Cohomology of groups acting on vector spaces over finite fields

Davide Lombardo and Laura Paladino

Abstract

Let \( \mathbb{F}_q \) be the finite field with \( q = p^m \) elements and \( G \) be a subgroup of \( \text{GL}_n(\mathbb{F}_q) \). A famous theorem of Nori published in 1987 states that there exists a (non-effective) constant \( c(n) \), depending only on \( n \), such that if \( p > c(n) \) and \( G \) acts semisimply on \( \mathbb{F}_p^n \), then \( H^1(G, \mathbb{F}_p^n) = 0 \). We solve the long-standing problem, also considered by Serre, of giving an effective proof of Nori’s theorem. Our approach yields the optimal constant \( c(n) = n + 2 \). We also prove a more general version of Nori’s theorem, namely, that for all powers \( q \) of \( p \), if \( G \) acts semisimply on \( \mathbb{F}_q^n \) and \( p > n + 2 \), then \( H^1(G, \mathbb{F}_q^n) \) is trivial. We apply these results to refine a criterion, proved by Çiperiani and Stix, which gives sufficient conditions for an affirmative answer to a classical question posed by Cassels in the case of abelian varieties over number fields.

1 Introduction

In the study of group actions, the first cohomology group is an object of fundamental importance, and much work has been devoted to understanding \( H^1(G, M) \) for general groups \( G \) and \( G \)-modules \( M \). Of particular interest are criteria guaranteeing the vanishing of \( H^1(G, M) \), of which there are several: for example, \( H^1(G, M) \) is known to be trivial when \( G \) is a group of Lie type and \( M \) is a minimal irreducible \( G \)-module \([6, 7]\) or \( M = L(\lambda) \) is an irreducible \( G \)-module of highest weight \( \lambda \) \([20]\). Let \( \mathbb{F}_q \) be the finite field with \( q = p^m \) elements, where \( p \) is a prime number and \( m \) is a positive integer, and let \( G \) be a subgroup of \( \text{GL}_n(\mathbb{F}_q) \), for some positive integer \( n \). In this work we are concerned with the vanishing of \( H^1(G, V) \) for the natural \( G \)-module \( V = \mathbb{F}_q^n \), under the assumption that the action of \( G \) on \( V \) is semisimple. A deep theorem of Nori \([16, \text{Theorem E, page 271}]\) gives the following sufficient conditions for the triviality of \( H^1(G, \mathbb{F}_q^n) \), when \( q = p \).

**Theorem 1.1** (Nori, 1987). Let \( p \) be a prime number and let \( n \) be a positive integer. Let \( G \) be a subgroup of \( \text{GL}_n(\mathbb{F}_p) \) acting semisimply on \( \mathbb{F}_p^n \). There exists a constant \( c(n) \), depending only on \( n \), such that if \( p > c(n) \), then

\[
H^1(G, \mathbb{F}_p^n) = 0.
\]
In his letter to Marie-France Vignéras in 1986, Serre gives an alternative proof of Nori’s theorem and mentions the problem of finding an explicit $c(n)$ (see [19]). He also states that he has no conjectures about the possible value of $c(n)$, as well as no examples [19, Remark 2, pag. 42]. There are no results in the literature which give an explicit $c(n)$ for all $G$. Only for groups $G$ containing no nontrivial normal $p$-subgroup, Guralnick [12] proved in 1999 that one can take $c(n) = n + 2$. Here we answer Serre’s question by showing that one can take $c(n) = n + 2$ for every $n$ and $G$. In addition, we prove more generally that Nori’s theorem can be extended (with the same optimal constant $c(n) = n + 2$) to subgroups $G \leq \text{GL}_n(\mathbb{F}_q)$ acting semisimply on $\mathbb{F}_q^n$, where $q$ is now allowed to be any power of $p$.

**Theorem 1.2.** Let $p$ be a prime number and let $m, n$ be positive integers. Let $G$ be a subgroup of $\text{GL}_n(\mathbb{F}_q)$ acting semisimply on $\mathbb{F}_q^n$, where $q = p^m$. If $p > n + 2$, then

$$H^1(G, \mathbb{F}_q^n) = 0.$$ 

The constant $c(n) = n + 2$ is sharp, since there are counterexamples for $p \leq n + 2$. The simplest counterexamples can be obtained from the alternating groups $A_p$, with $p \geq 5$, in dimension $n = p − 2$. Let $U = \{(x_1, \ldots, x_p) \in \mathbb{F}_p^p : \sum_{i=1}^p x_i = 0\}$ and $W = \{(x, \ldots, x) \in \mathbb{F}_p^p : x \in \mathbb{F}_p\} \subset U$. Clearly, $W \cong \mathbb{F}_p$ is a trivial 1-dimensional $A_p$-module, while, by [13, p. 186], $U/W$ is a simple $A_p$-module of dimension $p − 2$. Using [13 Lemma 5.3.4], one checks immediately that the sequence

$$\{0\} \to W \to U \to U/W \to \{0\}$$

does not split, which proves $H^1(A_p, U/W) \neq (0)$. Further counterexamples with $n = p − 2$ are given by certain projective special linear groups $\text{PSL}_r(w)$, where $w = r^\alpha$ is a power of a prime $r \neq p$ and $p$ equals $\frac{w-1}{w-1}$ (see the introduction to [12]).

