$;*

(e.9) *a group of type $\mathcal{C}_9$, the group $C_3 \cdot A_7$, of order $9 \cdot 7 \cdot 5!$, for $q = p = 5$.*

Proof of Theorem 3.1 for $n = 3$. As in the case when $n = 2$, since $H^1_{\mathrm{loc}}(G, .)$ is an additive functor, we assume without loss of generality that G is not of type $\mathcal{C}_1$ and then it is a subgroup of the groups listed in Lemma 3.9. We are going to show that $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 3$. In cases **(a)**, **(b)** and **(d)** the p-Sylow subgroup of G is either trivial or cyclic, for all p (recall that case **(a)** occur only for $p \geq 5$ and case **(a)** occur only for $q = p \equiv 1 \pmod 3$). Therefore $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Assume that we are in case **(g)**. Since this case may occur only for $p \neq 3$, then the p-Sylow subgroup of G is isomorphic to a subgroup of $\mathrm{PSL}_2(7)$. Therefore, for every $p \geq 2$, the p-Sylow subgroup of G is either trivial or cyclic and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$ (recall that this case does not hold when $p = 2$ too). Assume that we are in case **(h)**. If $p \geq 3$, then the p-Sylow subgroup of G is trivial or cyclic again (observe that this case does not happen when $p = 3$). Assume that we are in case **(c)**. For every $p \neq 3$, the p-Sylow subgroup of G is a subgroup of $\mathrm{SL}_3(q_0)$. Since $\mathrm{SL}_3(q_0)$ is a normal subgroup of G and G is very strongly irreducible, we may assume, without loss of generality, that $G \subseteq \mathrm{SL}_3(q_0)$. If $G = \mathrm{SL}_3(q_0)$, then $H^1(G, \mathcal{A}[p]) = 0$, by Lemma 3.6. If G is trivial, then $H^1(G, \mathcal{A}[p]) = 0$ too. So, suppose that G is a non-trivial proper subgroup of $\mathrm{SL}_3(q_0)$. If G is still of type $\mathcal{C}_5$ in $\mathrm{SL}_3(q_0)$, then G is contained in $\mathrm{SL}_3(q_1).C_{s_1}$, where $q_0 = q_1^2$ and $s_1 = \frac{\gcd(q_0-1,9)}{3}$. Again, we may

assume that G is strictly contained in $\mathrm{SL}_3(q_1)$ and so on. Since q is finite, after a finite number of steps we find that G is of type $\mathcal{C}_i$, with $i \neq 5$. We have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, by the arguments used for the subgroups of classes $\mathcal{C}_i$, with $i \neq 5$. Thus $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$ too. If $p = 3$, we can use the same argument as for $p \neq 3$, combined with Lemma 3.2 (by the hypothesis of the very strongly irreducibility of $\mathcal{A}[p]$). Assume that we are in case **(e)**. Again, for all p, the p-Sylow subgroup G_p of G is contained in $\mathrm{SO}_3(q)$. Since G is very strongly irreducible, by Lemma 3.2 we may assume without loss of generality that G is contained in $\mathrm{SO}_3(q)$. The group $\mathrm{SO}_3(q)$ is isomorphic to $\mathrm{SL}_2(q)$ (see [3, Proposition 1.10.1]). If $G = \mathrm{SO}_3(q)$, then $-I \in G$ and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, because of Lemma 2.5. Assume that G is strictly contained in $\mathrm{SO}_3(q)$. In the proof of Theorem 3.1 for $n = 2$, we have seen that G still contains $-I$ or its p-Sylow subgroup G_p is either trivial or cyclic. In all cases the first cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ vanishes.

Suppose that we are in case **(f)**. By Lemma 3.2 and the assumption that $\mathcal{A}[p]$ is very strongly irreducible, we may assume without loss of generality that $G \leq \mathrm{SU}_3$. Thus we use Lemma 3.10. There are only four cases in which the subgroups of SU_3 are different from the ones listed in Lemma 3.9, i. e. cases **(e.3)**, **(e.5)**, **(e.8)** and **(e.9)**. For all p, in cases **(e.5)**, **(e.8)** and **(e.9)**, the p-Sylow subgroup is either trivial or cyclic. Thus $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Since the p-Sylow subgroup of $\mathrm{SU}_3(q_0)$ coincides with the p-Sylow subgroup of $\mathrm{SL}_3(q_0)$, we can treat case **(e.3)** in the same way as case **(c)**. We have proved that for every possible G, if $\mathcal{A}[p]$ is a very strongly irreducible G-module and $p \geq 3$, then the local-global divisibility by p holds in $\mathcal{A}$ over k. □

3.3 General Case

To prove Theorem 3.1 for every n, we use the description of the subgroups of $\mathrm{GL}_n(q)$ of geometric type shown in Table 1. For some classes of groups we also use induction, having already proved the statement for $n \leq 3$. When the p-Sylow subgroup of G is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, there are known counterexample to the local-global divisibility (see the mentioned [15], [16], [36]) and also even when $(\mathbb{Z}/p\mathbb{Z})^3$ there are counterexamples (see [35] again). Then in various parts of the proof we will show that for $p \geq n + 1$, or respectively for $p \geq n/2 + 1$, the p-Sylow subgroup of G is either trivial or cyclic (which does not hold for $p \leq n + 1$, or respectively $p \leq n/2 + 1$).

Proof of Theorem 3.1 Since we have already proved the statement for $n \in \{2, 3\}$, we

assume $n \geq 4$. Suppose that for every integer $n' < n$, the local-global divisibility by p holds in commutative algebraic groups $\mathcal{A}$ over k when $G \leq \mathrm{GL}_{n'}$ acts very strongly irreducibly on $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{n'}$ and $p > n'$. As in the cases when $n = 2$ and $n = 3$, since $H^1_{\mathrm{loc}}(G, .)$ is an additive functor, we may assume, without loss of generality, that G is not of class $\mathcal{C}_1$.

Part i. Subgroups of geometric type

Class $\mathcal{C}_2$

Assume that G is of class $\mathcal{C}_2$. In this case $\mathcal{A}[p] = \bigoplus_{i=1}^{r} A_i$, with each A_i of dimension t and $G = (G_1 \times ... \times G_r) \wr S_r$, where G_i is a subgroup of $\mathrm{GL}_t(q)$ acting on $\mathcal{A}_i$ and $tr = n$. In this situation $\mathcal{A}[p]$ is irreducible, but not very strongly irreducible (nor strongly irreducible). By our assumptions, then $\mathcal{A}[p]$ has to be a direct sum of very strongly irreducible G-modules. In particular G_i is very strongly irreducible for all $1 \leq i \leq r$. If $p > r$, then the p-Sylow subgroup of G is contained in $G_1 \times ... \times G_r$. Since $H^1_{\mathrm{loc}}(G, .)$ is an additive functor, by induction we get that $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for $p \geq \max\{r+1, t+1\}$. Observe that the greatest r that we can have is $r = n$ itself. But in this case $t = 1$ and $\mathcal{A}[p] = \bigoplus_{i=1}^{n} A_i$, with each A_i of dimension 1. The group G is then a subgroup of $C_{q-1}^n.S_n$. If $p > n/2$, the p-Sylow subgroup of G is either trivial or cyclic and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ is trivial. If $r \neq n$, then $r \leq n/2$, and $t \leq n/2$ too. Thus $\max\{r+1, t+1\} \leq n/2$. If $p \geq n/2 + 1$, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$.

Class $\mathcal{C}_3$

Suppose that G is of type $\mathcal{C}_3$. In this situation the G-module $\mathcal{A}[p]$ is considered as vector space over a a field extension $\tilde{F}$ of $\mathbb{F}_{p^m}$ with degree a prime number r dividing n. The p-torsion subgroup $\mathcal{A}[p]$ has dimension $t := n/r$ as a vector space over $\tilde{F}$ (see [28, §5.3 and Table 2.1.A]) and G is isomorphic to a subgroup of $\mathrm{GL}_t(p^{mr}).C_r$. If $r = n$ (this in particular happens if n is a prime), then the only possible subgroup of class C_3 is $\mathrm{GL}_1(p^{mn}).C_n$. Since the cardinality of $\mathrm{GL}_1(p^{mn})$ is $\frac{p^{mn}-1}{p-1}$, then, for every p, the p-Sylow subgroup of G is either trivial or cyclic and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. If $r \neq n$, then $1 < r \leq n/2$. Therefore, for all $p \geq n/2 + 1$, the p-Sylow subgroup of G is contained in $\mathrm{GL}_t(p^{mr})$. Observe that $G \cap \mathrm{GL}_t(p^{mr})$ is very strongly irreducible too. Since $1 < t \leq n/2$ too, we use induction (recall that here $\mathcal{A}[p]$ is considered as a vector space of dimension $t < n$ over $\tilde{F}$) and Lemma 3.2 to get $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for every $p \geq n/2 + 1$.

