

Algebra & Number Theory

Volume 20
2026
No. 2

**On the minimal dimension of a faithful linear representation of a
finite group**

Alexander Moretó



On the minimal dimension of a faithful linear representation of a finite group

Alexander Moretó

The representation dimension of a finite group G is the minimal dimension of a faithful complex linear representation of G . We prove that the representation dimension of any finite group G is at most $\sqrt{|G|}$ except if G is a 2-group with elementary abelian center of order 8 and all irreducible characters of G whose kernel does not contain $Z(G)$ are fully ramified with respect to $G/Z(G)$. We also obtain bounds for the representation dimension of quotients of G in terms of the representation dimension of G , and discuss the relation of this invariant with the essential dimension of G .

1. Introduction

Given a positive integer n , the study of the (finite complex) linear groups of degree n has been a classical theme of research in finite group theory. For instance, in 1878, C. Jordan proved that if G is a linear group of degree n , then there exists $A \trianglelefteq G$ abelian such that $|G : A| \leq j(n)$ for some integer valued function $j(n)$ (see [33] for a modern classification-free proof of this theorem and for a description of earlier proofs.) After the classification of finite simple groups was completed, sharp bounds for the function $j(n)$ were found by M. Collins [11] in 2008, improving on an earlier unpublished manuscript by B. Weisfeiler.

Following [10], let $\text{rdim } G$ be the minimal integer such that a finite group G embeds into $\text{GL}(\text{rdim } G, \mathbb{C})$, i.e., $\text{rdim } G$ is the smallest integer n such that a finite group G is a linear group of degree n . This was called the representation dimension in [10]. Clearly, $\text{rdim } G \leq |G|$. Surprisingly, this natural invariant of a finite group has not been very studied from a group-theoretic point of view. Recently, it has been proven to be very relevant in a large number of areas outside finite group representation theory. See for instance the preface of [35] for its relevance in group cohomology theory, or [6; 17] for its role in showing that certain Cayley graphs are expander graphs. All the nontrivial results we are aware of on $\text{rdim } G$ when G is not close to a simple group have been motivated by the so-called essential dimension of a finite group $\text{ed}(G)$. This concept was introduced in 1997 by J. Buhler and Z. Reichstein in [7] with

The author's research is supported by Ministerio de Ciencia e Innovación (Grants PID2019-103854GB-I00 and PID2022-137612NB-I00 funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe") and Generalitat Valenciana (AICO/2020/298 and CIAICO/2021/163). I thank D. Holt, Z. Reichstein and G. Robinson for helpful comments; in particular, Z. Reichstein asked the question that led to Theorem D. I am also indebted to D. Rae for pointing out an earlier mistake. Last, but not least, I thank the referee for a careful reading of this paper, many helpful suggestions and pointing out an omitted case.

MSC2020: primary 20C15; secondary 14E07, 12F10.

Keywords: representation dimension, essential dimension, faithful representation.

motivations from algebraic geometry. Since then it has found applications in a large number of areas (see [28; 29]). It is known that $\text{ed}(G) \leq \text{rdim } G$ (see Proposition 4.15 of [3]). Both $\text{ed}(G)$ and $\text{rdim } G$ depend on the field over which we are considering the representations of G and are of interest over arbitrary fields. For simplicity, in this note we will restrict ourselves to the field of complex numbers, although our arguments work over any field with sufficiently many roots of unity. A major result was the proof by N. Karpenko and A. Merkurjev [23] that $\text{ed}(G) = \text{rdim } G$ when G is a p -group. This has motivated the study of $\text{rdim } G$ for several families of p -groups. See [30; 10; 1; 2].

In this paper, prompted by a question raised on the Math Overflow web site, we study the problem of finding sharp bounds for $\text{rdim } G$ in terms of $|G|$. More precisely, the question asked was whether $\text{rdim } G \leq \sqrt{|G|}$. As pointed out by D. Holt, $C_2 \times C_2 \times C_2$ is a counterexample. Our first main result shows that all counterexamples are closely related to Holt's example. In the following statement, $\text{Soc}(G)$ is the socle of G and $\text{Irr}(G|Z(G))$ is the set of irreducible characters of G that lie over a nonprincipal linear character of the center of G . Recall that if N is a normal subgroup of a finite group G and $\chi \in \text{Irr}(G)$, we say that χ is fully ramified with respect to G/N if $\chi_N = |G : N|^{1/2}\theta$ for some $\theta \in \text{Irr}(N)$. In this situation we also say that θ is fully ramified.

Theorem A. *Let G be a finite group. Then one of the following holds:*

- (i) $\text{rdim } G \leq \sqrt{|G|}$.
- (ii) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$. For any such group G , $\text{rdim } G = \frac{3}{\sqrt{8}}\sqrt{|G|}$.

