# AN UPPER BOUND ON THE ESSENTIAL DIMENSION OF A CENTRAL SIMPLE ALGEBRA

AUREL MEYER† AND ZINOVY REICHSTEIN††

Abstract. We prove a new upper bound on the essential $p$-dimension of the projective linear group $\mathrm{PGL}_n$.

Contents



## 1. Introduction

Let $k$ be a base field; all other fields will be assumed to be extensions of $k$.

Given a central simple algebra $A$ over a field $K$ one can ask whether $A$ can be written as $A = A_0 \otimes_{K_0} K$ where $A_0$ is a central simple algebra over some subfield $K_0$ of $K$. In that situation we say that $A$ *descends* to $K_0$. The *essential dimension* of $A$, denoted $\mathrm{ed}(A)$, is the minimal transcendence degree over $k$ of a field $K_0 \subset K$ such that $A$ descends to $K_0$. It can be thought of as "the minimal number of independent parameters" required to define $A$.

For a prime number $p$, the related notion of essential dimension at $p$ of an algebra $A/K$ is defined as $\mathrm{ed}(A; p) = \min \mathrm{ed}(A_{K'})$, where $K'/K$ runs over all finite field extensions of degree prime to $p$.

---

2000 *Mathematics Subject Classification.* 16K20, 20C10.

*Key words and phrases.* Essential dimension, central simple algebra, projective linear group, $G$-lattice.

† Aurel Meyer was partially supported by a University Graduate Fellowship at the University of British Columbia.

†† Z. Reichstein was partially supported by NSERC Discovery and Accelerator Supplement grants.

We also define
$$\mathrm{ed}(\mathrm{PGL}_n) := \mathbf{max}\,\{\,\mathrm{ed}(A)\,\}\,,$$
and
$$\mathrm{ed}(\mathrm{PGL}_n;p) := \mathbf{max}\,\{\,\mathrm{ed}(A;p)\,\}\,,$$
where the maximum is taken over all fields $K/k$ and over all central simple $K$-algebras $A$ of degree $n$. The appearance of $\mathrm{PGL}_n$ in the symbols $\mathrm{ed}(\mathrm{PGL}_n)$ and $\mathrm{ed}(\mathrm{PGL}_n;p)$ has to do with the fact that central simple algebras of degree $n$ are in a natural bijective correspondence with $\mathrm{PGL}_n$-torsors. In fact, one can define $\mathrm{ed}(G)$ and $\mathrm{ed}(G;p)$ for every algebraic $k$-group $G$ in a similar manner, using $G$-torsors instead of central simple algebras; see [Re$_2$], [RY] or [BF].

To the best of our knowledge, the problem of computing $\mathrm{ed}(\mathrm{PGL}_n)$ was first raised by C. Procesi in the 1960s. Procesi and S. Amitsur constructed so-called *universal division algebras* $\mathrm{UD}(n)$ and showed that $\mathrm{UD}(n)$ has various generic properties among central simple algebras of degree $n$. In particular, their arguments can be used to show that
$$\mathrm{ed}(\mathrm{UD}(n)) \geq \mathrm{ed}(A) \text{ and } \mathrm{ed}(\mathrm{UD}(n);p) \geq \mathrm{ed}(A;p)$$
for any prime integer $p$; cf. [LRRS, Remark 2.8]. Equivalently,
$$\mathrm{ed}(\mathrm{UD}(n)) = \mathrm{ed}(\mathrm{PGL}_n) \text{ and } \mathrm{ed}(\mathrm{UD}(n);p) = \mathrm{ed}(\mathrm{PGL}_n;p).$$
Since the center of $\mathrm{UD}(n)$ has transcendence degree $n^2+1$ over $k$, we conclude that $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2+1$. Procesi showed (using different terminology) that in fact,
$$\mathrm{ed}(\mathrm{PGL}_n) \leq n^2\,;$$
see [Pr, Theorem 2.1].

