ESSENTIAL DIMENSION AND ERROR-CORRECTING CODES

SHANE CERNELE AND ZINOVY REICHSTEIN, WITH AN APPENDIX BY ATHENA NGUYEN

To the memory of Robert Steinberg

ABSTRACT. One of the important open problems in the theory of central simple algebras is to compute the essential dimension of GL_n/μ_m, i.e., the essential dimension of a generic division algebra of degree n and exponent dividing m. In this paper we study the essential dimension of groups of the form

$$G = (\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r})/C\,,$$

where C is a central subgroup of $\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$. Equivalently, we are interested in the essential dimension of a generic r-tuple $(A_1, \dots, A_r)$ of central simple algebras such that $\deg(A_i) = n_i$ and the Brauer classes of $A_1, \dots, A_r$ satisfy a system of homogeneous linear equations in the Brauer group. The equations depend on the choice of C via the error-correcting code $\mathrm{Code}(C)$ which we naturally associate to C. We focus on the case where $n_1, \dots, n_r$ are powers of the same prime. The upper and lower bounds on $\mathrm{ed}(G)$ we obtain are expressed in terms of coding-theoretic parameters of $\mathrm{Code}(C)$, such as its weight distribution. Surprisingly, for many groups of the above form the essential dimension becomes easier to estimate when $r \geq 3$; in some cases we even compute the exact value. The Appendix by Athena Nguyen contains an explicit description of the Galois cohomology of groups of the form $(\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r})/C$. This description and its corollaries are used throughout the paper.

1. INTRODUCTION

Let k be a base field. Unless otherwise specified, we will assume that every field appearing in this paper contains k and every homomorphism (i.e., inclusion) of fields restricts to the identity map on k.

We begin by recalling the definition of the essential dimension of a covariant functor $\mathcal{F}$ from the category of fields to the category of sets. Given a field K and an object $\alpha \in \mathcal{F}(K)$, we will say that α *descends* to an intermediate field $k \subset K_0 \subset K$ if α lies in the image of the natural map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The essential dimension $\mathrm{ed}(\alpha)$ of α is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$ such that α descends to a subfield $k \subset K_0 \subset K$. Given a prime integer p, the essential dimension $\mathrm{ed}_p(\alpha)$ of α at p is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$, where the minumum is taken over all finite field extensions L/K and all intermediate intermediate fields $k \subset K_0 \subset L$, such that $[L : K]$ is prime to p and α_L descends to K_0.

2010 *Mathematics Subject Classification.* Primary 20G15, 16K20, 16K50. Secondary 94B05.

This paper is based on a portion of the first author's Ph.D. thesis completed at the University of British Columbia. Both authors gratefully acknowledge financial support from the University of British Columbia and the Natural Sciences and Engineering Research Council of Canada.

The essential dimension $\mathrm{ed}(\mathcal{F})$ (respectively, the essential dimension $\mathrm{ed}_p(\mathcal{F})$ at p) of the functor $\mathcal{F}$ is defined as the maximal value of $\mathrm{ed}(\alpha)$ (respectively of $\mathrm{ed}_p(\alpha)$), where the maximum is taken over all feld extensions K/k and all objects $\alpha \in \mathcal{F}(K)$.

Informally speaking, $\mathrm{ed}(\alpha)$ is the minimal number of independent parameters required to define α, $\mathrm{ed}(\mathcal{F})$ is the minimal number of independent parameters required to define any object in $\mathcal{F}$, and $\mathrm{ed}_p(\alpha)$, $\mathrm{ed}_p(\mathcal{F})$ are relative versions of these notions at a prime p. These relative versions are somewhat less intuitive, but they tend to be more accessible and more amenable to computation than $\mathrm{ed}(\alpha)$ and $\mathrm{ed}(\mathcal{F})$. Clearly $\mathrm{ed}(\alpha) \geqslant \mathrm{ed}_p(\alpha)$ for each α, and $\mathrm{ed}(\mathcal{F}) \geqslant \mathrm{ed}_p(\mathcal{F})$. In most cases of interest $\mathrm{ed}(\alpha)$ is finite for every α. On the other hand, $\mathrm{ed}(\mathcal{F})$ (and even $\mathrm{ed}_p(\mathcal{F})$) can be infinite. For an introduction to the theory of essential dimension, we refer the reader to the surveys [BF03], [Re10], [Re12] and [M13].

To every algebraic group G one can associate the functor

$$\mathcal{F}_G := H^1(*, G)\colon K \mapsto \{\text{isomorphism classes of } G\text{-torsors over } \mathrm{Spec}(K)\}.$$

If G is affine, then the essential dimension of this functor is known to be finite; it is usually denoted by $\mathrm{ed}(G)$, rather than $\mathrm{ed}(\mathcal{F}_G)$. For many specific groups G, $H^1(K, G)$ is in a natural bijective correspondence with the set of isomorphism classes of some algebraic objects defined over K. In such cases, $\mathrm{ed}(G)$ may be viewed as the minimal number of independent parameters required to define any object of this type. This number is often related to classical problems in algebra.

For example, in the case where G is the projective linear group PGL_n, the objects in question are central simple algebras. That is,

$$H^1(K, \mathrm{PGL}_n) = \{\text{isomorphism classes of cenral simple } K\text{-algebras of degree } n\}. \tag{1}$$

The problem of computing $\mathrm{ed}(\mathrm{PGL}_n)$ is one of the important open problems in the theory of central simple algebras; see [ABGV11, Section 6]. This problem was first posed by C. Procesi, who showed (using different terminology) that

$$\mathrm{ed}(\mathrm{PGL}_n) \leqslant n^2\,; \tag{2}$$

see [Pr67, Theorem 2.1]. Stronger (but still quadratic) upper bounds can be found in [LRRS03, Theorem 1.1] and [Le04, Theorem 1.6].

A more general but closely related problem is computing $\mathrm{ed}(\mathrm{GL}_n/\mu_m)$, where m and n are positive integers and m divides n. Note that

$$H^1(K, \mathrm{GL}_n/\mu_m) = \begin{array}{l}\{\text{isomorphism classes of central simple } K\text{-algebras} \\ \qquad\qquad \text{of degree } n \text{ and exponent dividing } m\}.\end{array} \tag{3}$$

In particular, $\mathrm{ed}(\mathrm{PGL}_n) = \mathrm{ed}(\mathrm{GL}_n/\mu_n)$. The problem of computing $\mathrm{ed}(\mathrm{GL}_n/\mu_m)$ partially reduces to the case where $m = p^s$ and $n = p^a$ are powers of the same prime p and $1 \leqslant s \leqslant a$.

From now on we will always assume throughout that $\mathrm{char}(k) \neq p$. The inequalities

$$p^{2a-2} + p^{a-s} \geqslant \mathrm{ed}_p(\mathrm{GL}_{p^a}/\mu_{p^s}) \geqslant \begin{cases} (a-1)2^{a-1} & \text{if } p = 2 \text{ and } s = 1, \\ (a-1)p^a + p^{a-s} & \text{otherwise,} \end{cases} \tag{4}$$

proved in [BM12] represent a striking improvement on the best previously known bounds. (Here $a \geqslant 2$.) Yet the gap between the lower and upper bounds in (4) remains wide.

The gap between the best known upper and lower bounds becomes even wider when $\mathrm{ed}_p(\mathrm{GL}_{p^a}/\mu_{p^s})$ is replaced by $\mathrm{ed}(\mathrm{GL}_{p^a}/\mu_{p^s})$.

These gaps in our understanding of $\mathrm{ed}(\mathrm{GL}_n/\mu_m)$ will not deter us from considering the vastly more general problem of computing the essential dimension of groups of the form

$$G := (\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r})/C, \tag{5}$$

in the present paper. Here $n_1, \dots, n_r \geqslant 2$ are integers, and $C \subset \mathbb{G}_m^r$ is a central subgroup of $\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$.

As usual, we will identify elements $(m_1, \dots, m_r)$ of $\mathbb{Z}^r$ with characters $x\colon \mathbb{G}_m^r \to \mathbb{G}_m$, where $x\colon (\tau_1, \dots, \tau_r) \mapsto \tau_1^{m_1} \dots \tau_r^{m_r}$. The subgroup $C \subset \mathbb{G}_m^r$ is completely determined by the $\mathbb{Z}$-module

$$X(\mathbb{G}_m^r/C) = \{(m_1, \dots, m_r) \in \mathbb{Z}^r \mid \tau_1^{m_1} \dots \tau_r^{m_r} = 1 \ \ \forall (\tau_1, \dots, \tau_r) \in C\}, \tag{6}$$

consisting of characters of $\mathbb{G}_m^r$ which vanish on C. The Galois cohomology of G is explicitly described in the appendix: by Theorem A.1, $H^1(K, G)$ is naturally isomorphic to the set of isomorphism classes of r-tuples $(A_1, \dots, A_r)$ of central simple K-algebras such that

$$\deg(A_i) = n_i \quad \text{and} \quad A_1^{\otimes m_1} \otimes \cdots \otimes A_r^{\otimes m_r} \text{ is split over } K$$

for every $(m_1, \dots, m_r) \in X(\mathbb{G}_m^r/C)$. (Note that in the special case where $r = 1$, we recover (1) and (3).) It follows from this description that the essential dimension of G does not change if C is replaced by $C \cap \mu$, where

$$\mu := \mu_{n_1} \times \cdots \times \mu_{n_r}; \tag{7}$$

see Corollary A.2. Thus we will assume throughout that $C \subset \mu$. Unless otherwise specified, we will also assume that $n_1 = p^{a_1}, \dots, n_r = p^{a_r}$ are powers of the same prime p. Here $a_1, \dots, a_r \geqslant 1$ are integers. Under these assumptions, instead of $X(\mathbb{G}_m^r/C) \subset \mathbb{Z}^r$ we will consider the subgroup of $X(\mu) = (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$ given by

$$\mathrm{Code}(C) := X(\mu/C) = \{(m_1, \dots, m_r) \in X(\mu) \mid \tau_1^{m_1} \dots \tau_r^{m_r} = 1 \ \ \forall (\tau_1, \dots, \tau_r) \in C\}. \tag{8}$$

In other words, $\mathrm{Code}(C)$ consists of those characters of μ which vanish on C. The symbol "Code" indicates that we will view this group as an error-correcting code. In particular, we will define the Hamming weight $\mathrm{w}(y)$ of

$$y = (m_1, \dots, m_r) \in (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$$

as follows. Write $m_i := u_i p^{e_i}$ with $u_i \in (\mathbb{Z}/\,\mathrm{p}^{a_i}\mathbb{Z})^*$ and $0 \leq e_i \leq a_i$. Then

$$\mathrm{w}(y) := \sum_{i=1}^{r} (a_i - e_i).$$

Our main results relate $\mathrm{ed}(G)$ to coding-theoretic invariants of $\mathrm{Code}(C)$, such as its weight distribution; cf. also Corollary A.3. For an introduction to error-correcting coding theory, see [MS77].