The techniques we use to prove Theorem 1.2 are different from those employed by Nori. As a first step, we use the aforementioned result of Guralnick [12] to handle the special case when $V = \mathbb{F}_q^n$ is an irreducible $G$-module (see Proposition 3.1 for a slightly more general statement). As $V$ is assumed to be a semisimple $G$-module, we can write $V = \bigoplus_{i=1}^k V_i$, where each $V_i$ is an irreducible $G$-submodule of $V$. Since cohomology commutes with finite direct sums, we have $H^1(G, V) = \bigoplus_{i=1}^k H^1(G, V_i)$, where each $V_i$ is a simple $G$-module. However, the $V_i$ need not be faithful $G$-modules, hence we cannot simply apply the result for simple modules to every $H^1(G, V_i)$. We
circumvent this difficulty by a careful study of the kernels \(N_i\) of the natural projections \(\text{GL}(V) \to \text{GL}(\bigoplus_{j \neq i} V_j)\) and of their cohomology. Combined with a double induction (on \(|G|\) and on \(k\), the number of irreducible components of \(V\)), this leads to a proof of our main theorem.

The triviality of cohomology groups also has applications beyond group theory. As a first immediate consequence, in Section 4 we use Theorem 1.2 to obtain structural information about the semisimple subgroups of \(\text{GL}_n(F_q)\) when \(p > n + 3\) (see Corollary 4.1). In the same section we also make a remark about the vanishing of \(H^1\) for groups that decompose nontrivially as a tensor product (Proposition 4.2). This gives a further criterion for the vanishing of \(H^1\) which can be useful in itself, and shows that the constant in Theorem 1.2 though sharp in general, can be greatly improved if one restricts to special classes of subgroups of \(\text{GL}_n(F_q)\).

The vanishing of cohomology groups also finds applications in number theory, for instance in local-global questions (which often have an equivalent formulation in terms of principal homogeneous spaces under certain group schemes). We give an application of Theorem 1.2 to the following question, posed by Cassels in 1962, in the third paper of his remarkable series on the arithmetic of curves of genus one [2].

**Cassels’ question.** Let \(k\) be a number field, with algebraic closure \(\overline{k}\), and \(E\) be an elliptic curve defined over \(k\). Let \(G_k\) be the absolute Galois group \(\text{Gal}(\overline{k}/k)\) and \(\text{III}(k, E)\) be the Tate-Shafarevich group of \(E\) over \(k\). Fix a prime \(p\). Are the elements of \(\text{III}(k, E)\) infinitely divisible by \(p\), when considered as elements of the Weil-Châtelet group \(H^1(G_k, E)\) of all classes of principal homogeneous spaces for \(E\) defined over \(k\)?

An element \(\sigma \in \text{III}(k, E)\) is said to be infinitely divisible by a prime \(p\) when it is divisible by \(p^m\) for all positive integers \(m\), i.e., when for all \(m \in \mathbb{N}\) there exists \(\tau_m \in H^1(G_k, E)\) such that \(\sigma = p^m \tau_m\).

For \(m = 1\), in 1962 Cassels [3] showed (using a lemma of Tate) that every \(\sigma \in \text{III}(k, E)\) is divisible by \(p\) in \(H^1(G_k, E)\), but the question remained open for 50 years for powers \(p^m\) with \(m \geq 2\). Only in 2012 did we get a positive answer for all \(p \geq (3^{k/2} + 1)^2\) and all \(m\), implied by the results in [17] combined with [8] Theorem 3 (see [10] for further details and see also [4] Theorem B). In addition, results from 2014 [18] imply a positive answer over \(\mathbb{Q}\) for all \(p \geq 5\) (see [10] for more details and [14] for a second proof of the same result). This bound is best possible for \(k = \mathbb{Q}\): in 2016, Creutz gave counterexamples to the divisibility by \(p^m\) for \(p = 2, 3\) and \(m \geq 2\) [9].
Since 1972, Cassels’ question has also been considered in the more general setting of an abelian variety $A$ defined over $k$ instead of an elliptic curve $[1, 3, 8, 11]$. In $[8]$, Creutz constructed, for every prime $p$, infinitely many non-isomorphic abelian varieties over $\mathbb{Q}$ for which the answer to (the analogue of) Cassels’ question is negative.