Class $\mathcal{C}_4$

Suppose that G is of type $\mathcal{C}_4$. Observe that this case does not occur when n is a prime. The group G is isomorphic to a subgroup of a central product $\mathrm{GL}_t(p^m) \circ \mathrm{GL}_r(p^m)$ acting on a tensor product $V_1 \otimes V_2 = \mathcal{A}[p]$, where $rt = n$ and V_1, V_2 are vector spaces over $\mathbb{F}_{p^m}$, with dimension respectively t and r. A central product Γ of two groups is a quotient of their direct product by a subgroup of its center. Then every subgroup of Γ is a central product of two groups too (where one of the two groups or both can be trivial). So let $G = G_t \circ G_r$, with G_t acting on V_1 and G_r acting on V_2 (see also [28, §4.4]). Consider $Z_{\sigma\otimes\tau}$, with $\sigma \otimes \tau \in G_t \circ G_r$, representing a cocycle of G with values in $\mathcal{A}[p] = V_1 \otimes V_2$. If $Z_{\sigma\otimes\tau}$ satisfies the local conditions, then there exists $A_{\sigma\otimes\tau} \in V_1 \otimes V_2$ such that $Z_{\sigma\otimes\tau} = (\sigma \otimes \tau - 1 \otimes 1)A_{\sigma\otimes\tau}$, for all $\sigma \otimes \tau \in G_t \circ G_r$. Observe that $A_{\sigma\otimes\tau} = A^{(1)}_{\sigma\otimes\tau} \otimes A^{(2)}_{\sigma\otimes\tau}$, for some $A^{(1)}_{\sigma\otimes\tau} \in V_1$ and $A^{(2)}_{\sigma\otimes\tau} \in V_2$. We can construct a cocycle $Z_\sigma := (\sigma - 1)A_\sigma$, with $\sigma \in G_t$, by choosing A_σ among the possible $A^{(1)}_{\sigma\otimes\tau} \in V_1$. In the same way we can construct a cocycle $Z_\tau := (\tau - 1)A_\tau$, with $\tau \in G_r$, by choosing A_τ among the possible $A^{(2)}_{\sigma\otimes\tau} \in V_2$. For the tensor product construction, a priori we could have more than one choice of A_σ (respectively A_τ) for each σ (resp. τ). Anyway, we choose just one A_σ (resp. A_τ). Observe that even in the general case of Definition 2.1, when a cocycle satisfies the local conditions, there could exist various A_σ giving the equality $Z_\sigma = (\sigma - 1)A_\sigma$. Anyway we make just one choice for $A_\sigma \in \mathcal{A}[q]$, for each $\sigma \in G$. Since $r < n$, by induction $H^1_{\mathrm{loc}}(G_r, V_1) = 0$, for every $p \geq r + 1$ (observe that G_r is very strongly irreducible itself by our assumptions). Then there exists $A \in V_1$, such that $Z_\sigma = (\sigma - 1)A$, for all $\sigma \in G_r$. In the same way, since $t < n$, then by induction, for all $p \geq t + 1$, we have $H^1_{\mathrm{loc}}(G_t, V_2) = 0$ (again G_t itself is very strongly irreducible). Thus there exists $B \in V_2$, such that $Z_\tau = (\tau - 1)B$, for all $\tau \in G_t$. Therefore $Z_{\sigma\otimes\tau} = (\sigma \otimes \tau - 1 \otimes 1)A \otimes B$, for all $\sigma \otimes \tau \in G_t \circ G_r$, and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Since $r \leq n/2$ and $t \leq n/2$, as above, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for every $p \geq n/2 + 1$.

Class $\mathcal{C}_5$

If G is of class $\mathcal{C}_5$, then G is isomorphic to a subgroup of $\mathrm{GL}_n(p^t)$, where $m = tr$, with t a positive integer and r a prime. Observe that this case does not occur when $m = 1$. If G is the whole group $\mathrm{GL}_n(p^t)$, then by Lemma 3.6, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. If G is trivial, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ is trivial too. Suppose that G is a proper non-trivial subgroup of $\mathrm{GL}_n(p^t)$. If G is still of class $\mathcal{C}_5$, then G is isomorphic to a subgroup of $\mathrm{GL}_n(p^{t_2})$,

for some positive integer t_2, such that $t = r_2 t_2$, with r_2 prime. If $G = \mathrm{GL}_n(p^{t_2})$, again $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, by Remark 3.5 and Lemma 3.6. Then we may assume that G is a proper subgroup of $\mathrm{GL}_n(p^{t_2})$ and so on. Since m is finite and we are assuming that G is not trivial, then G is isomorphic to a subgroup of $\mathrm{GL}_n(p^{t_j})$ (for some positive integer t_j dividing m) of class $\mathcal{C}_i$, with $i \neq 5$. We may then repeat the arguments used (or that we will use) for other classes $\mathcal{C}_i$, with $i \notin \{1, 5\}$, to get $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$.

Class $\mathcal{C}_6$

Suppose that G is of class $\mathcal{C}_6$, i. e. G lies in the normalizer of an extraspecial group. This may happen only when $n = r^t$, with r a prime different from p and t a positive integer. The possible maximal subgroup of class $\mathcal{C}_6$ is $(C_{q-1} \circ r^{1+2t}).\mathrm{Sp}_{2t}(r)$ (see [28, §3.5]). To ease notation we denote by H the normal subgroup $C_{q-1} \circ r^{1+2t}$. Let $G' := G \cap H$. Owing to $p \neq r$, the p-Sylow subgroup G'_p of G' is trivial. Then the p-Sylow subgroup G_p of G is isomorphic to the p-Sylow subgroup of G/G' that is isomorphic to a subgroup of $\mathrm{Sp}_{2t}(r)$. Since $p \neq r$, then p divides the cardinality $|\mathrm{Sp}_{2t}(r)|$ if and only if p divides $\prod_{i=1}^{t}(r^{2i} - 1) = (r-1)(r+1)...(r^{t-1} - 1)(r^{t-1} + 1)(r^t - 1)(r^t + 1)$. Observe that $r^{t-1} = r^t/r \geq n/2$. If $p \neq 2$, then $r^{t-1} = n/r < n/2$. Moreover for all $p \neq 2$, if $p|(n+1)$, then $p \nmid (n-1)$ and the other way around. The greatest factor of $(r-1)(r+1)...(r^{t-1} - 1)(r^{t-1} + 1)(r^t - 1)(r^t + 1)$ is $r^t + 1 = n + 1$. If $p > n/2$ (in particular we have $p > 2$, being $n \geq 4$), then $p^2 > n^2/4 > n + 1$, for all $n > 4$. Thus if $p \geq n/2 + 1/2$ and $n > 4$, we have that $p^2 \nmid |\mathrm{Sp}_{2t}(r)|$ and the p-Sylow subgroup of G is either trivial or cyclic. Consequently $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. We have to control what happens for $n = 4$. By the classification of the maximal subgroups of $\mathrm{SL}_4(q)$ appearing in [3, Table 8.9, pag. 381], one sees that there are the following two maximal subgroups of class $\mathcal{C}_6$

the group $C_4 \circ 2^{1+4}.S_6$, for $q = p \equiv 1 \pmod 8$;

the group $C_4 \circ 2^{1+4}.A_6$, for $q = p \equiv 5 \pmod 8$.

In both cases the p-Sylow subgroups of G is either trivial or cyclic for every p (since the groups occur only for certain primes as above). We can conclude for every n, that $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ is trivial, for all $p \geq n/2 + 1$.