At this point we should warn the reader that our notions of error-correcting code and Hamming weight are somewhat unusual. In coding-theoretic literature (linear) codes are usually defined as linear subspaces of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the field of q elements. In this paper by a code we will mean an additive subgroup of $(\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$. Nevertheless, in an important special case, where $a_1 = \cdots = a_r = 1$, our codes are linear codes of length

r over $\mathbb{F}_p$ in the usual sense of error-correcting coding theory, and our definition of the Hamming weight coincides with the usual definition.

Theorem 1.1. *Let p be a prime, $G := (\mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}})/C$, where $C \subset \mu_{p^{a_1}} \times \cdots \times \mu_{p^{a_r}}$ is a central subgroup, and $y_1, \dots, y_t$ be a minimal basis for* $\mathrm{Code}(C)$*; see Definition* 3.2. *Then*

(a) $\mathrm{ed}_p(G) \geqslant \left(\sum_{i=1}^t p^{\mathrm{w}(y_i)}\right) - p^{2a_1} - \cdots - p^{2a_r} + r - t$,

(b) $\mathrm{ed}(G) \leqslant \left(\sum_{i=1}^t p^{\mathrm{w}(y_i)}\right) - t + \mathrm{ed}(\overline{G})$ *and* $\mathrm{ed}_p(G) \leqslant \left(\sum_{i=1}^t p^{\mathrm{w}(y_i)}\right) - t + \mathrm{ed}_p(\overline{G})$,

where $\overline{G} := \mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_r}}$.

Although the upper and lower bounds of Theorem 1.1 never meet, for many central subgroups $C \subset \mu \subset G$, the term $\displaystyle\sum_{i=1}^t p^{\mathrm{w}(y_i)}$ is much larger than any of the other terms appearing in the above inequalities and may be viewed as giving the asymptotic value of $\mathrm{ed}(G)$. (In particular, note that in view of (2),

$$\mathrm{ed}_p(\overline{G}) \leqslant \mathrm{ed}(\overline{G}) \leqslant \mathrm{ed}(\mathrm{PGL}_{p^{a_1}}) + \cdots + \mathrm{ed}(\mathrm{PGL}_{p^{a_r}}) \leqslant p^{2a_1} + \cdots + p^{2a_r}.) \tag{9}$$

Under additional assumptions on C, we will determine $\mathrm{ed}(G)$ exactly; see Theorem 1.2.

The fact that we can determine $\mathrm{ed}(G)$ for many choices of C, either asymptotically or exactly, was rather surprising to us, given the wide gap between the best known upper and lower bounds on $\mathrm{ed}(G)$ in the simplest case, where $r = 1$; see (4). Our informal explanation of this surprising phenomenon is as follows. If $\mathrm{Code}(C)$ can be generated by vectors $y_1, \dots, y_t$ of small weight, then $\displaystyle\sum_{i=1}^t p^{\mathrm{w}(y_i)}$ no longer dominates the other terms. In particular, this always happens if $r \leqslant 2$. In such cases the value of $\mathrm{ed}(G)$ is controlled by the more subtle "lower order effects", which are poorly understood.

To state our next result, we will need the following terminology. Suppose $2 \leqslant n_1 \leqslant \cdots \leqslant n_t$ and $z = (z_1, \dots, z_r) \in (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$, where $z_{j_1}, \dots, z_{j_s} \neq 0$ for some $1 \leqslant j_1 < \cdots < j_s \leqslant r$ and $z_j = 0$ for any $j \notin \{j_1, \dots, j_r\}$. We will say that z is *balanced* if

(i) $n_{j_s} \leqslant \dfrac{1}{2} n_{j_1} n_{j_2} \dots n_{j_{s-1}}$ and

(ii) $(n_{j_1}, \dots, n_{j_s}) \neq (2,2,2,2), (3,3,3)$ or $(2,n,n)$ for any $n \geqslant 2$.

Note that condition (i) can only hold if $s \geqslant 3$. In particular, $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ has no balanced elements if $r \leqslant 2$. In the sequel we will usually assume that $n_1, \dots, n_r$ are powers of the same prime p. In this situation condition (ii) is vacuous, unless $p = 2$ or 3.

Theorem 1.2. *Let p be a prime, $G := (\mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}})/C$, where $a_r \geqslant \cdots \geqslant a_1 \geqslant 1$ are integers, and C is a subgroup of μ, as in* (7). *Assume that the base field k is of characteristic zero and* $\mathrm{Code}(C)$ *has a minimal basis $y_i = (y_{i1}, \dots, y_{ir})$, $i = 1, \dots, t$ satisfying the following conditions:*

(a) $y_{ij} = -1$, 0 or 1 in $\mathbb{Z}/p^{a_j}\mathbb{Z}$, for every $i = 1, \dots, t$ and $j = 1, \dots, r$.

(b) For every $j = 1, \dots, r$ there exists an $i \in \{1, \dots, t\}$ such that y_i is balanced and $y_{ij} \neq 0$.

Then $\operatorname{ed}(G) = \operatorname{ed}_p(G) = \left(\sum_{i=1}^{t} p^{\mathrm{w}(y_i)}\right) - p^{2a_1} - \cdots - p^{2a_r} + r - t.$

Specializing Theorem 1.2 to the case where $\operatorname{Code}(C)$ is generated by the single element $(1, \dots, 1)$, we obtain the following.

Theorem 1.3. *Let* $a_r \geqslant a_{r-1} \geqslant \cdots \geqslant a_1 \geqslant 1$ *be integers and* $\mathcal{F}\colon \mathbf{Fields}_k \to \mathbf{Sets}$ *be the covariant functor given by*

$$\mathcal{F}(K) := \left\{ \begin{array}{l} \text{isomorphism classes of } r\text{-tuples } (A_1, \dots, A_r) \text{ of central simple } K\text{-algebras} \\ \text{such that } \deg(A_i) = p^{a_i} \ \forall\ i = 1, \dots, r, \text{ and } A_1 \otimes \ldots \otimes A_r \text{ is split over } K. \end{array} \right\}$$

(a) If $a_r \geqslant a_1 + \cdots + a_{r-1}$, *then* $\operatorname{ed}(\mathcal{F}) = \operatorname{ed}(\mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_{r-1}}})$ *and*

$$\operatorname{ed}_p(\mathcal{F}) = \operatorname{ed}_p(\mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_{r-1}}}).$$

In particular, $\operatorname{ed}(\mathcal{F}) \leqslant p^{2a_1} + \cdots + p^{2a_{r-1}}$.

(b) Assume that $\operatorname{char}(k) = 0$, $a_r < a_1 + \cdots + a_{r-1}$, *and* $(p^{a_1}, \dots, p^{a_r})$ *is not of the form* $(2, 2, 2, 2)$, $(3, 3, 3)$ *or* $(2, 2^a, 2^a)$, *for any* $a \geqslant 1$. *Then*

$$\operatorname{ed}(\mathcal{F}) = \operatorname{ed}_p(\mathcal{F}) = p^{a_1 + \cdots + a_r} - \sum_{i=1}^{r} p^{2a_i} + r - 1\,. \tag{10}$$

(c) If $(p^{a_1}, \dots, p^{a_r}) = (2, 2, 2)$, *then* $\operatorname{ed}(\mathcal{F}) = \operatorname{ed}_2(\mathcal{F}) = 3$.

Here part (c) treats the smallest of the exceptional cases in part (b). Note that in this case $p = 2$, $r = 3$ and $a_1 = a_2 = a_3 = 1$. Thus $p^{a_1 + \cdots + a_r} - \sum_{i=1}^{r} p^{2a_i} + r - 1 = -2$, and formula (10) fails. The values of $\operatorname{ed}(\mathcal{F})$ and $\operatorname{ed}_p(\mathcal{F})$ in the other exceptional cases, where $(p^{a_1}, \dots, p^{a_r}) = (2, 2, 2, 2)$, $(3, 3, 3)$, or $(2, 2^a, 2^a)$ for some $a \geqslant 2$, remain open.

The results of this paper naturally lead to combinatorial questions, which we believe to be of intependent interest but will not address here. For each code (i.e. subgroup) $X \subset (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$ of rank t, let $(w_1, \dots, w_t)$ be the minimal profile of X with respect to the Hamming weight function, in the sense of Proposition 3.1. That is, $w_i = \mathrm{w}(y_i)$, where $y_1, \dots, y_t$ is a minimal basis of X. Fixing p, $a_1 \leqslant \cdots \leqslant a_r$ and t, and letting X range over all possible codes with these parameters,

- What is the lexicographically largest profile $(w_1, \dots, w_t)$?
- What is the maximal value of w_t?
- What is the probability that $w_1 = \cdots = w_t$?
- What is the maximal value of $p^{w_1} + \cdots + p^{w_t}$?
- What is the average value of $p^{w_1} + \cdots + p^{w_t}$?
- What is the probability that $w_t > 2a_r$?

Note that the expression $p^{w_1} + \cdots + p^{w_t}$ appears in the formulas given in Theorem 1.1. For large p the condition that $w_t > 2a_r$ makes $p^{w_1} + \cdots + p^{w_t}$ the dominant term in these formulas. To the best of our knowledge, questions of this type (focusing on the minimal profile of a code, rather than the minimal weight) have not been previously investigated by coding theorists even in the case, where $a_1 = \cdots = a_r = 1$.

The rest of this paper is structured as follows. In Section 2 we prove general bounds on the essential dimension of certain central extensions of algebraic groups. These bounds will serve as the starting point for the proofs of the main theorems. To make these bounds explicit for groups of the form $(\mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}})/C$ we introduce and study the notion of a minimal basis in Section 3. Theorem 1.1, 1.2 and 1.3 are then proved in Sections 4, 5 and 6, respectively. The Appendix by Athena Nguyen contains an explicit description of the Galois cohomology of groups of the form (5). This description and its corollaries are used throughout the paper.

2. Essential dimension and central extensions

Let $T = \mathbb{G}_m^r$ be a split k-torus of rank r, and

$$1 \to T \to G \to \overline{G} \to 1 \tag{11}$$

be a central exact sequence of affine algebraic groups. This sequence gives rise to the exact sequence of pointed sets

$$H^1(K, G) \to H^1(K, \overline{G}) \xrightarrow{\partial} H^2(K, T)$$

for any field extension K of the base field k. Any character $x\colon T \to \mathbb{G}_m$, induces a homomorphism $x_*\colon H^2(K, T) \to H^2(K, \mathbb{G}_m)$. We define $\mathrm{ind}^x(G, T)$ as the maximal index of $x_* \circ \partial_K(E) \in H^2(K, T)$, where the maximum is taken over all field extensions K/k and over all $E \in H^1(K, \overline{G})$. In fact, this maximal value is always attained in the case where $E = E_{\mathrm{vers}} \to \mathrm{Spec}(K)$ is a versal G-torsor (for a suitable field K). That is,

$$\mathrm{ind}^x(G, T) = \mathrm{ind}(x_* \circ \partial_K(E_{\mathrm{vers}})) \tag{12}$$

for every $x \in X(T)$; see [M13, Theorem 6.1]. Finally, we set

$$\mathrm{ind}(G, T) := \min \{ \sum_{i=1}^{r} \mathrm{ind}^{x_i}(G, T) \,|\, x_1, \dots, x_r \text{ generate } X(T) \}\,. \tag{13}$$

Our starting point for the proof of the main theorems is the following proposition.