Let $A[p^m]$ be the $p^m$-torsion subgroup of $A$ and $A[p^m]^\vee$ be its Cartier dual. The aforementioned result of Creutz $[8, \text{Theorem 3}]$ implies that the triviality of $X(k, A[p^m]^\vee)$, for every $m$, is a sufficient condition for Cassels’ question to have an affirmative answer for $p$ and $A$ (see also $[3, \text{Proposition 4.3}]$). Çiperiani and Stix $[3, \text{Theorem D}]$ also found sufficient conditions ensuring the triviality of $X(k, A[p^m])$ for all $m \geq 1$. In particular, the vanishing of these groups implies an affirmative answer to Cassels’ question in the case of principally polarized abelian varieties.

As a consequence of Theorem 1.2, we refine the criterion of Çiperiani and Stix and give sufficient conditions on $A[p]$ which ensure the simultaneous triviality of $X(k, A[p^m]^\vee)$ and $X(k, A[p^m])$, and in particular, imply a positive answer to Cassels’ question. Notice that this result also applies to non-principally polarised abelian varieties.

**Theorem 1.3.** Let $A$ be an abelian variety of dimension $g$ defined over a number field $k$. For any prime $p > 2g + 2$, if $A[p]$ is an irreducible $G_k$-module which is not isomorphic to a subquotient of $\text{End}(A[p])$, then Cassels’ question has an affirmative answer for $p$ and $A/k$.

On a related topic, in $[4]$ and $[9]$ the authors ask whether a local-global principle for divisibility by $p^m$ holds in $H^1(G_k, A)$. Let $v$ be a place of $k$ and let $k_v$ be the completion of $k$ at $v$. We denote by $k_v$ the algebraic closure of $k_v$ and by $G_{k_v}$ the Galois group $\text{Gal}(\overline{k_v}/k_v)$. An element $\sigma \in H^1(G_k, A)$ is locally divisible by $p^m$ over $k_v$ if there exists $\tau_v \in H^1(G_{k_v}, A)$ such that $\text{res}_v(\sigma) = p^m \tau_v$, where $\text{res}_v(\sigma)$ is the image of $\sigma$ under the restriction map $\text{res}_v : H^1(G_k, A) \rightarrow H^1(G_{k_v}, A)$. It is natural to ask whether an element locally divisible by $p^m$ for all $k_v$ is divisible by $p^m$ in $H^1(G_k, A)$, i.e., if the local-global principle for divisibility by $p^m$ holds in $H^1(G_k, A)$. In Section 5 we show that the hypotheses of Theorem 1.3 are also sufficient to ensure the validity of this local-global principle.

**Corollary 1.4.** Let $A$ be an abelian variety of dimension $g$ defined over a number field $k$. For every prime $p > 2g + 2$, if $A[p]$ is an irreducible $G_k$-module which is not isomorphic to...
to a subquotient of $\text{End}(A[p])$, then the local-global principle for divisibility by $p^m$ holds in $H^1(G_k, A)$, for every $m \geq 1$.

# 2 Notation and preliminaries

Let $n, m$ be positive integers, let $p$ be a prime number, and let $V = \mathbb{F}_q^n$, with $q = p^m$. We will write $\text{GL}_n(q)$ for the group $\text{GL}_n(\mathbb{F}_q) \cong \text{GL}(V)$. Throughout the paper, when we say that a group $G \leq \text{GL}_n(q)$ acts on $V$ we mean the natural action given by matrix multiplication.

## 2.1 Preliminary lemmas

We collect here two facts about the invariants of a group acting on a vector space and a criterion for the vanishing of $H^1(G, V)$ in terms of the vanishing of $H^1(H, V)$ for a normal subgroup $H$ of $G$.

**Lemma 2.1.** Let $p$ be a prime number, $k$ be a finite field of characteristic $p$, and $G$ be a $p$-group. For every finite-dimensional $k$-vector space $V$ and every linear action of $G$ on $V$ (that is, an action of $G$ on $V$ via $\text{GL}(V)$), the subspace $V^G = \{v \in V : g \cdot v = v \forall g \in G\}$ has positive dimension.

**Proof.** Consider the orbit equation

$$|V| = |V^G| + \sum_{v \in R} |\text{Orbit}(v)|,$$

where $R$ is a set of representatives for the non-trivial orbits of the action of $G$ on $V$. For $v \in R$ the cardinality $|\text{Orbit}(v)| = \frac{|G|}{|\text{Stab}(v)|}$ is a power of $p$ which is not 1 (since $\text{Stab}(v)$ is a proper subgroup of $G$, and the order of $G$ is a power of $p$). The equation above then gives $|V| \equiv |V^G|$ (mod $p$). We obtain $|V^G| \equiv |V| \equiv |k|^\dim V \equiv 0$ (mod $p$), so $|V^G|$ cannot consist only of the zero vector. \qed

**Lemma 2.2.** Let $G$ be a group acting linearly on the vector space $V$. Let $N$ be a normal subgroup of $G$. The subspace

$$V^N := \{v \in V : n \cdot v = v \forall n \in N\}$$

is invariant under the action of $G$. In particular, if $V$ is irreducible and $V^N \neq \{0\}$, then $V^N = V$. 