Class $\mathcal{C}_7$

Assume that G is of class $\mathcal{C}_7$. This case occur only when $n = r^t$, where r is a prime and $t > 1$. The group G is the stabilizer of a tensor product decomposition $\bigotimes_{i=1}^{t} V_r$, with $n = r^t$, $t \geq 2$ and $\dim(V_i) = r$, for every $1 \leq i \leq t$. Thus G is a subgroup of $\underbrace{(\mathrm{GL}_r(q) \circ ... \circ \mathrm{GL}_r(q))}_{t}.S_t$. If $p > t$, then the p-Sylow subgroup of G is contained in $G' = G \cap \underbrace{(\mathrm{GL}_r(q) \circ ... \circ \mathrm{GL}_r(q))}_{t}$. In this case, by using induction on t and the argument given in the case when G is of class $\mathcal{C}_4$ as the base of the induction, we have $H^1_{\mathrm{loc}}(G', \mathcal{A}[p]) = 0$, for all $p \geq \max\{t+1, r+1\}$ (recall that we are assuming that $\mathcal{A}[p]$ is very strongly irreducible). Obviously $t \leq n/2$ and $r \leq n/2$. Then if we take $p \geq n/2+1$, we still have that the p-Sylow subgroup of G is contained in G' and $H^1_{\mathrm{loc}}(G', \mathcal{A}[p]) = 0$.

Class $\mathcal{C}_8$

Suppose that G is of class $\mathcal{C}_8$. If n is even, then G is contained either in the group $\mathrm{Sp}_n(p^m)$, or in a group $\mathrm{O}^\epsilon_n(p^m)$, for some $\epsilon \in \{+,-\}$, or in the group $U_n(p^{\frac{m}{2}})$, with m even too. If n is odd, then G is contained either in $\mathrm{O}_n(p^m)$, or in $U_n(p^{\frac{m}{2}})$ (with m even). If G is the whole group $U_n(p^{\frac{m}{2}})$, then its p-Sylow subgroup G_p coincides with the p-Sylow subgroup of $\mathrm{GL}_n(p^m)$, i. e. the p-Sylow subgroup of $\mathrm{SL}_n(p^m)$. By Lemma 3.6, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. If G is the whole symplectic group $\mathrm{Sp}_n(p^m)$ (with n even) or one of the whole orthogonal groups, then contains $-I$ and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, by Lemma 2.5. Assume that G is strictly contained in one of those classical groups. Aschbacher's theorem holds for unitary, symplectic and orthogonal groups too and the maximal subgrops of those classical groups are still divided in the same 9 classes (see [28]). From the classification of the maximal subgroups of $\mathrm{Sp}_n(p^m)$, $\mathrm{O}_n(p^m)$, $\mathrm{O}^\epsilon_n(p^m)$ and $U_n(p^{\frac{m}{2}})$ of class $\mathcal{C}_i$, $i \neq 9$ appearing in [28, Table 3.5B, Table 3.5C, Table 3.5D and Table 3.5E], we have that $\mathrm{O}_n(p^m)$, $\mathrm{O}^\epsilon_n(p^m)$ and $U_n(p^{\frac{m}{2}})$ do not contain groups of class $\mathcal{C}_8$ and that the subgroups of $\mathrm{Sp}_n(p^m)$ of class $\mathcal{C}_8$ are $\mathrm{O}^\epsilon_n(p^m)$ themselves. Since we are assuming that G is strictly contained in one of those three groups, then it is a subgroup of class $\mathcal{C}_i$, for some $i \neq 8$. By repeating the arguments used for the maximal subgroups of $\mathrm{SL}_n(q)$ of class $\mathcal{C}_i$, with $i \neq 8$ (see *ii* below for class $\mathcal{C}_9$), for the maximal subgroups of symplectic, orthogonal and unitary groups, we get the conclusion.

Part ii. Subgroups of class $\mathcal{C}_9$

Suppose that G is of class $\mathcal{C}_9$ and let $Z(G)$ be its center. By the description of the subgroups of class C_9, recalled in Section 2, the group $G/Z(G)$ is almost simple. Because

of Sah's Theorem, if $Z(G)$ is nontrivial, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. So, without loss of generality, we may assume that $Z(G)$ is trivial and G is almost simple. Thus G contains a simple group S and it is contained in the automorphism group of S

$$S \leq G \leq \mathrm{Aut}(S). \tag{3.9}$$

In particular, if G is a subgroup of $\mathrm{GL}_n(p^m)$, then S is a subgroup of $\mathrm{GL}_n(p^m)$ too. So, first of all, we consider the possible simple groups S contained in $\mathrm{GL}_n(p^m)$, for a certain n. Observe that S is not a cyclic group by (3.9). The classification of the finite simple groups is well-known, as well as the list of their automorphisms groups. One of the most complete references in the literature is Wilson's book on finite simple groups [48]. Following that text, we will divide the simple groups in four classes: alternating groups, sporadic groups, classical groups and exceptional groups. We will consider the twisted exceptional group (i. e. the Ree groups, the Suzuki groups, the group ${}^3D_4(q)$ and the group ${}^2E_6(q)$) among the exceptional groups. We will also call groups of Lie type the classical and the exceptional groups.

Alternating groups

Assume that S is an alternating group A_N, for some positive integer N. Since the cardinality of the outer automorphism group of A_N divides 4 for all N, then we may assume without loss of generality that $G = S$. By [28, Proposition 5.3.7 (i)], we have that the minimal degree for a representation of A_N in $\mathrm{GL}_n(p^l)$, for $n \geq 9$, is $N - 2$, i. e. $n \geq N - 2$. Then $N \leq n + 2$. Since $|A_{n+2}| = \dfrac{(n+2)!}{2}$, if $p \geq n + 1$, then $p^2 \nmid |A_{n+2}|$ (recall $n \geq 9$). In particular p^2 does not divide the cardinality of every possible subgroup of $\mathrm{GL}_n(p^l)$ of type C_9 isomorphic to A_N, for every positive integer N. We have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq n+1$, $n \geq 9$. We will treat the case when $n \leq 8$ in *Part iii.* below. In particular we will see that the bound $p \geq n/2 + 1$ is in fact sufficient for the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$, when G is an alternating group, for all $4 \leq n \leq 250$.

Sporadic groups

Assume that S is a sporadic group. Then $p = 13$ is the greatest prime number such that p^2 could eventually divide its cardinality (this is the case of the Monster group). Furthermore, for every sporadic group, the outer automorphism group is either trivial or cyclic of order 2. Then for $p > 13$, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. If $n \geq 25$, the bound

$p \geq n/2+1$ covers the case of sporadic groups too, as well as the cases of the groups of geometric type. We will see in *Part iii.* below that the same bound $p \geq n/2+1$ assures the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$, when G is a sporadic group, for all $n \leq 25$.

Groups of Lie type

Now assume that S is neither alternating, nor sporadic. If $p > 3$, then the automorphisms of the field $\mathbb{F}_{p^m}$, generated by the Frobenius map $\mathfrak{f} : x \mapsto x^p$, are the only automorphisms of S, whose order can be divided by p. The Frobenius automorphisms form a group of outer automorphisms of S isomorphic to C_m. Then we have outer automorphisms of S with order divided by p if and only if $p \mid m$. Thus we may assume $G \simeq S.C_m$. Being $\mathcal{A}[p]$ very strongly irreducible, we have that the vanishing of $H^1_{\mathrm{loc}}(S, \mathcal{A}[p])$ implies the vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$, by Lemma 3.2. So it suffices to prove $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, for all group S of Lie type, whenever $p \geq n+1$. We are going to consider two distinct situation: when the characteristic of the field of definition of S is different from p (the so-called cross characteristic case in the literature) and when the characteristic of the field of definition of S is equal to p (the so-called defining characteristic case).

Cross characteristic case

If the characteristic of the field of definition of S is different from p, then we have an explicit lower bound for the degrees of the representations of S, as one can see in [28, Table 5.3.A, pag. 188] (see also [31] and [25]). In particular if S is isomorphic to $\mathrm{PSL}_2(r^\alpha)$, for some odd prime r and some positive integer α, then $n \geq \frac{r^\alpha - 1}{2}$ (by [28, Table 5.3.A, pag. 188]). Thus $r^\alpha \leq 2n+1$. Being $r \neq p$, if a prime p does not divide $(r^\alpha+1)(r^\alpha-1)$, then p does not divide the cardinality of $\mathrm{SL}_2(r^\alpha)$.