Proposition 2.1. *Assume that the image of every $E \in H^1(K, \overline{G})$ under*

$$\partial\colon H^1(K, \overline{G}) \to H^2(K, T)$$

is p-torsion for every field extension K/k. Then

(a) $\mathrm{ed}_p(G) \geqslant \mathrm{ind}(G, T) - \dim(G)$,

(b) $\mathrm{ed}(G) \leqslant \mathrm{ind}(G, T) + \mathrm{ed}(\overline{G}) - r$ *and* $\mathrm{ed}_p(G) \leqslant \mathrm{ind}(G, T) + \mathrm{ed}_p(\overline{G}) - r$.

These bounds are variants of results that have previously appeared in the literature. Part (a) is a generalization of [BRV12, Corollary 4.2] (where r is taken to be 1). In the case where T is μ_p^r, rather than $\mathbb{G}_m^r$, a variant of part (a) is proved in [Re10, Theorem 4.1] (see also [M13, Theorem 6.2]) and a variant of part (b) in [M13, Corollaries 5.8 and 5.12].

Our proof of Proposition 2.1 proceeds along the same lines as these earlier proofs; it relies on the notions of essential and canonical dimension of a gerbe (for which we refer the reader to [BRV12] and [M13]), and the computation of the canonical dimension of a product of p-primary Brauer-Severi varieties in [KM08, Theorem 2.1]. In fact, the

argument is easier for $T = \mathbb{G}_m^r$ than for μ_p^r. In the former case (which is of interest to us here) the essential dimension of a gerbe banded by T is readily expressible in terms of its canonical dimension (see formula (15) below), while an analogous formula for gerbes banded by μ_p^r requires a far greater effort to prove. (For $r = 1$, compare the proofs of parts (a) and (b) of [BRV12, Theorem 4.1]. For arbitrary $r \geqslant 1$, see [KM08, Theorem 3.1] or [M13, Theorem 5.11].)

Proof. If K/k is a field, and $E \in H^1(K, G)$, i.e. $E \to \operatorname{Spec}(K)$ is a $\overline{G}$-torsor, then the quotient stack $[E/G]$ is a gerbe over $\operatorname{Spec}(K)$ banded by T. By [BRV12, Corollary 3.3] and [M13, Corollary 5.7], $\operatorname{ed}(G) \geqslant \max_{K,E} \operatorname{ed}([E/G]) - \dim(\overline{G})$ and similarly

$$\operatorname{ed}_p(G) \geqslant \max_{K,E} \operatorname{ed}_p([E/G]) - \dim(\overline{G})\,,$$

where the maximum is taken over all field extensions K/k and all $E \in H^1(K, \overline{G})$. On the other hand, by [Lö13, Example 3.4(i)]

$$\operatorname{ed}(G) \leqslant \operatorname{ed}(\overline{G}) + \max_{K,E} \operatorname{ed}([E/G]) \quad \text{and} \quad \operatorname{ed}_p(G) \leqslant \operatorname{ed}_p(\overline{G}) + \max_{K,E} \operatorname{ed}_p([E/G])\,;$$

see also [M13, Corollary 5.8]. Since $\dim(G) = \dim(\overline{G}) + r$, it remains to show that

$$\max_{K,E} \operatorname{ed}([E/G]) = \max_{K,E} \operatorname{ed}_p([E/G]) = \operatorname{ind}(G, T) - r\,. \tag{14}$$

Choose a $\mathbb{Z}$-basis $x_1, \dots, x_r$ for the character group $X(T) \simeq \mathbb{Z}^r$ and let $P := P_1 \times \dots \times P_r$, where P_i is the Brauer–Severi variety associated to $(x_i)_* \circ \partial(E) \in H^2(K, \mathbb{G}_m)$. Since T is a special group (i.e., every T-torsor over every field K/k is split), the set $[E/G](K)$ of isomorphism classes of K-points of $[E/G]$ consists of exactly one element if $P(K) \neq \emptyset$ and is empty otherwise. Thus

$$\operatorname{ed}([E/G]) = \operatorname{cdim}(P) \text{ and } \operatorname{ed}_p([E/G]) = \operatorname{cdim}_p(P), \tag{15}$$

where $\operatorname{cdim}(P)$ denotes the canonical dimension of P. (The same argument is used in the proof of [BRV12, Theorem 4.1(a)] in the case, where $r = 1$.) Since we are assuming that $\partial(E)$ is p-torsion, the index of each Brauer-Severi variety P_i is a power of p. Thus by [KM08, Theorem 2.1],

$$\operatorname{cdim}(P) = \operatorname{cdim}_p(P) = \min\{\sum_{i=1}^{r} \operatorname{ind}((x_i)_* \circ \partial_K(E)) \,|\, x_1, \dots, x_r \text{ generate } X(T)\} - r\,;$$

see also [M13, Theorem 4.14]. Taking $E := E_{\text{vers}}$ to be a versal $\overline{G}$-torsor, we obtain

$$\operatorname{cdim}(P) = \operatorname{cdim}_p(P) = \min\{\sum_{i=1}^{r} \operatorname{ind}^{x_i}(G, T)) \,|\, x_1, \dots, x_r \text{ generate } X(T)\} - r\,;$$

see (12). By the definition (13) of $\operatorname{ind}(G, T)$, the last formula can be rewritten as $\operatorname{cdim}(P) = \operatorname{cdim}_p(P) = \operatorname{ind}(G, T) - r$. Combining these equalities with (15), we obtain (14). □

Remark 2.2. Our strategy for proving Theorem 1.1 will be to apply Proposition 2.1 to the exact sequence (11) with $G = (\mathrm{GL}_{p^{a_1}} \times \dots \times \mathrm{GL}_{p^{a_r}})/C$, and $T := \mathbb{G}_m^r/C$. The only remaining issue is to find an expression for $\operatorname{ind}(G, T)$ in terms of $\operatorname{Code}(C)$.

Usually, the term $\operatorname{ind}(G,T)$ is computed using the formula $\operatorname{ind}^x(G,T) = \gcd \dim(\rho)$, as $\rho\colon G \to \mathrm{GL}(V)$ ranges over all finite-dimensional representations of G, such that $\tau \in T$ acts on V via scalar multiplication by $x(\tau)$. See, for example, [KM08, Theorem 4.4] or [M13, Theorem 6.1] or [LMMR13, Theorem 3.1]. We will not use this approach in the present paper. Instead, we will compute the values of $\operatorname{ind}^x(G,T)$ and $\operatorname{ind}(G,T)$ directly from the definition, using the description of the connecting map $\partial\colon H^1(K,\overline{G}) \to H^2(K,T)$ given by Theorem A.1; see the proof of Proposition 4.1 below.

3. Minimal bases

To carry out the program outlined in Remark 2.2 we will need the notion of a *minimal basis*. This section will be devoted to developing this notion.

The general setting is as follows. Let R be a local ring with maximal ideal $I \subset R$ and A be a finitely generated R-module. We will refer to a generating set $S \subset A$ as a *basis* if no proper subset of S generates A. In the sequel we will specialize R to $\mathbb{Z}/p^a\mathbb{Z}$ and A to a submodule of $(\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_t}\mathbb{Z})$, where $a = \max(a_1,\dots,a_r)$. However, in this section it will be convenient for us to work over an arbitrary local ring R.

Let $\pi\colon A \to A/IA$ be the natural projection. We will repeatedly appeal to Nakayama's Lemma, which asserts that a subset $S \subset A$ generates A as an R-module if and only if $\pi(S)$ generates A/IA as an R/I-vector space; see [Lang02, Section X.4].

By a *weight function* on A we shall mean any function $w : A \to \mathbb{N}$, where $\mathbb{N}$ denotes the set of non-negative integers. We will fix w throughout and will sometimes refer to $\mathrm{w}(y)$ as *the weight* of $y \in A$. For each basis $B = \{y_1,\dots,y_t\}$ of A, we will define the *profile* of B as

$$\mathrm{w}(B) := (\mathrm{w}(y_1),\dots,\mathrm{w}(y_t)) \in \mathbb{N}^t\,,$$

where $y_1,\dots,y_t$ are ordered so that $\mathrm{w}(y_1) \leqslant \mathrm{w}(y_2) \leqslant \cdots \leqslant \mathrm{w}(y_t)$. Let $\mathrm{Prof}(A) \subset \mathbb{N}^t$ denote the set of profiles of bases of A.

Proposition 3.1. $\mathrm{Prof}(A)$ *has a unique minimal element with respect to the partial order on* $\mathbb{N}^t$ *given by* $(\alpha_1,\dots,\alpha_t) \preceq (\beta_1,\dots,\beta_t)$ *if* $\alpha_i \leqslant \beta_i$ *for every* $i = 1,\dots,t$.

Note that since every descending chain in $(\mathrm{Prof}(A), \preceq)$ terminates, the unique minimal element is comparable to every element of $\mathrm{Prof}(A)$.

Proof. We argue by contradiction. Set $t := \dim(A/IA)$. Suppose $X = \{x_1,\dots,x_t\}$ and $Y = \{y_1,\dots,y_t\}$ are bases of A such that $\mathrm{w}(X)$ and $\mathrm{w}(Y)$ are distinct minimal elements of $\mathrm{Prof}(A)$. Let us order X and Y so that $\mathrm{w}(x_1) \leqslant \cdots \leqslant \mathrm{w}(x_t)$ and $\mathrm{w}(y_1) \leqslant \cdots \leqslant \mathrm{w}(y_t)$. Since $\mathrm{w}(X) \neq \mathrm{w}(Y)$, there exists an s between 0 and $t-1$ such that

$$\mathrm{w}(x_i) = \mathrm{w}(y_i) \text{ for all } i = 1,\dots,s$$

but $\mathrm{w}(x_{s+1}) \neq \mathrm{w}(y_{s+1})$. After possibly interchanging X and Y, we may assume without loss of generality that $\mathrm{w}(x_{s+1}) < \mathrm{w}(y_{s+1})$.

Let $\pi\colon A \to A/IA$ be the natural projection, as above. By Nakayama's Lemma, $\pi(x_1),\dots,\pi(x_{s+1})$ are R/I-linearly independent in A/IA. Choose $t-s-1$ elements of Y, say $y_{j_{s+2}},\dots,y_{j_t}$ such that $\pi(x_1),\dots,\pi(x_{s+1}),\pi(y_{j_{s+2}}),\dots,\pi(y_{j_t})$ form an R/I-basis of A/IA. After permuting $y_{j_{s+2}},\dots,y_{j_t}$, we may assume that $\mathrm{w}(y_{j_{s+2}}) \leqslant \cdots \leqslant \mathrm{w}(y_{j_t})$.

Applying Nakayama's lemma once again, we see that $Z = \{x_1, \dots, x_{s+1}, y_{j_{s+2}}, \dots, y_{j_t}\}$ is a basis of A.

We claim that $\mathrm{w}(Z) \prec \mathrm{w}(Y)$, where the inequality is strict. Since we assumed that $\mathrm{w}(Y)$ is minimal in $\mathrm{Prof}(A)$, this claim leads to a contradiction, thus completing the proof of Proposition 3.1.