The problem of computing $\mathrm{ed}(\mathrm{PGL}_n)$ was raised again by B. Kahn in the early 1990s. In particular, in 1992 Kahn asked the second author if $\mathrm{ed}(\mathrm{PGL}_n)$ grows sublinearly in $n$, i.e., whether
$$\mathrm{ed}(\mathrm{PGL}_n) \leq an + b$$
for some positive real numbers $a$ and $b$. To the best of our knowledge, this question never appeared in print but it is implicit in [Ka, Section 2]. It remains open; the best known upper bound,
$$\mathrm{ed}(\mathrm{PGL}_n) \leq \begin{cases} \frac{(n-1)(n-2)}{2}, \text{ for every odd } n \geq 5 \text{ and} \\ n^2-3n+1, \text{ for every } n \geq 4 \end{cases} \tag{1}$$
(see [LR], [LRRS, Theorem 1.1], [Le, Proposition 1.6] and [FF]), is quadratic in $n$ and the best known lower bound,
$$\mathrm{ed}(\mathrm{PGL}_{p^r}) \geq \mathrm{ed}(\mathrm{PGL}_{p^r};p) \geq 2r\,,$$
is logarithmic.

Note that if $p^s$ is the largest power of $p$ dividing $n$ then one easily checks, using primary decomposition of central simple algebras, that $\mathrm{ed}(\mathrm{PGL}_n;p) =$

$\mathrm{ed}(\mathrm{PGL}_{p^s};p)$. Thus for the purpose of computing $\mathrm{ed}(\mathrm{PGL}_n;p)$ it suffices to consider the case where $n = p^s$. In this case we have showed that

$$\mathrm{ed}(\mathrm{PGL}_{p^s};p) \le p^{2s-1} - p^s + 1$$

for any $s \ge 2$; see [MR, Corollary 1.2]. The main result of this paper is the following stronger upper bound.

**Theorem 1.1.** *Let $n = p^s$ for some $s \ge 2$. Then*

$$\mathrm{ed}(\mathrm{PGL}_n;p) \le 2\frac{n^2}{p^2} - n + 1$$

A. S. Merkurjev [$\mathrm{Me}_2$] recently showed that for $s = 2$ this bound is sharp, i.e., $\mathrm{ed}(\mathrm{PGL}_{p^2};p) = p^2 + 1$. We conjecture that this bound is sharp for every $s \ge 2$; this would imply, in particular, that $\mathrm{ed}(\mathrm{PGL}_n)$ is not sublinear in $n$.

Our upper bound on $\mathrm{ed}(\mathrm{PGL}_n;p)$ is a consequence of the following result. Here $n$ is not assumed to be a prime power.

**Theorem 1.2.** *Let $A/K$ be a central simple algebra of degree $n$. Suppose $A$ contains a field $F$, Galois over $K$ and $\mathrm{Gal}(F/K)$ can be generated by $r \ge 1$ elements. If $[F : K] = n$ then we further assume that $r \ge 2$. Then*

$$\mathrm{ed}(A) \le r\frac{n^2}{[F : K]} - n + 1$$

Note that we always have $[F : K] \le n$. In the special case where equality holds, i.e., $A$ is a crossed product in the usual sense, Theorem 1.2 reduces to [LRRS, Corollary 3.10(a)].

To deduce Theorem 1.1 from Theorem 1.2, let $n = p^s$ and $A = \mathrm{UD}(n)$. In [$\mathrm{RS}_1$, 1.2], L. H. Rowen and D. J. Saltman showed that if $s \ge 2$ then there is a finite field extension $K'/K$ of degree prime to $p$, such that $A' := A \otimes_K K'$ contains a field $F$, Galois over $K'$ with $\mathrm{Gal}(F/K') \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. Thus, if $s \ge 2$, Theorem 1.2 tells us that

$$\mathrm{ed}(\mathrm{PGL}_n;p) = \mathrm{ed}(A;p) \le \mathrm{ed}(A') \le 2\frac{n^2}{p^2} - n + 1\,.$$

This proves Theorem 1.1. □

The remainder of this paper will be devoted to proving Theorem 1.2. We reduce the problem to a question about $G$-lattices, using the same approach as in [LRRS, Sections 2–3], but our analysis is more delicate here, and the results (Theorems 1.2 and 4.1) are stronger.