Observe that every odd prime p that divides $r^\alpha + 1$ does not divide $r^\alpha - 1$ and the other way around. Moreover $r^\alpha + 1 \leq 2n+2$. Suppose $p \geq n/2+1$. Then $p^2 > \frac{(n+1)^2}{4} \geq 2n+2$, for all $n \geq 7$. Therefore the p-Sylow subgroup of S is either trivial or cyclic and $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. In *Part iii.* we will analyze case by case all the subgroups of $\mathrm{GL}_n(p^m)$ of class $\mathcal{C}_9$, for every $n \leq 6$ and we will show that the bound $p \geq n/2+1$ assures $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all n. If S is isomorphic to $\mathrm{PSL}_2(2^\alpha)$, the bound for n is $n \geq 2^\alpha - 1$ (see again [28, Table 5.3.A, pag. 188]).

With an analogous argument as for odd primes r, if $p \geq n/2+1$, then p^2 does not divide $(2^\alpha+1)(2^\alpha-1)$, for all $n \geq 4$ and $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Now suppose $S = \mathrm{PSL}_t(r^\alpha)$, for some $t \geq n$ and $r \neq p$. The bound for n is $n \geq (r^\alpha)^{n-1} - 1$ [28, Table 5.3.A, pag. 188]. Then $r^\alpha \leq \sqrt[n-1]{n+1}$. As above, since $p \neq r$, if $p \nmid \prod_{i=2}^{t}((r^\alpha)^i - 1)$, then p does not divide the cardinality of $\mathrm{SL}_t(r^\alpha)$. Observe that $\prod_{i=2}^{t}((r^\alpha)^i - 1) \leq \prod_{i=2}^{n-1}(\sqrt[n-1]{(n+1)^i} - 1)$. The greatest factor in the last product is $\sqrt[n-1]{(n+1)^{n-1}} - 1 = n$. If $p \geq n$ (in particular if $p \geq n+1$), then p^2 does not divide $\prod_{i=2}^{t}((r^\alpha)^i - 1)$. Therefore the p-Sylow subgroup of S is either trivial or cyclic and then $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. Now suppose $S = PU_t(r^\alpha)$, for some $t \geq n$ and $r \neq p$. To ease notation, from now on let $r^\alpha = w$. When n is odd, the bound is $n \geq w\frac{w^{n-1}-1}{w+1}$, and, when n is even, the bound is $n \geq \frac{w^{n-1}-1}{w+1}$ [28, Table 5.3.A, pag. 188]. Firstly suppose that n is odd. We have $w \leq \sqrt[n-1]{\frac{w+1}{w}n+1}$. Observe that $\frac{w+1}{w} \leq \frac{3}{2}$. Thus $w \leq \sqrt[n-1]{\frac{3}{2}n+1}$. If a prime p does not divide $\prod_{i=2}^{t}((w)^i - (-1)^i)$, then it does not divides the cardinality of $S = PU_t(w)$. We have $\prod_{i=2}^{t}((w)^i - (-1)^i) \leq \prod_{i=2}^{n-1}\left(\sqrt[n-1]{\left(\frac{3}{2}n+1\right)^i} - (-1)^i\right)$. The greatest factor in the last product is $\sqrt[n-1]{\left(\frac{3}{2}n+1\right)^{n-1}} - (-1)^{n-1} = \frac{3}{2}n+2$ (recall that n is odd). Observe that $n+1 > \frac{1}{2}\left(\frac{3}{2}n+2\right)$. If $p \geq n+1$, then $p^2 \nmid \frac{3}{2}n+2$. Moreover $p \geq n+1 > \frac{w^i+1}{2}$, for all i, and in particular $p \geq n+1 \geq \frac{w^i-(-1)^i}{2}$. Suppose that $p \mid (w)^i - (-1)^i$ and $p \mid (w)^j - (-1)^j$, for some $2 \leq i < j \leq n-1$. If i, j are both odd, then p divides $w^j + 1 - (w^i + 1) = w^i(w^{j-i} - 1)$. Being $p \neq r$, we have $p \mid w^{j-i} - 1$. Since $p \geq n+1 > \frac{w^{j-i}-1}{2}$, the only possibility is $p = w^{j-i} - 1$. Then $n+1 \leq p = w^{j-i} - 1 \leq \sqrt[n-1]{(\frac{3}{2}n+1)^{j-i}} + 1 \leq \sqrt[n-1]{(\frac{3}{2}n+1)^{n-2}} + 1$ and we have a contraddiction. So, for all $p \geq n+1$ the p-Sylow subgroup of G is either trivial or cyclic and $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. If i, j are both even, we can repeat the same argument. If j is even and i is odd (or i is even and j odd), we get that p divides $w^i(w^{j-i} + 1)$. We may apply again the same argument, owing to $p \geq n+1 \geq \frac{w^i+1}{2}$, for all i. If n is even the bound is $n \geq \frac{w^{n-1}-1}{w+1}$. So $w \leq \sqrt[n-1]{\frac{w+1}{w}} \leq \sqrt[n-1]{\frac{w+1}{w}}$ and we may use the same argument applied when n is odd to get $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. The other minimal bounds for n appearing in [28, Table 5.3.A, pag. 188], when S is a classical group in cross characteristic, are very similar to the ones already discussed. So, with arguments that are very much akin to the ones already shown when S is the projective special linear group or the unitary group, one can verify that $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, for all $p \geq n+1$,

whenever S is a classical group of Lie Type in cross characteristic.

Assume that S is the exceptional group $E_8(w)$. In this case the lower bound for the dimension of the representation is $w^{27}(w^2-1)$ (again [28, Table 5.3.A, pag. 188]). Thus $w^{27} \leq \frac{n}{w^2-1} \leq \frac{n}{3}$, i. e. $w \leq \sqrt[27]{\frac{n}{3}}$. A prime $p \neq r$ divides the cardinality of $E_8(w)$ if and only if it divides the product $\prod_{i=0}^{3}(w^{6i+2}-1)\prod_{i=2}^{5}(w^{6i}-1)$. We have $\prod_{i=0}^{3}(w^{6i+2}-1)\prod_{i=2}^{5}(w^{6i}-1) \leq \prod_{i=0}^{3}(\sqrt[27]{(\frac{n}{3})^{6i+2}}-1)\prod_{i=2}^{5}(\sqrt[27]{(\frac{n}{3})^{6i}}-1)$. If $p \geq n+1$, then p is always strictly greater than every factor in that last product, except the greatest one $\sqrt[27]{(\frac{n}{3})^{30}}-1$. Anyway, in this case $p^2 \geq (n+1)^2 > \sqrt[27]{(\frac{n}{3})^{30}}-1$. Thus the p-Sylow subgroups of G is either trivial or cyclic and $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. In similar ways, using the bounds in [28, Table 5.3.A, pag. 188], one sees that the assumption $p \geq n+1$ is always sufficient to get the conclusion $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, when S is an exceptional group of Lie type in cross characteristic.

Defining characteristic case

Assume that the characteristic of the field of definition of S is p. We have that S is a classic group, with dimension $t < n$ (see [28, Table 5.4.C, pag. 200]) or an exceptional group. If S is a classic group then S is a projective linear group or a projective symplectic group or a projective unitary group or a projective orthogonal group. In all cases S is a quotient by scalar matrices of a classical matrix group. Observe that if Γ is a matrix group and $P\Gamma$ is its quotient modulo scalar matrices, then the p-Sylow subgroup of $P\Gamma$ is an isomorphic copy of the p-Sylow subgroup of Γ (no scalar matrix has order dividing p, for $p > 2$). Thus $H^1_{\mathrm{loc}}(\Gamma, \mathcal{A}[p]) = 0$ implies $H^1_{\mathrm{loc}}(P\Gamma, \mathcal{A}[p]) = 0$. Since S has dimension $t < n$, then by using induction, we deduce $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$.