To prove the claim, let $z_1, \dots, z_t$, be the elements of Z, in increasing order of their weight: $\mathrm{w}(z_1) \leqslant \mathrm{w}(z_2) \leqslant \dots \leqslant \mathrm{w}(z_t)$. It suffices to show that $\mathrm{w}(z_i) \leqslant \mathrm{w}(y_i)$ for every $i = 1, \dots, t$, and $\mathrm{w}(z_{s+1}) < \mathrm{w}(y_{s+1})$. Let us consider three cases.

(i) $i \leqslant s$. Since

$$\mathrm{w}(x_1) = \mathrm{w}(y_1) \leqslant \mathrm{w}(x_2) = \mathrm{w}(y_2) \leqslant \dots \leqslant \mathrm{w}(x_i) = \mathrm{w}(y_i)\,,$$

Z has at least i elements whose weight is $\leqslant \mathrm{w}(y_i)$, namely $x_1, \dots, x_i$. Thus $\mathrm{w}(z_i) \leqslant \mathrm{w}(y_i)$.

(ii) $i = s + 1$. Z has at least $s + 1$ elements, namely $x_1, \dots, x_{s+1}$ whose weight is at most $\mathrm{w}(x_{s+1})$. Hence, $\mathrm{w}(z_{s+1}) \leqslant \mathrm{w}(x_{s+1}) < \mathrm{w}(y_{s+1})$, as desired.

(iii) $i > s + 1$. Recall that both $y_1, \dots, y_t$ and $y_{j_{s+2}}, \dots, y_{j_t}$ are arranged in weight-increasing order. For any $i \geqslant s+2$ there are at least $t - i + 1$ elements of Y whose weight is $\geqslant \mathrm{w}(y_{j_i})$, namely $y_{j_i}, y_{j_{i+1}}, \dots, y_{j_t}$. Thus

$$\mathrm{w}(y_{j_i}) \leqslant \mathrm{w}(y_i)$$

for any $i = s+2, \dots, t$. Consequently, Z has at least i elements of weight $\leqslant \mathrm{w}(y_i)$, namely $x_1, \dots, x_{s+1}, y_{j_{s+2}}, \dots, y_{j_i}$. Hence, $\mathrm{w}(z_i) \leqslant \mathrm{w}(y_i)$, as desired.

This completes the proof of the claim and hence of Proposition 3.1. □

Definition 3.2. We will say that a basis $y_1, \dots, y_t$ of A is *minimal* if its profile is the minimal element of $\mathrm{Prof}(A)$, as in Proposition 3.1. Note that a minimal basis in A is usually not unique; however any two minimal bases have the same profile in $\mathbb{N}^t$.

Remark 3.3. We can construct a minimal basis of A using the following "greedy algorithm". Select $y_1 \in A$ of minimal weight, subject to the condition that $\pi(y_1) \neq 0$. Next select y_2 of minimal weight, subject to the condition that $\pi(y_1)$ and $\pi(y_2)$ are R/I-linear independent in A/IA. Then select y_3 of minimal weight, subject to the condition that $\pi(y_1), \pi(y_2)$ and $\pi(y_3)$ are R/I-linear independent in A/IA. Continue recursively. After $t = \dim_{R/I}(A/IA)$ steps, we obtain a minimal basis $y_1, \dots, y_t$ for A.

Example 3.4. Set $R := \mathbb{F}_p$, $I := (0)$, G a finite p-group, $D := Z(G)[p]$ the subgroup of p-torsion elements of the center $Z(G)$, and $A := X(D)$ the group of characters of D. For $x \in A$, define $\mathrm{w}(x)$ to be the minimal dimension of a representation $G \to \mathrm{GL}(V_x)$, such that D acts on V_x via scalar multiplication by x. If $\{x_1, \dots, x_t\}$ is a minimal basis of A, then $V_{x_1} \oplus \dots \oplus V_{x_t}$ is a faithful representation of G of minimal dimension; see [KM08, Remark 4.7].

4. Conclusion of the proof of Theorem 1.1

Recall that we are interested in the essential dimension of the group

$$G = (\mathrm{GL}_{p^{a_1}} \times \dots \times \mathrm{GL}_{p^{a_r}})/C\,,$$

where C is a subgroup of $\mu := \mu_{p^{a_1}} \times \cdots \times \mu_{p^{a_r}}$. We will think of the group of characters $X(\mathbb{G}_m^r)$ as $\mathbb{Z}^r$ by identifying the character $x(\tau_1, \dots, \tau_r) = \tau_1^{m_1} \dots \tau_r^{m_r}$ with $(m_1, \dots, m_r) \in \mathbb{Z}^r$. Characters of $T := \mathbb{G}_m^r / C$ are identified in this manner with the r-tuples $(m_1, \dots, m_r) \in \mathbb{Z}^r$ such that $\tau_1^{m_1} \dots \tau_r^{m_r} = 1$ for every $(\tau_1, \dots, \tau_r) \in C$. The relationship among these character groups is illustrated by the following diagram

$$\begin{array}{ccccc} & & X(\mathbb{G}_m^r/C) & \hookrightarrow & X(\mathbb{G}_m^r) & = & \mathbb{Z} \times \cdots \times \mathbb{Z} \ (r \text{ times}) \\ & & \downarrow & & \downarrow \pi & & \downarrow \pi \\ \mathrm{Code}(C) & = & X(\mu/C) & \hookrightarrow & X(\mu) & = & (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z}). \end{array}$$

Here $\mathrm{Code}(C)$ is as in (8) and π is the natural projection, given by restricting a character from $\mathbb{G}_m^r$ to μ.

Our proof of Theorem 1.1 will be based on the strategy outlined in Remark 2.2. In view of Proposition 2.1 it suffices to establish the following:

Proposition 4.1. *Consider the central exact sequence*

$$1 \to T \to G \to \overline{G} \to 1\,, \tag{16}$$

where $G = (\mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}})/C$, *$C$ is a subgroup of* $\mu := \mu_{p^{a_1}} \times \cdots \times \mu_{p^{a_r}}$, $T := \mathbb{G}_m^r/C$ *and* $\overline{G} := \mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_r}}$.

(a) If $x \in X(T)$ and $y = \pi(x) \in \mathrm{Code}(C)$ then $\mathrm{ind}^x(G,T) = p^{\mathrm{w}(y)}$.

(b) $\mathrm{ind}(G,T) = p^{\mathrm{w}(z_1)} + \cdots + p^{\mathrm{w}(z_t)} + r - t$, *where $z_1, \dots, z_t$ is a minimal basis of* $\mathrm{Code}(C)$.

Proof of Proposition 4.1(a). Consider the connecting map $\partial\colon H^1(K, \overline{G}) \to H^2(K,T)$ associated to the central exact sequence (16). Given a character $x\colon T \to \mathbb{G}_m$, $x(\tau_1, \dots, \tau_r) = \tau_1^{m_1} \dots \tau_r^{m_r}$, $\mathrm{ind}^x(G,T)$ is, by definition, the maximal value of $\mathrm{ind}(x_*\partial(E))$, as K ranges over all fields containing k and E ranges over $H^1(K, \overline{G})$. In this case, $\overline{G} = \mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_r}}$, and thus $H^1(K, \overline{G})$ is the set of r-tuples $(A_1, \dots, A_r)$ of central simple algebras, where the degree of A_i is p^{a_i}. The group $H^2(K, \mathbb{G}_m)$ is naturally identified with the Brauer group $\mathrm{Br}(K)$, and the map $x_*\partial$ takes an r-tuple $(A_1, \dots, A_r)$, as above, to the Brauer class of $A := A_1^{\otimes m_1} \otimes \cdots \otimes A_r^{\otimes m_r}$.

Since $\deg(A_i) = p^{a_i}$, the Brauer class of A depends only on

$$y = \pi(x) = (m_1 \mod p^{a_1}, \dots, m_r \mod p^{a_r}) \in (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z}))\,.$$

Moreover, if $m_i \equiv u_i p^{e_i} \pmod{p^{a_i}}$, where u_i is prime to p and $0 \leqslant e_i \leqslant a_i$ then $\mathrm{ind}(A_i^{\otimes m_i}) \leqslant p^{a_i - e_i}$. Now recall that $\mathrm{w}(y)$ is defined as $\sum_{i=1}^r (a_i - e_i)$. Thus

$$\mathrm{ind}(A) \leqslant \prod_{i=1}^r \mathrm{ind}(A_i^{\otimes m_i}) \leqslant \prod_{i=1}^r p^{a_i - e_i} = p^{\mathrm{w}(y)}\,.$$

To prove the opposite inequality, we set A_i to be the symbol algebra $(\alpha_i, \beta_i)_{p^{a_i}}$, over the field $K = k(\zeta)(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r)$, where ζ is a primitive root of unity of degree $p^{\max(a_1, \dots, a_r)}$ and $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$ are $2r$ independent variables over k. Writing $m_i = u_i p^{e_i}$, as above, we see that $A_i^{\otimes m_i}$ is Brauer equivalent to $B_i := (\alpha_i, \beta_i^{u_i})_{p^{a_i - e_i}}$ over K. An easy valuation-theoretic argument shows that $B := B_1 \otimes_K \cdots \otimes_K B_t$ is a division algebra.

(In particular, the norm form of B is a Pfister polynomial and hence, is anisotropic; see [Re99, Theorem 3.2 and Proposition 3.4].) Thus

$$\operatorname{ind}(A) = \operatorname{ind}(B) = \operatorname{ind}(B_1) \cdot \ldots \cdot \operatorname{ind}(B_t) = p^{(a_1-e_1)+\cdots+(a_t-e_t)} = p^{\mathrm{w}(y)},$$

as desired. We conclude that $\operatorname{ind}^x(G,T) \geqslant \operatorname{ind}(A) = p^{\mathrm{w}(y)}$, thus completing the proof of Proposition 4.1(a). □

Our proof of Proposition 4.1(b) will rely on the following elementary lemma.

Lemma 4.2. *Let p be a prime, M be a finite abelian p-group, and $f\colon \mathbb{Z}^n \to M$ be a surjective $\mathbb{Z}$-module homomorphism for some $n \geqslant 1$. Then for every basis $y_1, \ldots, y_t$ of M, there exists a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of $\mathbb{Z}^n$ and an integer c prime to p, such that $f(x_1) = cy_1, f(x_2) = y_2, \ldots, f(x_t) = y_t$ and $f(x_{t+1}) = \cdots = f(x_n) = 0$.*

Proof. By [Lang02, Theorem III.7.8] there exists a basis $e_1, \ldots, e_n$ of $\mathbb{Z}^n$ such that $\operatorname{Ker}(f)$ is generated by $p^{d_i}e_i$ for some integers $d_1, \ldots, d_t \geqslant 0$. Since M has rank t, we may assume without loss of generality that $d_1, \ldots, d_t \geqslant 1$ and $d_{t+1} = \cdots = d_n = 0$. That is, we may identify M with $(\mathbb{Z}/p^{d_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{d_t}\mathbb{Z})$ and assume that

$$f(r_1, \ldots, r_n) = (\, r_1 \mod p^{d_1}, \ \ldots\ , \ r_t \mod p^{d_t}) \quad \forall (r_1, \ldots, r_n) \in \mathbb{Z}^n\ .$$

It now suffices to lift $cy_1, \ldots, y_t \in M$ to a basis $x_1, \ldots, x_t$ of $\mathbb{Z}^t$, for a suitable integer c, prime to p. Indeed, if we manage to do this, then we will obtain a basis of $\mathbb{Z}^n$ of the desired form by appending

$$x_{t+1} := e_{t+1}, \ldots, x_n := e_n \in \operatorname{Ker}(f)$$

to $x_1, \ldots, x_t$. Thus we may assume that $n = t$.