## 2. $G/H$-crossed products

**Lemma 2.1.** *In the course of proving Theorem 1.2 we may assume without loss of generality that $F$ is contained in a subfield $L$ of $A$ such that $L/K$ is a separable extension of degree $n = \deg(A)$.*

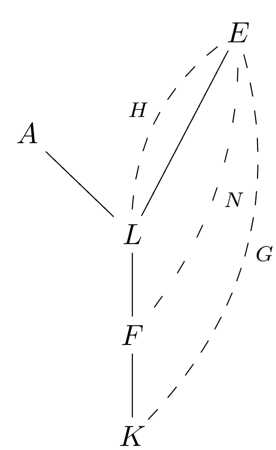
*Proof.* Note that we are free to replace $K$ by $K(t)$, $F$ by $F(t)$ and $A$ by $A(t) = A \otimes_K K(t)$, where $t$ is an independent variable. Indeed, $\mathrm{ed}_k\, A(t) = \mathrm{ed}_k(A)$; see, e.g., [LRRS, Lemma 2.7(a)]. Thus if the inequality of Theorem 1.2 is proved for $A(t)$, it will also hold for $A$.

The advantage of passing from $A$ to $A(t)$ is that $K(t)$ if Hilbertian for any infinite field $K$; see, e.g., [FJ, Proposition 13.2.1]. Thus after adjoining two variables, $t_1$ and $t_2$ as above, we may assume without loss of generality that $K$ is Hilbertian. (Note that a subfield $L \subset A$ of degree $n$ over $K$ may not exist without this assumption.)

Let $F \subset F'$ be maximal among separable field extension of $F$ contained in $A$. We will look for $L$ inside the centralizer $C_A(F')$. By the Double Centralizer Theorem, $C_A(F')$ is a central simple algebra with center $F'$. The maximality of $F'$ tells us that $C_A(F')$ contains no non-trivial field extensions of $F'$. In particular, $C_A(F') = \mathrm{M}_r(F')$, where $r[F' : K] = n$.

On the other hand, since $K$ is Hilbertian, so is its finite separable extension $F'$; cf. [FJ, 12.2.3]. Consequently, $F'$ admits a finite separable extension $L/F'$ of degree $r$. (To construct $L/F'$, start with the field extension $L_r = F'(t_1, \dots, t_r)[x]/(f(x))$ of $F'(t_1, \dots, t_n)$ of degree $r$, where $f(x) = x^r + t_1 x^{r-1} + \dots + t_{n-1}x + t_n$ is the general polynomial of degree $r$. Then specialize $t_1, \dots, t_r$ in $F'$, using the Hilbertian property, to obtain a field extension $L/F'$ of degree $r$.) Any such $L/F'$ can be embedded into $\mathrm{M}_r(F')$ via the regular representation of $L$ on $L = (F')^r$; cf. [Pi, Lemma 13.1a]. By the maximality of $F'$, we conclude that $L = F'$, i.e., $r = 1$ and $[L : K] = n$, as desired. □

Let us now assume that our central simple algebra $A/K$ has a separable maximal subfield $L/K$, as in Lemma 2.1. We will denote the Galois closure of $L$ over $K$ by $E$ and the associated Galois groups by $G = \mathrm{Gal}(E/K)$, $H = \mathrm{Gal}(E/L)$ and $N = \mathrm{Gal}(E/F)$, as in the diagram below.




In the terminology of [LRRS], $A/K$ is a $G/H$-crossed product; cf. also [FSS, Appendix]. Note that since $E/K$ is the smallest Galois extension containing

$L/K$, we have

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g = \{1\}\,. \tag{2}$$

where $H^g := gHg^{-1}$. We will assume that this condition is satisfied whenever we talk about $G/H$-crossed products.

Using the notation introduced above and remembering that $[G : H] = [L : K] = \deg(A) = n$, and $\dfrac{n}{[F : K]} = [L : F] = [N : H]$, we can restate Theorem 1.2 as follows.

**Theorem 2.2.** *Let $A$ be a $G/H$-crossed product. Suppose $H$ is contained in a normal subgroup $N$ of $G$ and $G/N$ is generated by $r$ elements. Furthermore, assume that either $H \neq \{1\}$ or $r \geq 2$. Then*

$$\mathrm{ed}(A) \leq r[G : H] \cdot [N : H] - [G : H] + 1\,.$$

## 3. $G$-lattices

In the sequel $H \leq G$ will be finite groups. Given $g \in G$ we will write $\overline{g}$ for the left coset $gH$ of $H$. We will denote the identity element of $G$ by 1.