Assume that S is an exceptional group of Lie type. By [10] (see in particular Table (4.5) at page 186) and [11] (see in particular Table (4.3) at page 193), the cohomology group $H^1(S, \mathcal{A}[p])$ is trivial, for all $p > 3$, when n is the possible minimal degree of the representation of S and when n is the dimension of the Lie algebra with automorphism group S (in this case S has a natural representation in dimension n and this often coincides with the representation of S with minimal degree). If the representation of S is neither the minimal nor the natural one, then we can proceed as follows. We first consider the groups S that are not twisted. Let $L(\lambda)$ denote the irreducible G-module of highest weight λ. In [45, Thm 1.2.3] the authors prove that for all $p > 31$ the first cohomology group $H^1(S, L(\lambda))$ is trivial, when λ is a fundamental dominant weight (or it is less

than a fundamental dominant weight) and S is not a twisted group. In 1950 Chevalley proved that whenever M is an irreducible S-module, then $M = L(\lambda)$, for some dominant weight λ (see [22] and [7]). In particular, since we are assuming that $\mathcal{A}[p]$ is irreducible, then $\mathcal{A}[p] = L(\lambda)$, for some dominant weight λ. In addition, every dominant weight is a positive integer linear combination of fundamental dominant weights and it is well-known in the theory of Lie groups that this implies a decomposition $L(\lambda) = \otimes_{i=1}^{s} L(\omega_i)$, where s is a positive integer and ω_i is a fundamental weight, for every $1 \leq i \leq s$. Thus $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) \simeq H^1_{\mathrm{loc}}(S, \otimes_{i=1}^{s} L(\omega_i))$, for certain fundamental weights ω_i and the group S preserves a tensor product decomposition. In particular S acts on $\mathcal{A}[p]$ in the same way as the subgroups of class $\mathcal{C}_4$ or $\mathcal{C}_7$ (see [28, §4.4]). Since the mentioned Theorem 1.2.3 in [45] assures the triviality of $H^1(S, L(\omega_i))$, for all $1 \leq i \leq s$, we can use the arguments given for groups of class $\mathcal{C}_4$ or $\mathcal{C}_7$ to deduce the triviality of $H^1_{\mathrm{loc}}(S, \mathcal{A}[p])$. Observe that when $n \geq 31$, we have that $p \geq n+1$ implies $p > 31$. Thus we may apply Theorem 1.2.3 in [45] for all exceptional groups and get $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$, with the other arguments as above. If $n < 31$, then every representation of an exceptional group of degree n is either minimal or fundamental (or both), except the representation of the group $G_2(q)$ of degree 27. But for groups of type $G_2(q)$ the conclusion of the mentioned Theorem 1.2.3 in [45] holds for all $p > 3$. So, again we may apply all the arguments as above to get $H^1_{\mathrm{loc}}(S, \mathcal{A}[p]) = 0$. We have to prove the same conclusion for twisted groups of lie type. If we assume that $p > 3$, then we have neither Suzuki groups nor Ree groups in the defining characteristic (see [48] for further details). We are left with groups ${}^2E_6(q)$ and ${}^3D_4(q)$. The group ${}^2E_6(q)$ is a subgroup of $E_6(q^2)$ modulo scalars (see [48, 4.11]). We may apply Shapiro's Lemma (see for instance [33, Theorem 4.19] or [46, Lemma 6.3.2 and Lemma 6.3.4]) to get

$$H^1\left(E_6(q^2), \mathrm{Ind}_{{}^2E_6(q)}^{E_6(q^2)} \mathcal{A}[p]\right) \simeq H^1({}^2E_6(q), \mathcal{A}[p]),$$

where $\mathrm{Ind}_{{}^2E_6(q)}^{E_6(q^2)}$ denotes the induced G-module $\bigoplus_i^s \sigma_i(\mathcal{A}[p])$, where σ_i varies in a system of left coset representatives of H in G, $s := [E_6(q^2) :^2 E_6(q)]$ denotes the index of ${}^2E_6(q)$ in $E_6(q^2)$ (see [33, Definition 4.18]) and $\sigma_i(\mathcal{A}[p])$ is isomorphic to $\mathcal{A}[p]$. Being $H^1(G, -)$ and additive functor for every group G, we have

$$\bigoplus_{i=1}^{s} H^1(E_6(q^2), \sigma_i(\mathcal{A}[p])) \simeq H^1({}^2E_6(q), \mathcal{A}[p]).$$

We have already proved that $H^1_{\mathrm{loc}}(E_6(q^2), \mathcal{A}[p]) = 0$, under the assumption that $\mathcal{A}[p]$ is

irreducible. Therefore $H^1_{\mathrm{loc}}(E_6(q^2), \sigma_i(\mathcal{A}[p])) = 0$, for all i, and $H^1_{\mathrm{loc}}({}^2E_6(q), \mathcal{A}[p]) = 0$. The group ${}^3D_4(q)$ is a subgroup of $\Omega_8^+(q^3)$. The cited results in [10] and in [45] hold for $\Omega_8^+(q^3)$ (but they do not hold in general for symplectic groups). Then we may apply all the arguments as above to get $H^1_{\mathrm{loc}}(\Omega_8^+(q^3), \mathcal{A}[p]) = 0$ and deduce $H^1_{\mathrm{loc}}({}^3D_4(q), \mathcal{A}[p]) = 0$, by Shapiro's Lemma.

To finish the proof we have to control that $p \geq n/2 + 1$ is a sufficient bound for the subgroups of class $\mathcal{C}_9$ of $\mathrm{SL}_n(q)$, when $4 \leq n \leq 250$.

Part iii. The cases when $4 \leq n \leq 250$

In accordance with part *i.*, the bound $p \geq n/2 + 1$ is sufficient, whenever G is a subgroup of class $\mathcal{C}_i$, with $1 \leq i \leq 8$. To show that the same bound works even when G is a subgroup of class $\mathcal{C}_9$, we are going to control case by case what happens for such groups when $4 \leq n \leq 250$.

$n = 4$

Let $d := \gcd(q - 1, 4)$. By the classification of the maximal subgroups of $\mathrm{SL}_4(q)$ appearing in [3, Table 8.9, pag. 381], we have the following maximal subgroups of class $\mathcal{C}_9$.

(a) the group A_7, only if $q = p = 2$;

(b) the group $C_d \circ C_2 \cdot \mathrm{PSL}_2(7)$, for $q = p \equiv 1, 2, 4 \pmod 7$, $p \neq 2$;

(c) the group $C_d \circ C_2 \cdot A_7$, for $q = p \equiv 1, 2, 4 \pmod 7$, $p \neq 2$;

(d) the group $C_d \circ C_2 \cdot \mathrm{U}_4(2)$, for $q = p \equiv 1 \pmod 6$.

In cases **(b)**, **(c)** and **(d)** the p-Sylow subgroups of G is either trivial or cyclic for all p (observe that those cases occur only for certain primes). In case **a)** the p-Sylow subgroup of G is either trivial or cyclic, for all $p \geq 3$. Then we get the conclusion.

$n = 5$

Let $d := \gcd(q - 1, 5)$. We have to prove $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 3$. Since this bound is sufficient to have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, when G is of class $\mathcal{C}_i$, for $i \neq 9$,

we have to consider only the subgroups of of $\mathrm{SL}_5(q)$ of class $\mathcal{C}_9$, i. e. the ones appearing in the following list (see [3, Table 8.19, pag. 386])

(a) the group $\mathrm{PSL}_2(11) \times C_d$ if $q = p \equiv 1, 3, 4, 5, 9 \pmod{11}$;

(b) the group $U_4(2) \times C_d$, if $p \equiv 1 \pmod 6$, for $q = p \equiv 1 \pmod 6$;

(c) the Mathieu group M_{11} if $q = 3$.

Assume that we are in case **(a)** and G is isomorphic to a subgroup of $\mathrm{PSL}_2(11) \times C_d$. Then the cardinality of G divides $2^3 \cdot 3 \cdot 5 \cdot 11 \cdot d$ and its p-Sylow subgroup is either trivial or cyclic, for every $p \geq 3$. Assume that we are in case **(b)**. The group $U_4(2)$ has order $2^6 \cdot 3^5 \cdot 5$. Since this case does not occur if $q \in \{2, 3\}$, then, for every $p \geq 2$, the p-Sylow subgroup of G is either trivial or cyclic again. Therefore $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. Assume that we are in case **(c)**. This case may happen only if $q = 3$. The Mathieu group M_{11} has cardinality $2^4 \cdot 3^2 \cdot 5 \cdot 11$. In this last case, for every $p \geq 5$, the p-Sylow subgroup of G is either trivial or cyclic. So we have the bound $p > 3$ appearing in the statement of Theorem 1.3.