Now observe that $f\colon \mathbb{Z}^n \to M$, factors as $\mathbb{Z}^n \to (\mathbb{Z}/p^d\mathbb{Z})^n \to M$, where $d := \max(d_1, \ldots, d_t)$. Lift each $y_i \in M$ to some $y_i' \in (\mathbb{Z}/p^d\mathbb{Z})^n$. By Nakayama's Lemma $y_1', \ldots, y_n'$ form a $\mathbb{Z}/p^d\mathbb{Z}$-basis of $(\mathbb{Z}/p^d\mathbb{Z})^n$. It now suffices to lift $cy_1', y_2', \ldots, y_n'$ to a basis of $\mathbb{Z}^n$, for a suitable integer c, prime to p. In other words, we may assume without loss of generality that $M = (\mathbb{Z}/p^d\mathbb{Z})^n$, and $f\colon \mathbb{Z}^n \to (\mathbb{Z}/p^d\mathbb{Z})^n$ is the natural projection.

Now suppose $y_i = (y_{i1}, \ldots, y_{in})$ for some $y_{ij} \in \mathbb{Z}/p^d\mathbb{Z}$. Since $y_1, \ldots, y_m$ form a basis of $(\mathbb{Z}/p^d\mathbb{Z})^n$, the matrix $A = (y_{ij})$ is invertible, i.e., $A \in \mathrm{GL}_n(\mathbb{Z}/p^d\mathbb{Z})$. After rescaling y_1 by $c := \det(A)^{-1}$ in $\mathbb{Z}/p^d\mathbb{Z}$, we may assume that $\det(A) = 1$. The lemma now follows from the surjectivity of the natural projection $\mathrm{SL}_t(\mathbb{Z}) \to \mathrm{SL}_t(\mathbb{Z}/p^d\mathbb{Z})$; see [Sh71, Lemma 1.38]. □

Proof of Proposition 4.1(b). By definition, $\operatorname{ind}(G,T)$ is the minimal value of $\operatorname{ind}^{x_1}(G,T) + \cdots + \operatorname{ind}^{x_r}(G,T)$, as $x_1, \ldots, x_r$ range over the bases of $X(T) \subset \mathbb{Z}^r$. By part (a), we can rewrite this as

$$\operatorname{ind}(G,T) = \min\{p^{\mathrm{w}(\pi(x_1))} + \cdots + p^{\mathrm{w}(\pi(x_r))} \mid x_1, \ldots, x_r \text{ is a } \mathbb{Z}\text{-basis of } X(T)\}.$$

Here, as before, $\pi(x_i) \in \operatorname{Code}(C)$ is the restriction of x_i from $T = \mathbb{G}_m^r/C$ to μ/C.

Let $z_1, \ldots, z_t \in \operatorname{Code}(C)$ be a minimal basis, as in the statement of the proposition. We will prove part (b) by showing that

(i) $p^{\mathrm{w}(\pi(x_1))} + \cdots + p^{\mathrm{w}(\pi(x_r))} \geqslant p^{\mathrm{w}(z_1)} + \cdots + p^{\mathrm{w}(z_t)} + r - t$ for every $\mathbb{Z}$-basis $x_1, \ldots, x_r$ of $X(T)$, and

(ii) there exists a particular $\mathbb{Z}$-basis $x_1, \dots, x_r$ of $X(T)$ such that $p^{\mathrm{w}(\pi(x_1))} + \dots + p^{\mathrm{w}(\pi(x_r))} = p^{\mathrm{w}(z_1)} + \dots + p^{\mathrm{w}(z_t)} + r - t$.

To prove (i), note that if $x_1, \dots, x_r$ form a $\mathbb{Z}$-basis of $X(T)$, then $\pi(x_1), \dots, \pi(x_r)$ form a generating set for $\mathrm{Code}(C)$. By Nakayama's Lemma every generating set for $\mathrm{Code}(C)$ contains a basis. After renumbering $x_1, \dots, x_r$ we may assume that $\pi(x_1), \dots, \pi(x_t)$ is a basis of $\mathrm{Code}(C)$ and $\mathrm{w}(\pi(x_1)) \leqslant \dots \leqslant \mathrm{w}(\pi(x_t))$. By Proposition 3.1, $\mathrm{w}(z_i) \leqslant \mathrm{w}(\pi(x_i))$ for every $i = 1, \dots, t$. Thus

$$p^{\mathrm{w}(\pi(x_1))}+\dots+p^{\mathrm{w}(\pi(x_r))} \geqslant p^{\mathrm{w}(\pi(x_1))}+\dots+p^{\mathrm{w}(\pi(x_t))}+\underbrace{p^0+\dots+p^0}_{r-t \text{ times}} \geqslant p^{\mathrm{w}(z_1)}+\dots+p^{\mathrm{w}(z_t)}+r-t\,.$$

To prove (ii), recall that by Lemma 4.2 there exists an integer c, prime to p, and a $\mathbb{Z}$-basis $x_1, \dots, x_r$ of $X(T)$ such that $\pi(x_1) = cz_1, \pi(x_2) = z_2, \dots, \pi(x_t) = z_t$, and $\pi(x_{t+1}) = \dots = \pi(x_r) = 0$. Since c is prime to p, $\mathrm{w}(cz_1) = \mathrm{w}(z_1)$. Thus for this particular choice of $x_1, \dots, x_r$, we have

$$p^{\mathrm{w}(\pi(x_1))}+\dots+p^{\mathrm{w}(\pi(x_r))} = p^{\mathrm{w}(cz_1)}+p^{\mathrm{w}(z_2)}\dots+p^{\mathrm{w}(z_t)}+\underbrace{p^0+\dots+p^0}_{r-t \text{ times}} = p^{\mathrm{w}(z_1)}+\dots+p^{\mathrm{w}(z_t)}+r-t\,.$$

as desired. □

5. Proof of Theorem 1.2

Consider the action of a linear algebraic group Γ on an absolutely irreducible algebraic variety X defined over k. We say that a subgroup $S \subset \Gamma$ is a *stabilizer in general position* for this action if there exists a dense open subset $U \subset X$ such that the scheme-theoretic stabilizer $\mathrm{Stab}_\Gamma(x)$ is conjugate to S over $\overline{k}$ for every $x \in U(\overline{k})$. Here, as usual, $\overline{k}$ denotes the algebraic closure of k. In the sequel we will not specify U and will simply say that $\mathrm{Stab}_\Gamma(x)$ is conjugate to S for $x \in X(\overline{k})$ in general position. Note that a stabilizer in general position S for a Γ-action on X does not always exist, and when it does, it is usually not unique. However, over $\overline{k}$, S is unique up to conjugacy.

For the rest of this section we will always assume that $\mathrm{char}(k) = 0$. A theorem of R. W. Richardson [Ri72] tells us that under this assumption every linear action of a reductive group Γ on a vector space V has a stabilizer $S \subset \Gamma$ in general position. Note that in Richardson's paper [Ri72], k is assumed to be algebraically closed. Thus a priori the subgroup S and the open subset $U \subset V$, where all stabilizers are conjugate to S, are only defined over $\overline{k}$. However, after intersecting U with its Galois translates, we may assume that U is defined over k. Moreover, we may take $S := \mathrm{Stab}_G(x)$ for some k-point $x \in U(k)$ and thus assume that S is defined over k. For a detailed discussion of stabilizers in general position over an algebraically closed field of characteristic zero, see [PV94, Section 7].

We will say that a Γ-action on X is *generically free* if the trivial subgroup $S = \{1_\Gamma\} \subset \Gamma$ is stabilizer in general position for this action.

Lemma 5.1. *Let Γ be a reductive linear algebraic group and $\rho\colon \Gamma \to \mathrm{GL}(V)$ be a finite-dimensional representation. If $\mathrm{Stab}_\Gamma(v)$ is central in Γ for $v \in V$ in general position, then the induced action of $\Gamma/\mathrm{Ker}(\rho)$ on V is generically free.*

Proof. Let $S \subset \Gamma$ be the stabilizer in general position for the Γ-action on V. Clearly $\mathrm{Ker}(\rho) \subset S$. We claim that, in fact, $\mathrm{Ker}(\rho) = S$; the lemma easily follows from this claim.

To prove the opposite inclusion, $S \subset \mathrm{Ker}(\rho)$, note that under the assumption of the lemma, S is central in Γ. Let $U \subset V$ be a dense open subset such that the stabilizer of every $v \in U(\overline{k})$ is conjugate to S. Since S is central, $\mathrm{Stab}_\Gamma(v)$ is, in fact, equal to S. In other words, S stabilizes every point in U and thus every point in V. That is, $S \subset \mathrm{Ker}(\rho)$, as claimed. □

Our interest in generically free actions in this section has to do with the following fact: if there exists a generically free linear representation $G \to \mathrm{GL}(V)$ then

$$\mathrm{ed}(G) \leqslant \dim(V) - \dim(G)\,; \tag{17}$$

see, e.g., [Re10, (2.3)] or [M13, Proposition 3.13]. This inequality will play a key role in our proof of Theorem 1.2.

Now set $\Gamma := \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$ and $\Gamma' := \mathrm{SL}_{n_1} \times \cdots \times \mathrm{SL}_{n_r}$. Let V_i be the natural n_i-dimensional representation, V_i^{-1} be the dual representation, and V_i^0 be the trivial 1-dimensional representation of GL_{n_i}. For $\epsilon = (\epsilon_1, \dots, \epsilon_r)$, where each ϵ_i is -1, 0 or 1, we define ρ_ϵ to be the natural representation of Γ on the tensor product

$$V_\epsilon = V_1^{\epsilon_1} \otimes \cdots \otimes V_r^{\epsilon_r}\,. \tag{18}$$

Lemma 5.2. *Suppose* $2 \leqslant n_1 \leqslant \ldots \leqslant n_r \leqslant \frac{1}{2} n_1 \ldots n_{r-1}$, *and*

$$(n_1, \dots, n_r) \neq (2,2,2,2),\ (3,3,3),\ \text{or}\ (2,n,n),\ \text{for any}\ n \geqslant 2.$$

If $\epsilon = (\epsilon_1, \dots, \epsilon_r) \in \{\pm 1\}^r$, *then the induced action of* $\Gamma/\mathrm{Ker}(\rho_\epsilon)$ *on* V_ϵ *is generically free.*

Proof. By Lemma 5.1 it suffices to prove the following claim: the stabilizer $\mathrm{Stab}_\Gamma(v)$ is central in Γ for $v \in V_\epsilon$ in general position. To prove this claim, we may assume without loss of generality that k is algebraically closed.