Proof. We check invariance: if \( v \) is in \( V^N \) and \( g \) is any element of \( G \), proving that \( g \cdot v \) is in \( V^N \) amounts to showing that \( n \cdot g \cdot v = g \cdot v \) for all \( n \in N \). Equivalently, we need to show \( (g^{-1}ng) \cdot v = v \) for all \( n \in N \). As \( N \) is a normal subgroup, \( g^{-1}ng \) is an element of \( N \) for every \( g \in G \), and by construction, \( v \) is fixed by any element of \( N \), so \( (g^{-1}ng) \cdot v = v \) as desired. The rest of the statement follows.

The next corollary deals with the case when \( G \) has a nontrivial normal subgroup \( H \) with trivial cohomology.

Corollary 2.3. Let \( V = \mathbb{F}_q^n \) and let \( G \leq \text{GL}_n(q) \) be a subgroup acting irreducibly on \( V \). Let \( H \) be a nontrivial normal subgroup of \( G \). If \( H^1(H,V) = 0 \), then \( H^1(G,V) = 0 \).

Proof. Consider the inflation-restriction exact sequence

\[
0 \to H^1(K, V^H) \to H^1(G, V) \to H^1(H, V)^K,
\]

where \( K = G/H \). Since \( H^1(H,V) = 0 \) by assumption, we have \( H^1(G,V) \cong H^1(K, V^H) \). By Lemma 2.2, the subspace \( V^H \) is a \( G \)-submodule of \( V \). As \( V \) is an irreducible \( G \)-module, \( V^H \) is either trivial or equal to \( V \), and since \( H \) is nontrivial the second case cannot arise. Thus, \( V^H \) is trivial, so we obtain \( H^1(K, V^H) = 0 \) and \( H^1(G,V) = 0 \).

3 Proof of the main theorem

We are now ready to prove our main theorem. The proof is by double induction, both on the order of \( G \) and on the number of irreducible components in the representation \( V \) of \( G \). We start with the following ‘base case’ when \( V \) has only one non-trivial irreducible component.

Proposition 3.1. Let \( p \) be a prime and \( m, n \) be positive integers. Write \( q = p^m \) and \( V = \mathbb{F}_q^n \). Let \( G \) be a subgroup of \( \text{GL}_n(q) \) and consider \( V \) as a \( G \)-module through the natural action. Suppose that, as a representation of \( G \), \( V \) decomposes as \( V_1 \oplus V_{\text{triv}} \), where \( V_1 \) is a non-trivial irreducible representation and \( V_{\text{triv}} \) is a subspace (of any dimension, including 0) on which \( G \) acts trivially. If \( p > n + 2 \), then \( H^1(G,V) = 0 \).

Proof. If \( G \) has no non-trivial normal \( p \)-subgroups, the result follows from [12] Theorem A1, so it suffices to show that this hypothesis holds. Suppose by contradiction that \( G \) admits a non-trivial normal \( p \)-subgroup \( N \). We can consider \( N \) as acting on \( V_1 \), and by Lemma 2.1 we have \( V_1^N \neq \{0\} \). By Lemma 2.2 this implies \( V_1^N = V_1 \). This equality
implies that $N$ acts trivially on all of $V$, hence that $N = \{\text{id}\}$, contradicting the fact that $N$ is nontrivial.

\[\square\]

**Proof of Theorem 1.2.** We consider $V = \mathbb{F}_q^n$ as a $G$-module. Since $V$ is semisimple, we can write it as $V = V_1 \oplus \cdots \oplus V_k$, where each subspace $V_i$ is a simple $G$-submodule of $V$. Several $V_i$ can be isomorphic to each other and the decomposition $V \cong V_1 \oplus \cdots \oplus V_k$ is not canonical, but we simply fix one such decomposition. Note that the number $k$ of simple summands is a well-defined invariant of $V$, independent of our choice of the simple submodules $V_i$ (by the Jordan-Hölder theorem).

The proof is by double induction, on the order $d$ of $G$ and the number $k$ of irreducible components of $V$. We well-order pairs $(d, k)$ by setting $(d_1, k_1) < (d_2, k_2)$ if $d_1 < d_2$ or $d_1 = d_2$ and $k_1 < k_2$. In other words, in the inductive step, we want to reduce either to a strictly smaller group, or to a group of the same order which acts via a representation with fewer irreducible components.

The case $d = 1$ is obviously trivial for any $k$ since the trivial group has trivial cohomology. The case of arbitrary $d$ and $k = 1$ follows from Proposition 3.1 (taking $V_{\text{triv}} = (0)$). We can now begin the inductive argument. Notice that, since we have already dealt with the case $k = 1$, we will be able to assume $k \geq 2$.