$n = 6$

We have to prove $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p > 3$. Let $d := \gcd(q - 1, 6)$. The maximal subgroups of $\mathrm{SL}_6(q)$ of class $\mathcal{C}_9$ are the ones appearing in the following list (see [3, Table 8.25, pag. 389])

(a) a group of type $\mathcal{C}_9$, the group $C_2 \times C_3^{\cdot} A_6.C_2$;

(b) a group of type $\mathcal{C}_9$, the group $C_2 \times C_3^{\cdot} A_6$;

(c) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} A_6$;

(d) a group of type $\mathcal{C}_9$, the group $C_d \circ C_2^{\cdot} \mathrm{PSL}_2(11)$;

(e) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} A_7$;

(f) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} \mathrm{PSL}_3(4)^{\cdot} C_2$;

(g) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} \mathrm{PSL}_3(4)$;

(h) a group of type $\mathcal{C}_9$, the group $C_2^{\cdot} M_{12}$;

(i) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} \mathrm{U}_4(3)^{\cdot} C_2$;

(l) a group of type $\mathcal{C}_9$, the group $C_6^{\cdot} \mathrm{U}_4(3)$;

(m) a group of type $\mathcal{C}_9$, the group $C_d \circ \mathrm{SL}_3(q)$.

Some of the cases in the list can occur only under certain conditions of q. Since the proof does not depend on those conditions, we avoided to write them, to ease the notation.

One easily verifies that in cases **(a)**, **(b)**, **(c)**, **(e)**, **(f)**, **(g)**, **(h)**, **(i)** and **(l)**, the p-Sylow subgroup of G is either trivial or cyclic, for all $p > 3$. Thus $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for every $p \geq 5$. Assume that we are in case **(d)**. If $p > 5$, then the p-Sylow subgroup of G is either trivial or cyclic too. If $p = 5$, then the p-Sylow subgroup of G is either trivial, or cyclic or isomorphic to the p-Sylow subgroup of $\mathrm{SL}_2(11)$. By Lemma 3.6, we get $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$ in this last case too. Assume that we are in case **(m)**. If $p \geq 5$, then the p-Sylow subgroup of G is isomorphic to a subgroup of $\mathrm{SL}_3(q)$. By the assumption that $\mathcal{A}[p]$ is very a strongly irreducible G-module and the results achieved in Section 3.2 for $n = 3$, we have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$. In the end $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 5$.

$n = 7$

Let $d := \gcd(q - 1, 7)$. The only maximal subgroup of $\mathrm{SL}_7(q)$ of class $\mathcal{C}_9$ is the group $C_d \times U_3(3)$, with cardinality $2^7 \cdot 3^3 \cdot 7 \cdot d$ (see [3, Table 8.36, pag. 395]). Observe that $d|7$ and when $p = 7$, in particular $d \neq 7$. Therefore, for all $p \geq 5$, the p-Sylow subgroup of G is either trivial or cyclic. Thus if G is a subgroup of $\mathrm{SL}_7(q)$ and $\mathcal{A}[p]$ is a very strongly irreducible G-module, then $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 5$.

$n = 8$

Let $d := \gcd(q - 1, 8)$. As above, we have to consider only the subgroups of $\mathrm{SL}_8(q)$ of class $\mathcal{C}_9$, i. e. the groups appearing in the following list (see [3, Table 8.45, pag. 399])

(a) the group $C_4 . \mathrm{PSL}_3(4)$;

(b) the group $C_d \circ C_4 . \mathrm{PSL}_3(4)$;

(c) the group $C_d \circ C_4 . \mathrm{PSL}_3(4).C_2$.

Again, some of the cases in the list can happen only under certain conditions on q. Since the proof does not depend on those condition, as above we avoid to write them, to ease the notation. One sees that the cardinality of every maximal subgroup

of $\mathrm{SL}_8(q)$ of class $\mathcal{C}_9$ divides $2^6 \cdot |\mathrm{SL}_2(4)| = 2^{12} \cdot 3 \cdot 5 \cdot 63$. Then, for every $p \geq 3$, the p-Sylow subgroup of all of those groups is either trivial or cyclic, implying the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$.

$n = 9$

Let $d := \gcd(q-1, 9)$. The maximal subgroups of $\mathrm{SL}_9(q)$ of class $\mathcal{C}_9$ are (see [3, Table 8.55, pag. 406])

(a) $C_3^{\cdot} A_7$, for $q = p$;

(b) $C_d \times \mathrm{PSL}_2(19)$, for $q = p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$;

(c) $\mathrm{PSL}_3(q^2).C_2$, for $q \equiv 0 \pmod 3$;

(d) $\mathrm{PSL}_3(q^2).S_3$, for $q \equiv 2 \pmod 3$;

(e) $C_9 \circ \mathrm{SL}_3(q^2).2$, for $q \equiv 1 \pmod 9$;

(f) $\mathrm{SL}_3(q^2).C_6$, for $q \equiv 4, 7 \pmod 9$.

For all $p \geq 5$, the groups in cases **(a)** and **(b)** have a p-Sylow subgroup that is either trivial or cyclic. In cases **(a)**, **(b)** **(c)**, **(d)**, **(e)** and **(f)** for all $p \geq 5$, the p-Sylow subgroup of G is isomorphic to a subgroup of $\mathrm{SL}_3(q^2)$. We use induction to get $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$.

$n = 10$

We have to prove $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 7$, when G is a subgroup of SL_{10} contained in one of its maximal subgroup of class $\mathcal{C}_9$. Let $d := \gcd(q-1, 10)$, $h := \gcd(q-1, 3)$ and $s := \frac{\gcd(q-1,4)}{2}$. The maximal subgroups of $\mathrm{SL}_{10}(q)$ of class $\mathcal{C}_9$ are (see [3, Table 8.61, pag. 410])

(a) $C_d \circ C_2^{\cdot} \mathrm{PSL}_2(19)$, for $q = p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$;

(b) $C_d \circ C_2^{\cdot} \mathrm{PSL}_3(4)$, for $q = p \equiv 11, 15, 23 \pmod{28}$;

(c) $C_d \circ C_2^{\cdot} \mathrm{PSL}_3(4).C_2$ (where C_2 is a specific quotient of $\mathrm{SL}_3(4)$), for $q = p \equiv 3, 9, 25 \pmod{28}$;

(d) $C_d \circ C_2^{\cdot} M_{12}$ (where M_{12} is the Mathieu group of order $2^6 \cdot 3^3 \cdot 5 \cdot 11$), for $q = p \equiv 3 \pmod 8$;

(e) $C_d \circ C_2^{\cdot} M_{12}.C_2$, for $q = p \equiv 1 \pmod 8$;

(f) $C_d \circ C_2^{\cdot} M_{22}$ (where M_{22} is the Mathieu group of order $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$), for $q = p \equiv 11, 15, 23 \pmod{28}$;

(g) $C_d \circ C_2^{\cdot} M_{22}.C_2$, for $q = p \equiv 1, 9, 25 \pmod{28}$;

(h) $C_d \times \mathrm{PSL}_3(q).C_h$, for $p \geq 5$;

(i) $C_d \circ C_s^{\cdot} \mathrm{PSL}_4(q).C_s$, for $p \geq 3$;

(j) $C_d \circ \mathrm{SL}_5(q)$.

Observe that $d|10$, but $d \neq 5$, when $p = 5$. Then, in cases **(a)**, **(b)**, **(c)**, **(d)**, **(e)**, **(f)** and **(g)**, for all $p \geq 5$, the p-Sylow subgroup G_p of G is isomorphic to a subgroup of one of the groups $\mathrm{SL}_2(19)$, $\mathrm{SL}_3(4)$, M_{12} and M_{22}. Thus G_p is either trivial or cyclic. We have $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$ in all those cases. For cases **(h)**, **(i)**, **(j)** we use induction and similar techniques as above.