Recall that a $G$-lattice $M$ is a (left) $\mathbb{Z}[G]$-module, which is free of finite rank over $\mathbb{Z}$. In particular, any finite set $X$ with a $G$-action gives rise to a $G$-lattice $\mathbb{Z}[X]$; $G$-lattices of this form are called *permutation*. For background material on $G$-lattices we refer the reader to [Lo].

Of particular interest to us will be the $G$-lattice $\omega(G/H)$, which is defined as the kernel of the natural augmentation map $\mathbb{Z}[G/H] \to \mathbb{Z}$, sending $n_1\overline{g_1} + \cdots + n_s\overline{g_s}$ to $n_1 + \cdots + n_s$.

The starting point for our proof of Theorem 2.2 (and hence, of Theorem 1.2) will be the following result from [LRRS].

**Theorem 3.1.** ([LRRS, Theorem 3.5]) *Let $P$ be a permutation $G$-lattice and*

$$0 \to M \to P \to \omega(G/H) \to 0$$

*be an exact sequence of $G$-lattices. If the $G$-action on $M$ is faithful then*

$$\mathrm{ed}(A) \leq \mathrm{rank}(M) - n + 1$$

*for any $G/H$-crossed product $A$.* □

The condition that $G$ acts faithfully on $M$ is not automatic. However, the following lemma shows that it is satisfied for many natural choices of $P$.

**Lemma 3.2.** *Let $G \neq \{1\}$ be a finite group $H \leq G$ be a subgroup of $G$, $H_1, \ldots, H_r$ be subgroups of $H$ and*

$$0 \to M \to \oplus_{i=1}^{r} \mathbb{Z}[G/H_i] \to \omega(G/H) \to 0 \tag{3}$$

*be an exact sequence of $G$-lattices. Assume that $H$ does not contain any nontrivial normal subgroup of $G$ (i.e., $H$ satisfies condition (2) above). Then the $G$-action on $M$ fails to be faithful if and only if $s = 1$ and $H_1 = H$.*

Here we are not specifying the map $\oplus_{i=1}^{r}\mathbb{Z}[G/H_i] \to \omega(G/H)$; the lemma holds for any exact sequence of the form (3). We also note that in the case where $H_1 = \cdots = H_r = \{1\}$, Lemma 3.2 reduces to [LRRS, Lemma 2.1].

*Proof.* To determine whether or not the $G$-action on $M$ is faithful, we may replace $M$ by $M_{\mathbb{Q}} := M \otimes \mathbb{Q}$. After tensoring with $\mathbb{Q}$, the sequence (3) splits, and we have an isomorphism

$$\omega(G/H)_{\mathbb{Q}} \oplus M_{\mathbb{Q}} \simeq \oplus_{i=1}^{r}\mathbb{Q}[G/H_i]\,. \tag{4}$$

Case 1: $r \geq 2$. Then $H_r$ is a subgroup of $H$, we have a natural surjective map $\mathbb{Q}[G/H_r] \to \mathbb{Q}[G/H]$. Using complete irreducibility over $\mathbb{Q}$ once again, we see that $\mathbb{Q}[G/H]$ (and hence $\omega(G/H)$) is a subrepresentation of $\mathbb{Q}[G/H_r]$. Thus (4) tells us that $\mathbb{Q}[G/H_{r-1}]$ is a subrepresentation of $M_{\mathbb{Q}}$. The kernel of the $G$-representation on $\mathbb{Q}[G/H_{r-1}]$ is a normal subgroup of $G$ contained in $H_{r-1}$ (and hence, in $H$); by our assumption on $H$, any such subgroup is trivial. This shows that $G$ acts faithfully on $\mathbb{Q}[G/H_{r-1}]$ and hence, on $M$.