For each $i = 1, \ldots, k$ there is a natural projection

$$\pi'_i : G \to \prod_{j \neq i} \text{GL}(V_j),$$

given by the restriction of the action to the subspace $W_i := \bigoplus_{j \neq i} V_j$ where we omit the $i$-th irreducible component. Notice that the image $H_i$ of $\pi'_i$ can be identified with a subgroup of $\prod_{j \neq i} \text{GL}(V_j) \subseteq \text{GL}(\bigoplus_{j \neq i} V_j) = \text{GL}(W_i)$, and that $H_i$ is the group through which $G$ acts on $W_i$. In particular, $W_i$ is a semisimple representation of $G$, and equivalently of $H_i$. We denote by $N_i$ the kernel of $\pi'_i$.

By Clifford’s theorem \[5\] Theorem 1], since $N_i$ is a normal subgroup of $G$ and $V$ is semisimple as a representation of $G$, the restriction of the representation $V$ to $N_i$ is still semisimple. Moreover, by Lemma 2.2 the subspace $V^{N_i}$ is a $G$-submodule of $V$. Notice that by construction we have $W_i \subseteq V^{N_i} \subseteq V$. Since $V/W_i \cong V_i$ is an irreducible representation of $G$, there are only two $G$-submodules of $V$ containing $W_i$, namely $W_i$ itself and $V$. Therefore, for each $i = 1, \ldots, k$ there are two cases, which we label $(a)_i$ and $(b)_i$:

$(a)_i$ \ $V^{N_i} = W_i$; in particular, $N_i$ is not the trivial group.
Proof of the main theorem

\((b)\) \(V^{N_i} = V\), that is, \(N_i\) acts trivially on all of \(V\), and therefore \(N_i = \{\text{id}\}\).

Consider now, for each \(i = 1, \ldots, k\), the inflation-restriction sequence corresponding to the normal subgroup \(N_i\) of \(G\):

\[
1 \rightarrow H^1(G/N_i, V^{N_i}) \xrightarrow{\text{inf}} H^1(G, V) \xrightarrow{\text{res}} H^1(N_i, V)^{G/N_i}.
\] (3.1)

We first show that, for every \(i\), the cohomology group \(H^1(N_i, V)^{G/N_i}\) vanishes. Indeed, in case \((b)\) the group \(N_i\) is trivial, hence its cohomology vanishes. On the other hand, in case \((a)\), we distinguish two subcases:

1. \(N_i\) is a proper subgroup of \(G\). We have already observed that the restriction of \(V\) to \(N_i\) is a semisimple representation, so we can apply the inductive hypothesis since \(|N_i| < |G|\) and obtain as desired that \(H^1(N_i, V) = 0\).

2. \(N_i = G\). By definition of \(N_i\), this means that \(G\) acts trivially on all \(V_j\) with \(j \neq i\). Hence, \(V\) is the direct sum of the simple representation \(V_i\) and of the trivial representation \(W_i\). If \(V_i\) is also the trivial representation, then \(G\) acts trivially on all of \(V\) and we are done (since then \(N_i = G\) is the trivial group, whose cohomology vanishes). Otherwise, if \(V_i\) is a non-trivial simple representation, the cohomology group \(H^1(N_i, V) = H^1(G, V) = H^1(G, V_i \oplus W_i)\) vanishes by Proposition 3.1 since \(W_i\) is a trivial representation of \(G\).

Thus, the inflation-restriction sequence (3.1) gives an isomorphism \(H^1(G/N_i, V^{N_i}) \cong H^1(G, V)\) for all \(i\), and to conclude the proof it suffices to show that \(H^1(G/N_i, V^{N_i})\) vanishes for at least one \(i\). Again we distinguish cases:

1. if, for some index \(i\), we are in case \((a)_i\), then by definition we have \(V^{N_i} = W_i\) and \(N_i\) is not the trivial group. We have already observed that the quotient \(G/N_i\) can be canonically identified with the image \(H_i\) of the natural map \(\pi'_i : G \rightarrow \prod_{j \neq i} \text{GL}(V_j) \subseteq \text{GL}(W_i)\), so \(V^{N_i}\) is the natural module for the subgroup \(H_i\) of \(\text{GL}(W_i)\). Recall that \(V^{N_i} = W_i = \bigoplus_{j \neq i} V_j\) is semisimple for the action of \(H_i\). Finally, \(p > \dim V + 2 > \dim W_i + 2\). Thus, since \(|H_i| = |G/N_i| < |G|\), we can apply the inductive hypothesis to deduce \(H^1(G/N_i, V^{N_i}) = H^1(H_i, V^{N_i}) = 0\), as desired.