$n = 11$

As for $n = 10$, it suffices to prove $H^1_{\mathrm{loc}}(G, \mathcal{A}[p]) = 0$, for all $p \geq 7$, when G is a subgroup of a maximal subgroup of $\mathrm{SL}_{11}(q)$ of class $\mathcal{C}_9$. Let $d := \gcd(q - 1, 11)$. The maximal subgroups of $\mathrm{SL}_{11}(q)$ of class $\mathcal{C}_9$ are (see [3, Table 8.71, pag. 418])

(a) $\mathrm{PSL}_2(23)$, for $q = 2$;

(b) $C_d \times \mathrm{PSL}_2(23)$, for $q = p \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \pmod{23}, q \neq 2$;

(c) $C_d \times U_5(2)$, for $q = p \equiv 1 \pmod{3}$;

(d) the mathieu group M_{24}, for $q = 2$.

Recall that the Mathieu group M_{24} has order $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ (moreover this case happens only for $q = 2$). Furthermore, we have $|\mathrm{SL}_2(23)| = 2^4 \cdot 3 \cdot 11 \cdot 23$ and $|U_5(2)| = 2^{10} \cdot 3^6 \cdot 5 \cdot 11$. Then, for all $p \geq 5$, the p-Sylow subgroup of G is either trivial or cyclic in all cases.

$n = 12$

Let $d := \gcd(q - 1, 12)$ and let Suz denote the Suzuki group of order $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$. As above it suffices to consider the maximal subgroups of $\mathrm{SL}_{12}(q)$ of class $\mathcal{C}_9$, listed below (see [3, Table 8.77, pag. 422])

(a) $C_d \circ C_6^{\cdot} A_6$, for $q = p \equiv 1, 4 \pmod{15}$;

(b) $C_{12} \circ C_6^{\cdot} A_6$, for $q = p^2$, $p \equiv 2, 3 \pmod 5$, $p \neq 2, 3$;

(c) $C_d \circ C_2^{\cdot} \mathrm{PSL}_2(23)$, for $q = p \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \pmod{23}$, $p \neq 2$;

(d) $C_{12}^{\cdot} \mathrm{PSL}_2(4)$ (where C_{12} is a specific subgroup of $\mathrm{SL}_2(23)$ of order 12), for $q = 49$;

(e) $C_d \circ C_6^{\cdot} \mathrm{Suz}$, for $q = p \equiv 1 \pmod 3$.

Assume that G is a subgroup of one of the groups appearing in the list.

If $p > 5$, then the p-Sylow subgroup of G is either trivial or cyclic in all cases **(a)**, **(b)**, **(c)**, **(d)** and **(e)**.

Therefore $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ is trivial, for all $p \geq 7$.

$13 \leq n \leq 250$

In [23], the authors list all the possible subgroups of class $\mathcal{C}_9$ of $\mathrm{SL}_n(q)$, for every $n \leq 250$, excluding the groups of Lie type in their defining characteristic (see also [24]). By part *i.* and part *ii.*, the bound $p \geq n/2 + 1$ works for all groups except some sporadic groups (only for $13 \leq n \leq 26$) and the groups of Lie type in cross characteristic. Proceeding as for $n \leq 12$, by analyzing the tables in [23], one sees that even when $13 \leq n \leq 250$ the first local cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p])$ is trivial for all $p \geq n/2 + 1$, for these two classes of groups. □

About the bounds for p we can make the following considerations.

Remark 3.11. A likely sharp bound. Looking at the proofs for $n \in \{2, 3\}$ and $4 \leq n \leq 250$, one sees that the bound $p \geq n/2 + 1$ is probably sharp in many cases. In fact, for $p \leq n/2$, the p-Sylow subgroup of G could be a direct product of two cyclic groups C_p (look for examples at the 3-Sylow subgroup of M_{11} when $n = 5$, or at the Klein group contained in the 2-Sylow subgroup of A_7, when $n = 4$, and so on). When the p-Sylow subgroup G_p of G is isomorphic to C_p^2, the local-global divisibility may fail as in the mentioned examples produced in [15], [17] and in [35], [36], [37]. One can rise those examples to similar ones for all n. So the local-global principle for divisibility by p could fail for $p \leq n/2$, when $G_p \simeq C_p^2$. Anyway for some n, as for $n = 8$ or $n = 10$, the bound $p \geq n/2 + 1$ is obviously not sharp. In those cases G_p is trivial or cyclic even for some $p \leq n/2$. We will now replace the bound $n/2 + 1$ with a bound p_n, that still depends only on n and that is probably sharp, for all n (see also Remark 3.13 below). In fact,

if $\hat{p}$ is the greatest prime $< p_n$, then the $\hat{p}$-Sylow subgroup of G can be isomorphic to $C_{\hat{p}}^2$ and the local-global principle for divisibility by $\hat{p}$ can fail. We cannot prove that the bound p_n is really sharp, only because we cannot prove that there exists a commutative algebraic group $\mathcal{A}$ with a prescribed $\hat{p}$-torsion subgroup $\mathcal{A}[\hat{p}]$ such that $G_{\hat{p}}$ is exactly a group for which the principle fails. We can only prove that for $p = \hat{p}$ the group $G_{\hat{p}}$ *could* be isomorphic to $C_{\hat{p}}^2$ and that this surely does not happen when $p \geq p_n$. By eventually changing the field of definition k, it is likely that we can have $G_{\hat{p}} \simeq C_{\hat{p}}^2$. This still does not assure that $H^1_{\mathrm{loc}}(G_{\hat{p}}, \mathcal{A}[\hat{p}]) = 0$. But among so many commutative algebraic groups $\mathcal{A}$ and number fields k, for each n, we expect that this happens for at least one of them, as in the case when $n = 2$ for elliptic curves. We are going to give a new version of Theorem 1.3 with such a bound p_n.

For every n, let ρ_n be the smallest prime such that, for all $p \geq \rho_n$ the square p^2 divides no cardinalities of the maximal subgroups of class $\mathcal{C}_9$ of $\mathrm{GL}_n(q)$. In addition, when $n = r^t$, for some prime r and some positive integer t, let $\mathfrak{p}_n$ be the smallest prime such that for all $p \geq \mathfrak{p}_n$, the square p^2 does not divide $\prod_{i=1}^{t}(r^{2i} - 1)$. Observe that p^2 divides no cardinalities of the subgroups of class $\mathcal{C}_6$ of $\mathrm{GL}_n(q)$. If n is not a power of a prime, there are no subgroups of class $\mathcal{C}_6$ in $\mathrm{GL}_n(q)$, so set $\mathfrak{p}_n = 1$ in that case. It is then clear from the proof of Theorem 3.1, that we can give a new version of Theorem 1.3 as follows.

Theorem 3.12. *Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, with $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. For every n, there exists a prime p_n, depending only on n, such that if $p \geq p_n$ and $\mathcal{A}[p]$ is a very strongly irreducible G_k-module or a direct sum of very strongly irreducible G_k-modules, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p]) = 0$. Moreover $p_n = \max\{p_d, \mathfrak{p}_n, \rho_n\}$, where d is the greatest divisor of n.*

Remark 3.13. In addition, it is probable that $p \geq n/2 + 1$ is a proper bound for every $n > 250$ too. In fact it does work for all groups except certain groups of Lie type in cross characteristic and certain alternating groups that can never occur for some prime numbers (or that can never occur at all). Anyway we can only conjecture this fact, since, as stated above, we do not know the classification of the subgroups of $\mathrm{GL}_n(q)$ of class $\mathcal{C}_9$, for $n > 250$.

We now proceed with the proofs of the corollaries stated in the introduction, that can be quickly deduced from the proof of Theorem 3.1.

Proof of Corollary 1.4 By the proof of Theorem 1.3 part *i.*, concerning subgroups of class $\mathcal{C}_6$, one easily deduces that for $p \geq n/2+1$, the p-Sylow subgroup G_p of G is trivial. Thus $H^1(G_p, \mathcal{A}[p]) = 0$. It is well-known that the restriction map

$$H^1(G, \mathcal{A}[p]) \to H^1(G_p, \mathcal{A}[p])$$

is injective on the p-primary part of $H^1(G, \mathcal{A}[p])$ (see for example [44, Thm 4, Chap. IX, §2]). Since $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$ is a p-group, the p-primary part of $H^1(G, \mathcal{A}[p])$ is the whole group. Then $H^1(G_p, \mathcal{A}[p]) = 0$ implies $H^1(G, \mathcal{A}[p]) = 0$. □

Proof of Corollary 1.5 By the proof of Theorem 1.3 part *ii.*, one can easily deduce that if $p > 2n+2$, then the p-Sylow subgroup G_p of G is trivial. Thus $H^1(G_p, \mathcal{A}[p]) = 0$. As in the proof of Corollary 1.4, this implies $H^1(G, \mathcal{A}[p]) = 0$. □

Remark 3.14. In the same way as Corollary 1.5 and Corollary 1.4 one sees that

a) if $p > n+2$ and the absolute Galois group G_k acts on $\mathcal{A}[p]$ as a subgroup of an alternating group, then $H^1(G, \mathcal{A}[p]) = 0$.

b) if $p > 13$ and the absolute Galois group G_k acts on $\mathcal{A}[p]$ as a subgroup of a sporadic group, then $H^1(G, \mathcal{A}[p]) = 0$.