We first reduce to the case where $\epsilon = (1, \dots, 1)$. Suppose the claim is true in this case, and let $(\epsilon_1, \dots, \epsilon_r) \in \{\pm 1\}^r$. By choosing bases of $V_1, \dots, V_r$ we can identify V_i with $V_i^{\epsilon_i}$ (we can take the identity map if $\epsilon_i = 1$). Define an automorphism:

$$\begin{aligned} \sigma : \Gamma &\to \Gamma \\ (g_1, \dots, g_r) &\mapsto (g_1^*, \dots, g_r^*) \end{aligned}$$

where

$$g_i^* = \begin{cases} g_i & \text{if } \epsilon_i = 1; \\ (g_i^{-1})^T & \text{if } \epsilon_i = -1. \end{cases}$$

Now $\rho_{(\epsilon_1,\dots,\epsilon_r)}$ is isomorphic to the representation $\rho_{(1,\dots,1)} \circ \sigma$. Since the center of Γ is invariant under σ, we see that the claim holds for ρ_ϵ as well.

From now on we will assume $\epsilon = (1, \dots, 1)$. By [P87, Theorem 2],

$$\Gamma/Z(\Gamma) = \mathrm{PGL}_{n_1} \times \cdots \times \mathrm{PGL}_{n_r} = \Gamma'/Z(\Gamma')$$

acts generically freely on the projective space $\mathbb{P}(V_\epsilon) = V_\epsilon/Z(\Gamma)$. In other words for $v \in V_\epsilon$ in general position the stabilizer in Γ of the associated projective point $[v] \in \mathbb{P}(V_\epsilon)$ is

trivial. Hence, the stabilizer of v is contained in $Z(\Gamma)$; see the exact sequence in [RV07, Lemma 3.1]. This completes the proof of the claim and thus of Lemma 5.2. □

We are now ready to proceed with the proof of Theorem 1.2. We begin by specializing n_i to p^{a_i} for every $i = 1, \dots, r$, so that Γ becomes $\mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}}$. Let

$$y_1, \dots, y_t \in (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$$

be a basis of $\mathrm{Code}(C)$ satisfying the conditions of Theorem 1.2. Lift each $y_i = (y_{i1}, \dots, y_{ir})$ to $x_i := (x_{i1}, \dots, x_{ir}) \in \mathbb{Z}^r$ by setting $x_{ij} := -1$, 0 or 1, depending on whether y_{ij} is -1, 0 or 1 in $\mathbb{Z}/p^{a_j}\mathbb{Z}$. (If $p^{a_j} = 2$, then we define each x_{ij} to be 0 or 1.) By Nakayama's Lemma the images of $y_1, \dots, y_t$ are $\mathbb{F}_p$-linearly independent in $\mathrm{Code}(C)/p\,\mathrm{Code}(C)$. Thus the integer vectors $x_1, \dots, x_t$ are $\mathbb{Z}$-linearly independent. (Note that, unlike in the situation of Lemma 4.2, here it will not matter to us whether $x_1, \dots, x_t$ can be completed to a $\mathbb{Z}$-basis of $\mathbb{Z}^r$.) We view each x_i as a character $\mathbb{G}_m^r \to \mathbb{G}_m$ and set

$$\widetilde{C} := \mathrm{Ker}(x_1) \cap \cdots \cap \mathrm{Ker}(x_t) \subset \mathbb{G}_m^r \ .$$

Since $x_1, \dots, x_t$ are linearly independent,

$$\dim(\widetilde{C}) = r - t. \tag{19}$$

Set $G := \Gamma/C$ and $\widetilde{G} := \Gamma/\widetilde{C}$. By our construction, $\widetilde{C} \cap \mu = C$. Corollary A.2 now tells us that $\mathrm{ed}_p(G) \leqslant \mathrm{ed}(G) = \mathrm{ed}(\widetilde{G})$. By Theorem 1.1(a)

$$\mathrm{ed}(G) \geqslant \mathrm{ed}_p(G) \geqslant \left(\sum_{i=1}^{t} p^{\mathrm{w}(y_i)} \right) - p^{2a_1} - \cdots - p^{2a_r} + r - t.$$

It thus suffices to show that $\mathrm{ed}(\widetilde{G}) \leqslant \left(\sum_{i=1}^{t} p^{\mathrm{w}(y_i)}\right) - p^{2a_1} - \cdots - p^{2a_r} + r - t$ or equivalently,

$$\mathrm{ed}(\widetilde{G}) \leqslant \left(\sum_{i=1}^{t} p^{\mathrm{w}(y_i)} \right) - \dim(\widetilde{G})\,;$$

see (19). By (17), in order to prove the last inequality it is enough to construct a generically free linear representation of $\widetilde{G}$ of dimension $\sum_{i=1}^{t} p^{\mathrm{w}(y_i)}$. Such a representation is furnished by the lemma below.

Recall that $x_i = (x_{i1}, \dots, x_{ir}) \in \mathbb{Z}^r$, where each $x_{ij} = -1$, 0 or 1, and ρ_{x_i} is the natural representation of $\Gamma := \mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}}$ on $V_{x_i} := V_1^{x_{i1}} \otimes \cdots \otimes V_r^{x_{ir}}$, as in (18), with $\dim(V_i) = n_i = p^{a_i}$.

Lemma 5.3. *Let $V = V_{x_1} \oplus \cdots \oplus V_{x_t}$ and $\rho := \rho_{x_1} \oplus \cdots \oplus \rho_{x_t} \colon \Gamma \to \mathrm{GL}(V)$. Then*

(a) $\dim(V) = p^{\mathrm{w}(y_1)} + \cdots + p^{\mathrm{w}(y_t)}$,

(b) $\mathrm{Ker}(\rho) = \widetilde{C}$, and

(c) the induced action of $\widetilde{G} = \Gamma/\widetilde{C}$ on V is generically free.

Proof. For each $i = 1, \dots t$, we have

$$\dim(V_{x_i}) = \prod_{x_{ij} \neq 0} p^{a_j} = \prod_{y_{ij} \neq 0} p^{a_j} = p^{\sum_{y_{ij} \neq 0} a_j} \ .$$

Since each $y_{ij} = -1$, 0 or 1, $\sum_{y_{ij}\neq 0} a_j = \mathrm{w}(y_i)$. Thus $\dim(V_{x_i}) = p^{\mathrm{w}(y_i)}$, and part (a) follows.

Now choose $v_i \in V_{x_i}$ in general position and set $v := (v_1, \dots, v_r)$. We claim that $\mathrm{Stab}_\Gamma(v)$ is central in Γ.

Suppose for a moment that this claim is established. Since the center $Z(\Gamma) = \mathbb{G}_m^r$ acts on V_{x_i} via scalar multiplication by the character $x_i\colon\ \mathbb{G}_m^r \to \mathbb{G}_m$, we see that

$$\mathrm{Ker}(\rho) = \mathrm{Ker}(\rho_{|\,\mathbb{G}_m^r}) = \mathrm{Ker}(x_1) \cap \dots \cap \mathrm{Ker}(x_t) = \widetilde{C}\,,$$

and part (b) follows. Moreover, by Lemma 5.1, the induced action of $\Gamma/\mathrm{Ker}(\rho)$ on V is generically free. By part (b), $\mathrm{Ker}(\rho) = \widetilde{C}$ and part (c) follows as well.

It remains to prove the claim. Choose $v_i \in V_{x_i}$ in general position and assume that $g = (g_1, \dots, g_r)$ stabilizes $v := (v_1, \dots, v_t)$ in V for some $g_j \in \mathrm{GL}_{p^{a_j}}$. Our goal is to show that g_j is, in fact, central in $\mathrm{GL}_{p^{a_j}}$ for each $j = 1, \dots, r$.

Let us fix j and focus on proving that g_j is central for this particular j. By assumption (b) of Theorem 1.2, there exists an $i = 1, \dots, t$ such that y_i is balanced and $y_{ij} \neq 0$. Let us assume that $y_{ij_1}, \dots, y_{ij_s} = \pm 1$ and $y_{ih} = 0$ for every $h \notin \{j_1, \dots, j_r\}$ and consequently, $x_{ij_1}, \dots, x_{ij_s} = \pm 1$ and $x_{ih} = 0$ for every $h \notin \{j_1, \dots, j_r\}$. By our assumption, $j \in \{j_1, \dots, j_s\}$.

The representation ρ_{x_i} of $\Gamma = \mathrm{GL}_{p^{a_1}} \times \dots \times \mathrm{GL}_{p^{a_r}}$ on

$$V_{x_i} := V^{x_{i1}} \otimes \dots \otimes V^{x_{it}} = V^{x_{ij_1}} \otimes \dots \otimes V^{x_{ij_s}}$$

factors through the projection $\Gamma \to \mathrm{GL}_{p^{a_{j_1}}} \times \dots \times \mathrm{GL}_{p^{a_{j_s}}}$. Thus if $g = (g_1, \dots, g_r)$ stabilizes $v = (v_1, \dots, v_t) \in V$ then, in particular, g stabilizes v_i and thus $(g_{j_1}, \dots, g_{j_s})$ stabilizes v_i.

Since y_i is assumed to be balanced, the conditions of Lemma 5.2 for the action of $\mathrm{GL}_{n_{j_1}} \times \dots \times \mathrm{GL}_{n_{j_s}}$ on $V_{x_i} = V^{x_{j_1}} \otimes \dots \otimes V^{x_{j_s}}$ are satisfied. (Recall that here $n_i = p^{a_i}$.) Since $(g_{j_1}, \dots, g_{j_s})$ stabilizes $v_i \in V_{x_i}$ in general position, Lemma 5.2 tells us that $g_{j_1}, \dots, g_{j_s}$ are central in $\mathrm{GL}_{n_{j_1}}, \dots \mathrm{GL}_{n_{j_s}}$, respectively. In particular, g_j is central in GL_{n_j}, as desired. This completes the proof of Lemma 5.3 and thus of Theorem 1.2. □

6. Proof of Theorem 1.3

Consider the central subgroups $\widetilde{C}$ and C of $\Gamma = \mathrm{GL}_{p^{a_1}} \times \dots \times \mathrm{GL}_{p^{a_r}}$ given by

$$\widetilde{C} = \{(\tau_1, \dots, \tau_r) \in \mathbb{G}_m^r \mid \tau_1 \dots \tau_r = 1\} \text{ and } C = \{(\tau_1, \dots, \tau_r) \in \mu \mid \tau_1 \dots \tau_r = 1\}.$$

Set $G := \Gamma/C$ and $\widetilde{G} := \Gamma/\widetilde{C}$. Note that $C = \widetilde{C} \cap \mu$. Thus Theorem A.1 and Corollary A.2 tell us that the functors $H^1(-, \widetilde{G})$ and $H^1(-, G)$ are both isomorphic to the functor $\mathcal{F}$ defined in the statement of Theorem 1.3. In particular, $\mathrm{ed}(\widetilde{G}) = \mathrm{ed}(G) = \mathrm{ed}(\mathcal{F})$ and $\mathrm{ed}_p(\widetilde{G}) = \mathrm{ed}_p(G) = \mathrm{ed}_p(\mathcal{F})$. We are now ready to proceed with the proof of Theorem 1.3.