2. suppose instead that for all indices \(i\) we are in case \((b)_i\), so that \(N_i = \{\text{id}\}\) for each \(i\). By definition, this means that for each \(i\) the projection \(G \rightarrow \text{GL} \left( \bigoplus_{j \neq i} V_j \right)\) is
injective, and therefore that $W_i = \bigoplus_{j \neq i} V_j$ is a faithful, semisimple $G$-module with $k - 1$ irreducible components. Moreover, one has $p > \dim V + 2 > \dim W_i + 2$. For each $i$ we can therefore apply the inductive hypothesis to deduce that $H^1(G, W_i) = (0)$. By additivity of the cohomology functor, this gives

$$(0) = H^1(G, \bigoplus_{j \neq i} V_j) = \bigoplus_{j \neq i} H^1(G, V_j),$$

hence $H^1(G, V_j) = (0)$ for all $j \neq i$. But since this holds for each $i$, we deduce $H^1(G, V_j) = (0)$ for all $j$ (here we use $k \geq 2$), hence

$$H^1(G, V) = H^1(G, \bigoplus_{i=1}^k V_i) = \bigoplus_{i=1}^k H^1(G, V_i) = (0),$$

as desired. $\square$

4 Two supplements

We begin by proving a direct consequence of Theorem 1.2 concerning semisimple subgroups of $GL_n(q)$.

**Corollary 4.1.** Let $n, m$ be positive integers and let $p$ be a prime greater than $n + 3$. Let $G$ be a subgroup of $GL_n(q)$, where $q = p^m$. If $G$ acts semisimply on $F^n_q$, then $G$ has no normal subgroup of index $p^k$, for any $k \geq 1$. In particular, $G$ admits no non-trivial homomorphism to a $p$-group.

**Proof.** Let $V = F^n_q$ be the natural module for the action of $G$ and consider the semisimple representation of $G$ given by $V' = V \oplus F_q$, where $G$ acts trivially on $F_q$. Since $\dim V' = n + 1$, Theorem 1.2 shows $H^1(G, V') \oplus H^1(G, F_q) = H^1(G, V') = 0$, which implies in particular $H^1(G, F_q) = \text{Hom}(G, F_q) = 0$. It follows that $G$ admits no non-trivial homomorphisms towards $C_p$, the cyclic group of order $p$. If $N$ were a normal subgroup of $G$ of index $p^k$ for some $k \geq 1$, then the $p$-group $G/N$ would admit $C_p$ as a quotient, so $G$ would also admit $C_p$ as a quotient, contradiction. $\square$

We also consider tensor product groups $G = G_1 \otimes \cdots \otimes G_t$, where each $G_i$ is a subgroup of $GL(V_i) \cong GL_{d_i}(q)$ for some $d_i$. The group $G$ acts on $V = V_1 \otimes \cdots \otimes V_t$, and it is a natural expectation that the triviality of all the groups $H^1(G_i, V_i)$ implies $H^1(G, V) = 0$. Assuming that $V$ is irreducible, we show the stronger statement that it suffices that one of the groups $H^1(G_i, V_i)$ (with $G_i$ nontrivial) vanishes to get $H^1(G, V) = 0$. In particular,
Proposition 4.2. Let \( V = \bigotimes_{i=1}^{t} V_{i} \), where each \( V_{i} \) is a \( \mathbb{F}_{q} \)-vector space of dimension \( d_{i} \), for every \( 1 \leq i \leq t \). Assume that \( G = G_{1} \otimes \cdots \otimes G_{t} \) acts on \( V \), where \( G_{i} \) is a nontrivial subgroup of \( \text{GL}(V_{i}) \). Assume further that \( V \) is an irreducible \( G \)-module. If, for some \( 1 \leq i \leq t \), the group \( H^{1}(G_{i}, V_{i}) \) vanishes, then \( H^{1}(G, V) = 0 \). In particular, if \( p > (\dim V)^{1/t} + 2 \), then \( H^{1}(G, V) = 0 \).

**Proof.** Let \( n := \prod_{i=1}^{t} d_{i} \). By \([13\, \S 4.4, \text{pag. 129}]\), \( V \) is a homogeneous \( G_{i} \)-module, i.e., \( V = \bigoplus_{j=1}^{n} W_{j} \), where \( W_{j} \) is an irreducible \( G_{i} \)-module isomorphic to \( V_{i} \), for every \( 1 \leq j \leq n \). Thus, if \( G_{i} \) is nontrivial and \( H^{1}(G_{i}, V_{i}) = 0 \), we have \( H^{1}(G_{i}, V) = H^{1}(G_{i}, \bigoplus_{j=1}^{n} W_{j}) \cong \bigoplus_{j=1}^{n} H^{1}(G_{i}, V_{i}) = 0 \). The triviality of \( H^{1}(G, V) \) then follows from Corollary \([4\, \text{Corollary 2.3}]\) because \( G_{i} \) is normal in \( G \).