Case 2: Now assume $r = 1$. Our exact sequence now assumes the form

$$0 \to M_{\mathbb{Q}} \to \mathbb{Q}[G/H_1] \to \omega(G/H)_{\mathbb{Q}} \to 0\,.$$

If $H = H_1$ then $M \simeq \mathbb{Z}$, with trivial (and hence, non-faithful) $G$-action.

Our goal is thus to show that if $H_1 \subsetneq H$ then the $G$-action on $M_{\mathbb{Q}}$ is faithful. Denote by $\mathbb{Q}[1]$ the trivial representation (it will be clear from the context of which group). Observe that

$$\begin{aligned}
\mathbb{Q}[G/H_1] &\simeq \operatorname{Ind}_{H_1}^{G}\mathbb{Q}[1] \simeq \operatorname{Ind}_{H}^{G}\operatorname{Ind}_{H_1}^{H}\mathbb{Q}[1] \simeq \operatorname{Ind}_{H}^{G}\mathbb{Q}[H/H_1] \\
&\simeq \operatorname{Ind}_{H}^{G}(\omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[1]) \\
&\simeq \operatorname{Ind}_{H}^{G}\omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[G/H] \\
&\simeq \operatorname{Ind}_{H}^{G}\omega(H/H_1)_{\mathbb{Q}} \oplus \omega(G/H)_{\mathbb{Q}} \oplus \mathbb{Q}[1]
\end{aligned}$$

and we obtain

$$M_{\mathbb{Q}} \simeq \operatorname{Ind}_{H}^{G}\omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[1]\,.$$

If $H_1 \subsetneq H$ then the kernel of the $G$-representation $\operatorname{Ind}_{H}^{G}\omega(H/H_1)_{\mathbb{Q}}$ is a normal subgroup of $G$ contained in $H_1$ (and hence, in $H$). By our assumption on $H$, this kernel is trivial. □

## 4. An upper bound

In this section we will prove the following upper bound on the essential dimension of a $G/H$-crossed product.

We will say that $g_1, \ldots, g_s \in G$ generate $G$ over $H$ if $G = \langle g_1, \ldots, g_s, H\rangle$.

**Theorem 4.1.** *Let $A$ be a $G/H$-crossed product. Suppose that*

*(i) $g_1, \ldots, g_s \in G$ generate $G$ over $H$, and*

*(ii) if $G$ is cyclic then $H \neq \{1\}$.*

*Then* $\operatorname{ed}(A) \leq \sum_{i=1}^{s}[G : (H \cap H^{g_i})] - [G : H] + 1$.

**Remark 4.2.** The index $[G : (H \cap H^{g_i})]$ appearing in the above formula can be rewritten as

$$[G : H] \cdot [H : (H \cap H^{g_i})] = [G : H] \cdot [(H \cdot H^{g_i}) : H]\,;$$

see, e.g., [Ro, 1.3.11(i)]. Note $H \cdot H^g := \{hh' \,|\, h \in H,\ h' \in H^g\}$ is a subset of $G$ but may not be a subgroup, and $[(H \cdot H^g) : H]$ is defined as $\dfrac{|H \cdot H^g|}{|H|}$.

If $H$ is contained in a normal subgroup $N$ of $G$ then clearly $H \cdot H^g$ lies in $N$, each $[H \cdot H^g : H] \leq [N : H]$ and thus Theorem 4.1 yields

$$\mathrm{ed}(A) \leq s[G : H] \cdot [N : H] - [G : H] + 1\,.$$

This is a bit weaker than the inequality of Theorem 2.2, even though the two look very similar. The difference is that we have replaced $r$ in the inequality of Theorem 2.2 by $s$, where $G$ is generated by $s$ elements over $H$ and by $r$ elements over $N$. A priori $r$ can be smaller than $s$. Nevertheless in the next section we will deduce Theorem 2.2 from Theorem 4.1 by a more delicate argument along these lines.

Our proof of Theorem 4.1 will rely on the following lemma.

**Lemma 4.3.** *Let $V$ be a $\mathbb{Z}[G]$-submodule of $\omega(G/H)$. Then*

$$G_V := \{g \in G \,|\, \overline{g} - \overline{1} \in V\}$$

*is a subgroup of $G$ containing $H$.*

*Proof.* The inclusion $H \subset G_V$ is obvious from the definition.