Acknowledgments. I am grateful to John van Bon, Gabriele Ranieri and Jacob Stix for useful discussions. I wrote a part of this paper at the Max Planck Institute for Mathematics in Bonn. I would like to warmly thank all people there for their kind hospitality. I am also grateful to Istituto Nazionale di Alta Matematica "F. Saveri" that partially supported this research with grant "Assegno di ricerca Ing. Giorgio Schirillo".

References

[1] Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math., **76** (1984), 469-514.

[2] Bašmakov M. I., *The cohomology of abelian varieties over a number field*, Russian Math. Surveys., **27** (1972) (English Translation), 25-70.

[3] Bray J. N., Holt D. F., Roney-Dougal C. M., *The maximal subgroups of the low-dimensional finite classical groups*, Cambridge University Press, Cambridge, 2013.

[4] Brauer R., *On finite projective groups*, 63-82, in [*Contributions to Algebra: A Collection of Papers Dedicated to Ellis Kolchin* edited by Bass H., Cassidy P. J., Kovacic J., Academic Press, New York, 1977].

[5] Cassels J. W. S., *Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups.*, Proc. London Math. Soc., **12** (1962), 259-296.

[6] Cassels J. W. S., *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung.*, J. reine angew. Math. **211** (1962), 95-112.

[7] Chevalley C., *Le poids dominants*, Séminaire Claude Chevalley, Tome 2 (1956-58), exp. no. 19.

[8] Chevalley C., Einberg S., *Cohomology theory of Lie groups and Lie algebras*, Trans. Amer. Math. Soc. **63** (1948), 85-124.

[9] Çiperiani M., Stix J., *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels.*, J. Reine Angew. Math., **700** (2015), 175-207.

[10] Cline E., Parshall B., Scott L.,*Cohomology of finite groups of Lie type, I*, Inst. Hautes ÃĽtudes Sci. Publ. Math., **45** (1975), 169-191.

[11] Cline E., Parshall B., Scott L.,*Cohomology of finite groups of Lie type, II*, J. Algebra **45** no. 1 (1977), 182-198.

[12] Creutz B., *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. London Math. Soc., **45** (2013), 935-942.

[13] Creutz B., *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett., **23** no. 2 (2016), 377-387.

[14] Dvornicich R., Paladino L., *Local-global questions for divisibility in commutative algebraic groups*, arXiv:1706.03726

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

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

[17] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., **39** (2007), 27-34.

[18] Gillibert F., Ranieri G., *On the local-global divisibility of torsion points on elliptic curves and* GL_2*-type varieties*, J. Number Theory, **174** (2017), 202-220.

[19] Gillibert F., Ranieri G., *On the local-global divisibility over abelian varieties*, Annales de l'Institut Fourier, **68** no. 2 (2018), 847-873.

[20] Gillibert F., Ranieri G., *On the local-global divisibility over* GL_2*-type varieties* https://arxiv.org/pdf/1703.06235.pdf

[21] Illengo M., *Cohomology of integer matrices and local-global divisibility on the torus*, Le Journal de Théorie des Nombres de Bordeaux, **20** (2008), 327-334.

[22] Hiss G., *Finite groups of Lie type and their representations* in: C. M. Campbell, M. R. Quick, E. F. Robertson, C. M. Roney-Dougal, G. C. Smith and G. Traustason (Eds.), Groups St Andrews 2009 in Bath, Cambridge University Press, Cambridge, 2011, pp. 1-40.

[23] Hiss G., Malle G., *Low-dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **4** (2001), 22-63.

[24] Hiss G., Malle G., *Corrigenda: L̈ow-dimensional representations of quasi-simple groups¨*, Corrigenda: "Low-dimensional representations of quasi-simple groups" [LMS J. Comput. Math. 4 (2001), 22âĂŞ63; MR1835851]. LMS J. Comput. Math. 5 (2002), 95-126.

[25] Hoffman C., *Cross characteristic projective representations of the finite Chevalley groups*, Journal of Algebra, **229** (2000), 666-677.

[26] Jacobson N. *Lie algebras*, Dover Publications, New York, 1979.

[27] Katz N. M., *Galois Properties on Torsion Points on Abelian Varieties*, Invent. math., **62** (191981), 481-502.

[28] Kleidman P. B., Liebeck M. W., *The subgroups structure of the finite classical groups*, London Math. Soc. Lecture Note Ser., 129, Cambridge University Press, Cambridge, 1990.

[29] Kneser M., *Lectures on Galois cohomology of classical groups*, Tata Institute of Fundamental Research, Bombay 1969.

[30] Lang S., *Elliptic curves: diophantine analysis*, Grundlehren der Mathemathischen Wissenschaften 231, Springer, Heidelberg, 1978.

[31] Landazuri V., *On the minimal degree of projective representations of the finite Chevalley groups*, Journal of Algebra, **32** (1974), 418-443.

[32] Milne J. S., *Abelian Varieties*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, 103-150.

[33] Neukirch J., *Class Field Theory-The Bonn Lectures- Edited by Alexander Schmidt*, Springer, Heidelberg, 2013.

[34] Nori M. V., *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$, Invent. Math., **88** (1987), 257-275.

[35] Paladino L., *Local-global divisibility by* 4 *in elliptic curves defined over* $\mathbb{Q}$, Annali di Matematica Pura e Applicata, **189** no. 1, (2010), 17-23.

[36] Paladino L., *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9*, Le Journal de Théorie des Nombres de Bordeaux, Vol. **22**, n. 1 (2010), 138-160.

[37] Paladino L., *On counterexamples to local-global divisibility in commutative algebraic groups*, Acta Arithmetica, **148** no. 1, (2011), 21-29.

[38] Paladino L., Ranieri G., Viada E., *Local-global divisibility by* p^2 *in elliptic curves*, Preprint, 2011, arXiv:1103.4963.

[39] Paladino L., Ranieri G., Viada E., *On Local-Global Divisibility by* p^n *in elliptic curves*, Bulletin of the London Mathematical Society, **44** no. 5 (2012), 789-802.

[40] Paladino L., Ranieri G., Viada E., *On minimal set for counterexamples to the local-global principle*, Journal of Algebra, **415** (2014), 290-304.

[41] Ranieri G., *Counterexamples to the local-global divisibility over elliptic curves*, Annali di Matematica Pura e Applicata, DOI:10.1007/s10231-017-0721-9 (2017), 1-11.

[42] Sansuc J.-J., *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. (French) [The Brauer group and arithmetic of linear algebraic groups on a number field]*, J. Reine Angew. Math. , **327** (1981), 12-80.

[43] Serre J-P., *Algebraic groups and class fields*, Springer-Verlag, Heidelberg, 1988.

[44] Serre J.-P., *Local fields*, Springer-Verlag, New York, 1971.

[45] University of Georgia Vigre Algebra Group, *First cohomology for finite groups of lie type: Simple modules with small dominant weights*, Transactions of the American Mathematical Society **365** no. 2, 1025-1050

[46] Weibel C. A., *An introduction to homological algebra*, Cambridge University Press, Cambridge, 2008.

[47] Whitehead J. H. C., *Combinatorial homotopy. II.* Bull. Amer. Math. Soc. **55** (1949), no. 5, 453-496.

[48] Wilson R. A., *The finite simple groups*, Springer-Verlag, Heidelberg, 2009.

[49] Wong S., *Power residues on abelian variety*, Manuscripta Math., no. **102** (2000), 129-137.

Laura Paladino

University of Calabria
Ponte Bucci, Cubo 30B
87036 Arcavacata di Rende
Italy
e-mail address: paladino@mat.unical.it