Since the action of \( G \) on \( V \) is irreducible, the action of each \( G_{i} \) on the corresponding space \( V_{i} \) is also irreducible, hence \( H^{1}(G_{i}, V_{i}) = 0 \) for all \( p > \dim V_{i} + 2 \) by Theorem \([12\, \text{Theorem 1.2}]\). In particular, letting \( i \) be the index for which \( \dim V_{i} \) is minimal, we have \( \dim V \geq (\dim V_{i})^{t} \), and the final claim follows. \( \square \)

5 An application to a question of Cassels

Let \( \mathcal{A} \) be an abelian variety defined over a number field \( k \) and let \( \mathcal{A}^{\vee} \) be its dual abelian variety. We denote by \( \overline{k} \) the algebraic closure of \( k \) and by \( G_{k} \) the absolute Galois group \( \text{Gal}(\overline{k}/k) \). Let \( \mathcal{A}[p^{m}] \) be the \( p^{m} \)-torsion subgroup of \( \mathcal{A} \) and \( \mathcal{A}[p^{m}]^{\vee} \) be its Cartier dual. As recalled in the introduction, an element \( \sigma \in \text{III}(k, \mathcal{A}) \) is said to be *infinitely divisible* by a prime \( p \) in \( H^{1}(G_{k}, \mathcal{A}) \) when it is divisible by \( p^{m} \) for all positive integers \( m \). In this case, for every \( m \), there exists \( \tau_{m} \in H^{1}(G_{k}, \mathcal{A}) \) such that \( \sigma = p^{m} \tau_{m} \). Creutz \([8\, \text{Theorem 3}]\) showed that \( \text{III}(k, \mathcal{A}) \subseteq p^{m} H^{1}(G_{k}, \mathcal{A}) \) if and only if the image of the natural map \( \text{III}(k, \mathcal{A}[p^{m}]^{\vee}) \rightarrow \text{III}(k, \mathcal{A}^{\vee}) \) is contained in the maximal divisible subgroup of \( \text{III}(k, \mathcal{A}^{\vee}) \). In particular, the vanishing of \( \text{III}(k, \mathcal{A}[p^{m}]^{\vee}) \), for all \( m \geq 1 \), is a sufficient condition for an affirmative answer to Cassels’ question for \( p \) and \( A/k \) (see also \([4\, \text{Proposition 4.3}]\)).

If \( \mathcal{A} \) has a principal polarization, then \( \mathcal{A}[p^{m}] \) and \( \mathcal{A}[p^{m}]^{\vee} \) are isomorphic. Therefore the triviality of \( \text{III}(k, \mathcal{A}[p^{m}]) \), for all \( m \geq 1 \), implies an affirmative answer to Cassels’ question for principally polarized abelian varieties. Çiperiani and Stix \([4\, \text{Proposition 4.3}]\) gave the following sufficient condition for the vanishing of \( \text{III}(k, \mathcal{A}[p^{m}]) \) for every \( m \geq 1 \).
An application to a question of Cassels

**Theorem 5.1** (Çiperiani, Stix, 2015). Let $G$ be the Galois group of the finite extension $k(A[p])/k$, where $k(A[p])$ denotes the $p$-division field of $A$ over $k$. Assume that

1) $H^1(G, A[p]) = 0$ and

2) the $G_k$-modules $A[p]$ and $\text{End}(A[p])$ have no common irreducible subquotient.

Then

$$\text{III}(k, A[p^m]) = 0, \text{ for every } m \geq 1.$$ 

Combining this result with Theorem 1.2 we obtain the following criterion.

**Theorem 5.2.** Let $A$ be an abelian variety of dimension $g$ defined over a number field $k$. For all $p > 2g + 2$, if $A[p]$ is an irreducible $G_k$-module and $\text{End}(A[p])$ has no subquotient isomorphic to $A[p]$, then

$$\text{III}(k, A[p^m]) = 0, \text{ for every } m \geq 1.$$ 

**Proof.** It is well known that if $A$ has dimension $g$, then $A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{2g} \simeq F_{p^2}^{2g}$ (see for example [15 Chap. II, pag. 61]). Thus, up to the choice of an $F_p$-basis of $A[p]$, the group $G$ has a natural faithful representation in $\text{GL}_{2g}(F_p)$. By Theorem 1.2 if $A[p]$ is an irreducible $G_k$-module (hence an irreducible $G$-module) and $p > 2g + 2$, then $H^1(G, A[p]) = 0$ and 1) in Theorem 5.1 is satisfied. Since we have assumed that $A[p]$ is irreducible and that $\text{End}(A[p])$ has no subquotient isomorphic to $A[p]$, then $A[p]$ and $\text{End}(A[p])$ do not have a common irreducible subquotient and 2) is also satisfied. Theorem 5.1 now implies $\text{III}(k, A[p^m]) = 0$ for all $m \geq 1$. \hfill $\square$

From Theorem 5.2 we now derive Theorem 1.3 which gives sufficient conditions for an affirmative answer to Cassels’ question for $p$ and $A/k$, even in the case of non-principally polarised abelian varieties $A$.