To see that $G_V$ is closed under multiplication, suppose $g, g' \in G_V$. That is, both $\overline{g} - \overline{1}$ and $\overline{g'} - \overline{1}$ lie in $V$. Then

$$\overline{gg'} - \overline{1} = g \cdot (\overline{g'} - \overline{1}) + (\overline{g} - \overline{1})$$

also lies in $V$, i.e., $gg' \in G_V$, as desired. □

*Proof of Theorem 4.1.* We claim that the elements $\overline{g_1} - \overline{1}, \ldots, \overline{g_s} - \overline{1}$ generate $\omega(G/H)$ as a $\mathbb{Z}[G]$-module.

Indeed, let $V$ be the $\mathbb{Z}[G]$-submodule of $\omega(G/H)$ generated by these elements. Lemma 4.3 and condition (i) tell us that $V$ contains $\overline{g} - \overline{1}$ for every $g \in G$. Translating these elements by $G$, we see that $V$ contains $\overline{a} - \overline{b}$ for every $a, b \in G$. Hence, $V = \omega(G/H)$, as claimed.

For $i = 1, \ldots, s$, let

$$S_i := \{g \in G \,|\, g \cdot (\overline{g_i} - \overline{1}) = \overline{g_i} - \overline{1}\}$$

be the stabilizer of $\overline{g_i} - \overline{1}$ in $G$. We may assume here that $g_i$ is not in $H$, otherwise it could be removed since it is not needed to generate $G$ over $H$. Then clearly $g \in S_i$ iff $\overline{gg_i} = \overline{g_i}$ and $\overline{g} = \overline{1}$. From this one easily sees that $S_i = H \cap H^{g_i}$. Thus we have an exact sequence

$$0 \to M \to \oplus_{i=1}^{s} \mathbb{Z}[G/S_i] \xrightarrow{\phi} \omega(G/H) \to 0$$

where $\phi$ sends a generator of $\mathbb{Z}[G/S_i]$ to $\overline{g_i} - \overline{1} \in \omega(G/H)$. By Theorem 3.1 it remains to show that $G$ acts faithfully on $M$.

By Lemma 3.2 $G$ fails to act faithfully on $M$ if and only if $r = 1$ and $S_1 = H = H^{g_1}$. But this possibility is ruled out by (ii). Indeed, assume that $s = 1$ and $S_1 = H = H^{g_1}$. Then $G = \langle g_1, H \rangle$ and $H = H^{g_1}$. Hence, $H$ is normal in $G$. Condition (2) then tells us that $H = \{1\}$. Moreover, in this case $G = \langle g_1, H \rangle = \langle g_1 \rangle$ is cyclic, contradicting (ii). □

## 5. Proof Theorem 1.2

As we saw above, it suffices to prove Theorem 2.2.

Let $t_1, \ldots, t_r \in G/N$ be a set of generators for $G/N$. Choose $g_1, \ldots, g_r \in G$ representing $t_1, \ldots, t_r$. and let $H' := \langle H, H^{g_1}, \ldots, H^{g_r} \rangle$. Since $H \leq N$ and $N$ is normal in $G$, $H' \leq N$. The group $H'$ depends on the choice of $g_1, \ldots, g_r \in G$, so that $g_i N = t_i$. Fix $t_1, \ldots, t_r$ and choose $g_1, \ldots, g_r \in G$ representing them, so that $H'$ has the largest possible order or equivalently the smallest possible index in $N$. Denote this minimal possible value of $[N : H']$ by $m$. In particular

$$m = [N : H'] \leq [N : (H^{g_i g} \cdot H)] \tag{5}$$

for any $i = 1, \ldots, r$ and any $g \in N$. Here $[N : (H^{g_i g} \cdot H)] = \dfrac{|N|}{|H^{g_i g} \cdot H|}$, as in Remark 4.2.