(a) If $A_1 \otimes \dots \otimes A_r$ is split over K, then A_r can be recovered from $A_1, \dots, A_{r-1}$ as the unique central simple K-algebra of degree p^{a_r} which is Brauer-equivalent to

$$(A_1 \otimes \dots \otimes A_{r-1})^{\mathrm{op}}\,.$$

(Here B^{op} denotes the opposite algebra of B.) In other words, the morphism of functors

$$\mathcal{F} \to H^1(-, \mathrm{PGL}_{p^{a_1}}) \times \dots \times H^1(-, \mathrm{PGL}_{p^{a_{r-1}}}) \tag{20}$$

given by $(A_1, \dots, A_{r-1}, A_r) \to (A_1, \dots, A_{r-1})$ is injective. We claim that if $a_r \geqslant a_1 + \dots + a_{r-1}$ (which is our assumption in part (a)), then this morphism if also surjective. Indeed,

$$\deg(A_1 \otimes \dots \otimes A_{r-1}) = p^{a_1 + \dots + a_{r-1}}$$

for any choice of central simple K-algebras $A_1, \dots, A_{r-1}$ such that $\deg(A_i) = p^{a_i}$. Hence, for any such choice there exists a central simple algebra of degree p^{a_r} which is Brauer-equivalent to $(A_1 \otimes \dots \otimes A_{r-1})^{\mathrm{op}}$. This proves the claim.

We conclude that if $a_r \geqslant a_1 + \dots + a_{r-1}$ then (20) is an isomorphism and thus $\operatorname{ed}(\widetilde{G}) = \operatorname{ed}(G) = \operatorname{ed}(\mathcal{F}) = \operatorname{ed}(\mathrm{PGL}_{p^{a_1}} \times \dots \times \mathrm{PGL}_{p^{a_{r-1}}})$ and

$$\operatorname{ed}_p(\widetilde{G}) = \operatorname{ed}_p(G) = \operatorname{ed}_p(\mathcal{F}) = \operatorname{ed}_p(\mathrm{PGL}_{p^{a_1}} \times \dots \times \mathrm{PGL}_{p^{a_{r-1}}})\,.$$

The inequality $\operatorname{ed}(\mathcal{F}) \leqslant p^{2a_1} + \dots + p^{2a_{r-1}}$ now follows from (9).

(b) Now suppose $a_r < a_1 + \dots + a_{r-1}$. In this case $\mathrm{Code}(C)$ has a minimal basis consisting of the single element $(1, \dots, 1) \in (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$. Moreover, $p^{a_r} \leqslant \frac{1}{2} p^{a_1} \dots p^{a_{r-1}}$ and consequently, Theorem 1.2 applies. It tells us that if the r-tuple $(p^{a_1}, \dots, p^{a_r})$ is not of the form $(2,2,2,2)$, $(3,3,3)$ or $(2, 2^a, 2^a)$, then

$$\operatorname{ed}(\mathcal{F}) = \operatorname{ed}_p(\mathcal{F}) = \operatorname{ed}(\widetilde{G}) = \operatorname{ed}_p(\widetilde{G}) = \operatorname{ed}(G) = \operatorname{ed}_p(G) = p^{a_1 + \dots + a_r} - \sum_{i=1}^{r} p^{2a_i} + r - 1\,,$$

as claimed.

(c) In the case where $(p^{a_1}, \dots, p^{a_r}) = (2,2,2)$, $\mathcal{F}(K)$ is the set of isomorphism classes of triples (A_1, A_2, A_3) of quaternion K-algebras, such that $A_1 \otimes A_2 \otimes A_3$ is split over K. We will show that (i) $\operatorname{ed}(\mathcal{F}) \leqslant 3$ and (ii) $\operatorname{ed}_2(\mathcal{F}) \geqslant 3$.

To prove (i), recall that by a theorem of Albert [Lam05, Theorem III.4.8], the condition that $A_1 \otimes A_2 \otimes A_3$ is split over K implies that A_1 and A_2 are linked over K. That is, there exist $a, b, c \in K^*$ such that $A_1 \simeq (a, b)$ and $A_2 \simeq (a, c)$ over K. Hence, the triple $(A_1, A_2, A_3) \in \mathcal{F}(K)$ descends to the triple $(B_1, B_2, B_3) \in \mathcal{F}(K_0)$, where $K_0 = k(a, b, c)$, $B_1 = (a, b)$, $B_2 = (a, c)$ and $B_3 = (a, bc)$ over K_0. Since $\operatorname{trdeg}(K_0/k) \leqslant 3$, assertion (i) follows.

To prove (ii), consider the morphism of functors $f\colon \mathcal{F} \to H^1(-, \mathrm{SO}_4)$ given by

$$f\colon (A_1, A_2, A_3) \mapsto \alpha\,,$$

where α is a 4-dimensional quadratic form such that

$$\alpha \oplus \mathbb{H} \oplus \mathbb{H} \cong N(A_1) \oplus (-N(A_2))\,.$$

Here $\mathbb{H}$ denotes the 2-dimensional hyperbolic form $\langle 1, -1 \rangle$, $N(A_1)$ denotes the norm form of A_1, and $-N(A_2)$ denotes the opposite norm form of A_2, i.e., the unique 4-dimensional form such that $N(A_2) \oplus (-N(A_2))$ is hyperbolic. Since $N(A_1)$ and $N(A_2)$ are forms of discriminant 1, so is α (this will also be apparent from the explicit computations below). Thus we may view α as an element of the Galois cohomology set $H^1(K, \mathrm{SO}_4)$, which classifies 4-dimensional quadratic forms of discriminant 1 over K, up to isomorphism. Note also that by the Witt Cancellation Theorem, α is unique up to isomorphism. We conclude that the morphism of functors f is well defined.

Equivalently, using the definition of the Albert form given in [Lam05, p. 69], α is the unique 4-dimensional quadratic form such that $\alpha \oplus \mathbb{H} \cong q$, where q is the 6-dimensional Albert form of A_1 and A_2. Here the Albert form of A_1 and A_2 is isotropic, and hence, can be written as $\alpha \oplus \mathbb{H}$, because A_1 and A_2 are linked; once again, see [Lam05, Theorem III.4.8].

Suppose $A_1 = (a, b)$, $A_2 = (a, c)$, and $A_3 = (a, bc)$, as above. Then

$$N(A_1) = \langle\langle -a, -b\rangle\rangle = \langle 1, -a, -b, ab\rangle\,,$$

and similarly $N(A_2) = \langle 1, -a, -c, ac\rangle$; see, e.g., [Lam05, Corollary III.2.2]. Thus

$$N(A_1) \oplus (-N(A_2)) = \langle 1, -1, -a, a, -b, c, ab, -ac\rangle \simeq \langle -b, c, ab, -ac\rangle \oplus \mathbb{H} \oplus \mathbb{H}$$

and we obtain an explicit formula for $\alpha = f(A_1, A_2, A_3)$: $\alpha \cong \langle -b, c, ab, -ac\rangle$.

It is easy to see that any 4-dimensional quadratic form of discriminant 1 over K can be written as $\langle -b, c, ab, -ac\rangle$ for some $a, b, c \in K^*$. In other words, the morphism of functors $f\colon\ \mathcal{F} \to H^1(-, \mathrm{SO}_4)$ is surjective. Consequently,

$$\mathrm{ed}_2(\mathcal{F}) \geq \mathrm{ed}_2(H^1(-, \mathrm{SO}_4)) = \mathrm{ed}_2(\mathrm{SO}_4)\,;$$

see, e.g., [BF03, Lemma 1.9] or [Re10, Lemma 2.2]. On the other hand, $\mathrm{ed}_2(\mathrm{SO}_4) = 3$; see [RY00, Theorem 8.1(2) & Remark 8.2] or [Re10, Corollary 3.6(a)]. Thus

$$\mathrm{ed}_2(\mathcal{F}) \geqslant \mathrm{ed}_2(\mathrm{SO}_4) = 3\,.$$

This completes the proof of (ii) and thus of part (c) and of Theorem 1.3. □

Appendix: Galois Cohomology of central quotients of products of general linear groups

by Athena Nguyen [1]

In this appendix we will study the Galois cohomology of algebraic groups of the form

$$G := \Gamma/C,$$

where $\Gamma := \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$ and $C \subset Z(\Gamma) = \mathbb{G}_m^r$ is a central subgroup. Here $n_1, \ldots, n_r \geqslant 1$ are integers, not necessarily prime powers. Let $\overline{G} := G/Z(G) = \mathrm{PGL}_{n_1} \times \cdots \times \mathrm{PGL}_{n_r} = \Gamma/Z(\Gamma)$. Recall that for any field K/k, $H^1(K, \mathrm{PGL}_n)$ is naturally identified with the set of isomorphism classes of central simple K-algebras of degree n, and

$$H^1(K, \overline{G}) = H^1(K, \mathrm{PGL}_{n_1}) \times \cdots \times H^1(K, \mathrm{PGL}_{n_r})$$

with the set of r-tuples $(A_1, \ldots, A_r)$ of central simple K-algebras such that $\deg(A_i) = n_i$. Denote by ∂_K^i the coboundary map $H^1(K, \mathrm{PGL}_{n_i}) \to H^2(K, \mathbb{G}_m)$ induced by the short exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{GL}_{n_i} \to \mathrm{PGL}_{n_i} \to 1.$$

This map sends a central simple algebra A_i to its Brauer class $[A_i]$ in $H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$.

[1]This appendix is based on a portion of the author's Master's thesis completed at the University of British Columbia. The author gratefully acknowledges the financial support from the University of British Columbia and the Natural Sciences and Engineering Research Council of Canada.

Of particular interest to us will be

$$X(\mathbb{G}_m^r/C) = \{(m_1, \dots, m_r) \in \mathbb{Z}^r \mid \tau_1^{m_1} \dots \tau_r^{m_r} = 1 \ \ \forall (\tau_1, \dots, \tau_r) \in \mathbb{G}_m^r\},$$

as in (6). We are now ready to state the main result of this appendix.

Theorem A.1. *Let $\pi\colon G \to \overline{G} := \mathrm{PGL}_{n_1} \times \dots \times \mathrm{PGL}_{n_r}$ be the natural projection and $\pi_*\colon H^1(K, G) \to H^1(K, \overline{G})$ be the induced map in cohomology. Here K/k is a field extension. Then*

(a) $\pi_*\colon H^1(K, G) \to H^1(K, \overline{G})$ is injective for every field K/k.

(b) π_* identifies $H^1(K, G)$ with the set of isomorphism classes of r-tuples $(A_1, \dots, A_r)$ of central simple K-algebras such that $\deg(A_i) = n_i$ and $A_1^{\otimes m_1} \otimes \dots \otimes A_r^{\otimes m_r}$ is split over K for every $(m_1, \dots, m_r) \in X(\mathbb{G}_m^r/C)$.