**Proof of Theorem 1.3.** Let $p > 2g + 2$. Suppose that $A[p]^\vee$ has a $G_k$-submodule $W$ which is stable under the action of $G_k$. Since $A[p]$ is an irreducible $G_k$-module, the dual $W^\vee$ of $W$ is either isomorphic to $A[p]$ or it is trivial. Consequently, $W$ is trivial or it is the whole $A[p]^\vee$. Hence $A[p]^\vee$ is an irreducible $G_k$-module. Furthermore, it is easy to see that if $S$ is a subquotient of $\text{End}(A[p])$, then $S^\vee$ is a subquotient of $\text{End}(A[p]^\vee)$. Since $\text{End}(A[p]) \simeq \text{End}(A[p]^\vee) \simeq \text{End}(A[p])^\vee$, we have that $A[p]$ is isomorphic to a subquotient of $\text{End}(A[p])$ if and only if $A[p]^\vee$ is isomorphic to a subquotient of $\text{End}(A[p]^\vee)$.
Therefore, $\text{End}(\mathcal{A}[p])$ has no subquotient isomorphic to $\mathcal{A}[p]$ if and only if $\text{End}(\mathcal{A}[p]^{\vee})$ has no subquotient isomorphic to $\mathcal{A}[p]^{\vee}$. Thus, we can apply Theorem 5.2 to $\mathcal{A}[p]^{\vee}$ and obtain $\text{III}(k, \mathcal{A}[p^m]^{\vee}) = 0$, for every $m \geq 1$ and $p > 2g + 2$. By [8, Theorem 3], this shows that Cassels’ question has a positive answer for $p$ and $\mathcal{A}$ (and also for $p$ and $\mathcal{A}^{\vee}$, by applying Theorem 5.2 and [8, Theorem 3] to $\mathcal{A}[p]$). □

Proof of Corollary 1.4. As in the proof of Theorem 1.3, we obtain $\text{III}(k, \mathcal{A}[p^m]^{\vee}) = 0$ for all $p > 2g + 2$ and all $m \geq 1$. By [9, Theorem 2.1], for every positive integer $n$, the triviality of $\text{III}(k, \mathcal{A}[n]^{\vee})$ is a sufficient condition for the validity of the local-global principle for divisibility by $n$ in $H^1(G_k, \mathcal{A})$ (see also [4, Theorem C]). The corollary follows. □

Acknowledgments. We thank an anonymous referee for pointing out some mistakes in an earlier version of this paper. We warmly thank Gabriele Ranieri, Florence Gillibert, John van Bon and Rocco Chirivi for useful discussions. We are grateful to Alessandra Caraceni for some helpful remarks. Davide Lombardo and Laura Paladino are members of INdAM-GNSAGA. Lombardo acknowledges funding from the University of Pisa via PRA 2022-10 “Spazi di moduli, rappresentazioni e strutture combinatorie”.

References

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

[2] 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.

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

[4] 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.

[5] Clifford A. H., Representations induced on an invariant subgroup, Ann. of Math. 38 no. 3 (1937), 533-550.

[6] Cline E., Parshall B., Scott L., Cohomology of finite groups of Lie type, I, Inst. Hautes Études Sci. Publ. Math., 45 (1975), 169-191.
[7] Cline E., Parshall B., Scott L., *Cohomology of finite groups of Lie type, II*, J. Algebra 45 no. 1 (1977), 182-198.

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

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

[10] Dvornicich R. and Paladino L., *Local-global questions for divisibility in commutative algebraic groups*, Eur. J. Math, 8 (2022), 599-628.

[11] Gillibert F., Ranieri G., *On the local-global divisibility over abelian varieties*, Ann. Inst. Fourier (Grenoble), 68 no. 2 (2018), 847-873.

[12] Guralnick R. M., *Small representations are completely reducible*, J. Algebra, 220 (1999), 531-541.

[13] 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.

[14] Lawson T., Wuthrich C., *Vanishing of Some Galois Cohomology Groups for Elliptic Curves*, Springer Proceedings in Mathematics and Statistics, 188 (2016), 373-399.

[15] Mumford D., *Abelian varieties*, American Mathematical Society, Tata Institute of Fundamental Research, 2008.

[16] Nori M. V., *On subgroups of GL_n(F_p)*, Invent. Math., 88 (1987), 257-275.

[17] Paladino L., Ranieri G., Viada E., *On Local-Global Divisibility by p^n in elliptic curves*, Bull. Lond. Math. Soc., 44 no. 5 (2012), 789-802.

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

[19] Serre J. P., *Oeuvres – Collected papers IV, 1985-1988*, Springer-Verlag, New York, 2000.
[20] University of Georgia Vigre Algebra Group, First cohomology for finite groups of Lie type: Simple modules with small dominant weights, Trans. Amer. Math. Soc. 365 no. 2 (2013), 1025-1050.

Davide Lombardo  
Dipartimento di Matematica  
Università di Pisa  
Largo Bruno Pontecorvo, 5  
56127 Pisa (PI)  
Italy  
e-mail address: davide.lombardo@unipi.it

Laura Paladino  
Dipartimento di Matematica e Informatica  
Università della Calabria  
Ponte Bucci, Cubo 30B  
87036 Rende (CS)  
Italy  
e-mail addresses: laura.paladino@unical.it