Choose a set of representatives $1 = n_1, n_2, \ldots, n_m \in N$ for the distinct left cosets of $H'$ in $N$. We claim that the elements

$$\{g_i n_j \,|\, i = 1, \ldots, r;\ j = 1, \ldots, m\}$$

generate $G$ over $H$. Indeed, let $G_0$ be the subgroup of $G$ generated by these elements and $H$. Since $n_1 = 1$, $G_0$ contains $g_1, \ldots, g_r$. Hence, $G_0$ contains $H'$. Moreover, $G_0$ contains $n_j = g_1^{-1}(g_1 n_j)$ for every $j$; hence, $G_0$ contains all of $N$. Finally, since $t_1 = g_1 N, \ldots, t_r = g_r N$ generate $G/N$, we conclude that $G_0$ contains all of $G$. This proves the claim.

We now apply Theorem 4.1 to the elements $\{g_i n_j\}$. Substituting

$$[G : H] \cdot [H : (H \cdot H^{g_i n_j})] \text{ for } [G : (H \cap H^{g_i n_j})],$$

as in Remark 4.2, we obtain

$$
\begin{aligned}
\operatorname{ed}(A) \leq & \quad \sum_{i=1}^{r}\sum_{j=1}^{m}[G:(H\cap H^{g_i n_j})] - [G:H] + 1 \\
= & \quad [G:H]\cdot\sum_{i=1}^{r}\sum_{j=1}^{m}[(H\cdot H^{g_i n_j}):H] - [G:H] + 1 \\
= & \quad [G:H]\cdot\sum_{i=1}^{r}\sum_{j=1}^{m}\frac{[N:H]}{[N:(H\cdot H^{g_i n_j})]} - [G:H] + 1 \\
\leq & \quad (\text{by } (5)) \quad [G:H]\cdot\sum_{i=1}^{r}\sum_{j=1}^{m}\frac{[N:H]}{m} - [G:H] + 1 \\
= & \quad r[G:H]\cdot[N:H] - [G:H] + 1
\end{aligned}
$$

as desired. This completes the proof of Theorem 2.2 and thus of Theorem 1.2. □

## Acknowledgments

The authors are grateful to B. A. Sethuraman, D. J. Saltman, and B. Totaro for helpful comments.

## References


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

[FF] G. Favi, M. Florence, *Tori and essential dimension.* J. Algebra **319** (2008), no. 9, 3885–3900.

[FSS] B. Fein, D. J. Saltman, M. Schacher, *Embedding problems for finite-dimensional division algebras*, J. Algebra **167** (1994), no. 3, 588–626.

[FJ] M. D. Fried, M. Jarden, *Field arithmetic*, third edition. Springer-Verlag, Berlin, 2008.

[Ka] B. Kahn, *Comparison of some field invariants*, J. Algebra **232** (2000), no. 2, 485–492.

[Le] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.

[Lo] M. Lorenz, Multiplicative invariant theory. Encyclopaedia of Mathematical Sciences, 135. Invariant Theory and Algebraic Transformation Groups, VI. Springer-Verlag, Berlin, 2005.

[LR] M. Lorenz, Z. Reichstein, *Lattices and parameter reduction in division algebras*, MSRI Preprint 2000-001, `http://www.msri.org/publications/preprints/online/2000-001.html`

[LRRS] 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.

[$\mathrm{Me}_2$] A. S. Merkurjev, *Essential p-dimension of* $\mathrm{PGL}(p^2)$, preprint, `http://www.math.uni-bielefeld.de/LAG/man/313.html`

[MR] A. Meyer, Z. Reichstein *The essential dimension of the normalizer of a maximal torus in the projective linear group*, To appear in Algebra and Number Theory.

[Pi] R. S. Pierce, *Associative algebras*, Springer-Verlag, New York-Berlin, 1982.

[Pr] C. Procesi, *Non-commutative affine rings*, Atti Acc. Naz. Lincei, S. VIII, v. VIII, fo. 6 (1967), 239–255.

[$Re_1$] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canad. J. Math. **51** (1999), no. 1, 69–95.

[$Re_2$] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.

[RY] Z. Reichstein, B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by János Kollár and Endre Szabó, Canad. J. Math. **52** (2000), no. 5, 1018–1056,

[Ro] D. J. S. Robinson, *A course in the theory of groups*, second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[$RS_1$] L. H. Rowen, D. J. Saltman, *Prime-to-p extensions of division algebras*, Israel J. Math. **78** (1992), no. 2-3, 197–207.

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