Proof. Throughout, we will identify $H^2(K, \mathbb{G}_m^r)$ with $H^2(K, \mathbb{G}_m)^r$ and $X(\mathbb{G}_m^r)$ with $\mathbb{Z}^n$. A character $x = (m_1, \dots, m_r) \in \mathbb{Z}^n$, i.e., a character $x\colon \mathbb{G}_m^r \to \mathbb{G}_m$ given by $(\tau_1, \dots, \tau_r) \to \tau_1^{m_1} \dots \tau_r^{m_r}$, induces a map $x_*\colon H^2(K, \mathbb{G}_m)^r \to H^2(K, \mathbb{G}_m)$ in cohomology given by

$$x_*(\alpha_1, \dots, \alpha_r) = \alpha_1^{m_1} \cdot \dots \cdot \alpha_r^{m_r}. \tag{21}$$

Let us now consider the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{G}_m^r & \longrightarrow & \Gamma & \longrightarrow & \prod_{i=1}^r \mathrm{PGL}_{n_i} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \eta} & & \downarrow & & \| & & \\
1 & \longrightarrow & \mathbb{G}_m^r/C & \longrightarrow & G & \xrightarrow{\pi} & \prod_{i=1}^r \mathrm{PGL}_{n_i} & \longrightarrow & 1.
\end{array}$$

Since $H^1(K, \mathbb{G}_m^r/C) = \{1\}$ by Hilbert's Theorem 90, we obtain the following diagram in cohomology with exact rows:

$$\begin{array}{ccccccc}
 & & H^1(K, \prod_{i=1}^r \mathrm{PGL}_{n_i}) & \xrightarrow{(\partial_K^1, \dots, \partial_K^r)} & H^2(K, \mathbb{G}_m^r) & & \\
 & & \| & & \downarrow{\scriptstyle \eta_*} & & \\
1 \longrightarrow H^1(K, G) & \xrightarrow{\pi_*} & H^1(K, \prod_{i=1}^r \mathrm{PGL}_{n_i}) & \xrightarrow{\partial_K} & H^2(K, \mathbb{G}_m^r/C) & &
\end{array}$$

(a) It follows from [S97, I.5, Proposition 42] that π_* is injective.

(b) Thus, π_* identifies $H^1(K, G)$ with the set of r-tuples $(A_1, \dots, A_r)$, where $A_i \in H^1(K, \mathrm{PGL}_{n_i})$ is a central simple algebra of degree n_i, and $(\partial_K^1(A_1), \dots, \partial_K^r(A_r)) \in \mathrm{Ker}(\eta_*)$. Recall that ∂_K^i sends a central simple algebra A_i to its Brauer class $[A_i] \in H^2(K, \mathbb{G}_m)$. In the sequel we will use additive notation for the abelian group $H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$.

Consider an r-tuple $\alpha := ([A_1], \dots, [A_r]) \in H^2(K, \mathbb{G}_m^r)$. Since $\mathbb{G}_m^r/C$ is diagonalizable, $\eta_*(\alpha) = 0$ if and only if $x_*(\eta_*(\alpha)) = 0$ for all $x \in X(\mathbb{G}_m^r/C)$. If $x = (m_1, \dots, m_r) \in X(\mathbb{G}_m^r/C)$, then $x_* \circ \eta_* = (m_1, \dots m_r) \in X(G_m^r)$. By (21), $x_*(\eta_*(\alpha)) = [A_1^{\otimes m_1} \otimes \dots \otimes A_r^{\otimes m_r}]$, and part (b) follows. □

Corollary A.2. *Let $\Gamma := \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$, C_1, C_2 be k-subgroups of $Z(\Gamma) = \mathbb{G}_m^r$, $G_1 = \Gamma/C_1$ and $G_2 = \Gamma/C_2$. Denote the central subgroup $\mu_{n_1} \times \cdots \times \mu_{n_r}$ of Γ by μ.*

If $C_1 \cap \mu = C_2 \cap \mu$ then the Galois cohomology functors $H^1(-, G_1)$ and $H^1(-, G_2)$ are isomorphic.

Proof. By Theorem A.1, $H^1(K, G_i)$ is naturally identified with the set of r-tuples $(A_1, \dots, A_r)$ of central simple algebras such that $\deg(A_i) = n_i$ and

$$A_1^{\otimes m_1} \otimes \cdots \otimes A_r^{\otimes m_r} \text{ is split over } K \text{ for every } (m_1, \dots, m_r) \in X(\mathbb{G}_m/C_i).$$

Note that since $A_i^{\otimes n_i}$ is split for every i, this condition depends only on the image of $(m_1, \dots, m_r)$ under the natural projection

$$\pi\colon X(\mathbb{G}_m^r) = \mathbb{Z}^r \to (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z}) = X(\mu)\,.$$

Our assumption that $C_1 \cap \mu = C_2 \cap \mu$ is equivalent to $X(\mathbb{G}_m^r/C_1)$ and $X(\mathbb{G}_m^r/C_2)$ having the same image under π, and the corollary follows. □

In order to state the second corollary of Theorem A.1, we will need the following definition. By a code we shall mean a subgroup of $X(\mu) = (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$. Given a subgroup $C \subset \mu$, we define the code $\mathrm{Code}(C) := X(\mu/C)$, as in (8).

We will say that two codes are called *equivalent* if one can be obtained from the other by repeatedly performing the following elementary operations:

(1) Permuting entries i and j in every vector of the code, for any i, j with $n_i = n_j$.

(2) Multiplying the i^{th} entry in every vector of the code by an integer c prime to n_i.

Corollary A.3. *Suppose C_1 and C_2 are subgroups of $\mu := \mu_{n_1} \times \cdots \times \mu_{n_r}$, $G_1 = \Gamma/C_1$ and $G_2 := \Gamma/C_2$. If $\mathrm{Code}(C_1)$ and $\mathrm{Code}(C_2)$ are equivalent, then*

(a) the Galois cohomology functors $H^1(-, G_1)$ and $H^1(-, G_2)$ are isomorphic, and

(b) in particular, $\mathrm{ed}(G_1) = \mathrm{ed}(G_2)$ and $\mathrm{ed}_p(G_1) = \mathrm{ed}_p(G_2)$ for every prime p.

Proof. (a) It suffices to show that $H^1(-, G_1)$ and $H^1(-, G_2)$ are isomorphic if C_2 is obtained from C_1 by an elementary operation.

(1) Suppose $n_i = n_j$ for some $i, j = 1, \dots, r$, and $\mathrm{Code}(C_2)$ is obtained from $\mathrm{Code}(C_1)$ by permuting entries i and j in every vector. In this case $C_2 = \alpha(C_1)$, where α is the automorphism of $\Gamma = \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$ which swaps the ith and the jth components. Then α induces an isomorphism between $G_1 = \Gamma/C_1$ and $G_2 = \Gamma/C_2$, and thus an isomorphism between $H^1(-, G_1)$ and $H^1(-, G_2)$.

(2) Now suppose that $\mathrm{Code}(C_1)$ is obtained from $\mathrm{Code}(C_2)$ by multiplying the i^{th} entry in every vector by some $c \in (\mathbb{Z}/n_i\mathbb{Z})^*$. The description of $H^1(K, G/\mu)$ given by Theorem A.1 now tells us that

$$\begin{aligned} H^1(K, G_1) &\to H^1(K, G_2) \\ (A_1, \dots, A_r) &\mapsto (A_1, \dots, A_{i-1}, [A_i^{\otimes c}]_{n_i}, A_{i+1}, \dots, A_r) \end{aligned}$$

is an isomorphism. Here, by $[A_i^{\otimes c}]_{n_i}$ we mean the unique central simple K-algebra of degree n_i which is Brauer equivalent to $A_i^{\otimes c}$.

(b) follows from (a), because $\mathrm{ed}(G)$ and $\mathrm{ed}_p(G)$ are defined entirely in terms of the Galois cohomology functor $H^1(-, G)$. □

References

[ABGV11] A. Auel, E. Brussel, E. Garibaldi, U. Vishne, *Open problems on central simple algebras*, Transform. Groups **16** (2011), no. 1, 219–264. MR2785502 (2012e:16050)

[BF03] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330. MR2029168 (2004m:11056)

[BM12] S. Baek and A. S. Merkurjev, *Essential dimension of central simple algebras*, Acta Math. **209** (2012), no. 1, 1–27. MR2979508

[BRV12] P. Brosnan, Z. Reichstein and A. Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1079–1112. MR2800485 (2012g:14012)

[KM08] N. A. Karpenko and A. S. Merkurjev, Essential dimension of finite p-groups, Invent. Math. **172** (2008), no. 3, 491–508. MR2393078 (2009b:12009)

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, 67, Amer. Math. Soc., Providence, RI, 2005. MR2104929 (2005h:11075)

[Lang02] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer, New York, 2002. MR1878556 (2003e:00003)

[Le04] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379. MR2105732 (2005j:20056)

[Lö13] R. Lötscher, A fiber dimension theorem for essential and canonical dimension, Compos. Math. **149** (2013), no. 1, 148–174. MR3011881

[LMMR13] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein, *Essential dimension of algebraic tori*, J. Reine Angew. Math. **677** (2013), 1–13. MR3039772

[LRRS03] M. Lorenz, Z. Reichstein, L. H. Rowen, D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670. MR2009442 (2004j:16022)

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland, Amsterdam, 1977. MR0465509 (57 #5408a)

[M13] A. S. Merkurjev, *Essential dimension: a survey.* Transform. Groups **18** (2013), no. 2, 415–481. MR3055773

[Pr67] C. Procesi, *Non-commutative affine rings*, Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8) **8** (1967), 237–255. MR0224657 (37 #256)

[P87] A. M. Popov, *Finite isotropy subgroups in general position of irreducible semisimple linear Lie groups* (in Russian), Trudy Moskov. Mat. Obshch. **50** (1987), 209–248, 262; English translation in Trans. Moscow Math. Soc. **1988**, 205–249. MR0912058 (89a:20049)

[PV94] V. L. Popov and E. B. Vinberg, *Invariant Theory*, in Algebraic geometry. IV, Encyclopaedia of Mathematical Sciences, 55, Springer, Berlin, 1994, 123–284. MR1309681 (95g:14002)

[RV07] Z. Reichstein and N. Vonessen, *Tame group actions on central simple algebras*, J. Algebra **318** (2007), no. 2, 1039–1056. MR2371986 (2008j:16061)

[RY00] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056. MR1782331 (2001k:14088)

[Re99] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canad. J. Math. **51** (1999), no. 1, 69–95. MR1692919 (2000h:12008)

[Re10] Z. Reichstein, *Essential dimension*, in Proceedings of the International Congress of Mathematicians. Volume II, 162–188, Hindustan Book Agency, New Delhi. MR2827790 (2012g:11074)

[Re12] Z. Reichstein, *What is...essential dimension?*, Notices Amer. Math. Soc. **59** (2012), no. 10, 1432–1434. MR3025902

[Ri72] R. W. Richardson, Jr., *Principal orbit types for algebraic transformation spaces in characteristic zero*, Invent. Math. **16** (1972), 6–14. MR0294336 (45 #3405)

[Sh71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. MR0314766 (47 #3318)

[S97] J.-P. Serre, *Galois cohomology*, translated from the French by Patrick Ion and revised by the author, Springer, Berlin, 1997. MR1466966 (98g:12007)

Department of Mathematics, University of British Columbia, Vancouver, BC, Canada, V6T 1Z2

E-mail address: shane.cernele@gmail.com, reichst@math.ubc.ca, athena@math.ubc.ca