We have also shown that the equality $\text{rdim } G = \sqrt{|G|}$ just holds in groups that are similar to those in (ii) above.

Theorem B. *Let G be a finite group. Then $\text{rdim } G = \sqrt{|G|}$ if and only if one of the following holds:*

- (i) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$.
- (ii) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2 \times C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$.

Interestingly, the groups with $\text{rdim } G$ as large as it can be in comparison with $|G|$ turn out to be 2-groups. There are nonabelian groups among those that appear in Theorem A(ii) and in Theorem B: consider for instance the Sylow 2-subgroups of $\text{GL}(3, 8)$ and $\text{GL}(3, 4)$ and $\text{GL}(3, 16)$. They are examples of nonabelian groups with the structure described in Theorem A(ii), Theorem B(i) and Theorem B(ii), respectively. They are also examples of the so-called Heisenberg groups. There are nonnilpotent groups G with $\text{rdim } G$ arbitrarily close to $\sqrt{|G|}$: consider the Frobenius groups of order $(p-1)p$ for any prime p .

For any positive integer n and prime p , the maximal representation dimension among p -groups of order p^n was determined in [10]. As pointed out in that paper, if $f_p(n) = \max_{r \in \mathbb{N}}(rp^{\lfloor (n-r)/2 \rfloor})$, then $\text{rdim } G \leq f_p(n)$ for any G p -group of order p^n . It was shown that, with a few exceptions for p and n listed in Theorem 1 of [10], there exists a p -group G of order p^n such that $\text{rdim } G = f_p(n)$. When $p = 2$

the exceptional cases are $n = 5$ and $n = 7$. In the next result we characterize the 2-groups where this equality occurs. It will be used in the proof of Theorems A and B.

Theorem C. *Let G be a 2-group of order 2^n for some positive integer $n \notin \{1, 5, 7\}$. Then $\text{rdim } G = f_2(n)$ if and only if one of the following holds:*

- (i) n is odd, $Z(G)$ is elementary abelian of order 8 and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.
- (ii) n is even, $Z(G)$ is elementary abelian of order either 4 or 16 and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.

When p is odd, the exceptional case in Theorem 1 of [10] is $n = 4$. We have the following.

Theorem D. *Let p be an odd prime and let G be a p -group of order p^n for some positive integer $n \notin \{1, 4\}$. Then $\text{rdim } G = f_p(n)$ if and only if one of the following holds:*

- (i) n is odd, $Z(G)$ has order p and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.
- (ii) n is even, $Z(G)$ is elementary abelian of order p^2 and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.

We obtain Theorems C and D as a consequence of a more general characterization of p -groups with center of rank r and $\text{rdim } G = rp^{\lfloor (n-r)/2 \rfloor}$ (see Theorem 2.5 and Theorem 2.6).

There is a related invariant that has been more studied with a group-theoretic motivation. This is the smallest dimension of a faithful permutation representation, denoted by $\mu(G)$. It was shown by P. Neumann [31] that there are groups G with normal subgroups N such that $\mu(G/N) > \mu(N)$. L. Kovács and C. Praeger [24] showed that $\mu(G/N) \leq \mu(G)$ holds whenever G/N does not have nontrivial abelian normal subgroups. Holt and J. Walton [18] proved that $\mu(G/N) \leq (4.5)^{\mu(G)-1}$. As, for instance, the double cover of M_{12} shows, it is not true that $\text{rdim } G/N \leq \text{rdim } G$ even when G/N does not have nontrivial abelian normal subgroups. As a consequence of Jordan's theorem, it is easy to obtain the following variation of the Holt–Walton theorem for representation dimension.

Theorem E. *Let G be a finite group and N a normal subgroup of G . Write $\text{rdim } G = n$. Then*

$$\text{rdim } G/N \leq nj(n),$$

where $j(n)$ is any bound in Jordan's theorem.

It is an old conjecture of Praeger and Easdown [13] that if $N \trianglelefteq G$ and G/N is abelian, then $\mu(G/N) \leq \mu(G)$. This conjecture still remains open. In the case when G is a p -group with an abelian maximal subgroup it was proved in [15] that $\mu(G/G') \leq \mu(G)$. We will see that it is not true that $\text{rdim } G/G' \leq \text{rdim } G$ even in this case. However, we can obtain the following bound.

Theorem F. *Let G be a finite group and N a normal subgroup of G with G/N abelian. Write $\text{rdim } G = n$. Then*

$$\text{rdim } G/N \leq 3n/2.$$

This bound in [Theorem F](#) depends on the classification of finite simple groups (this is the only result in the paper that relies on the CFSG). Without the CFSG, we can prove that $\text{rdim } G/N \leq Kn^2/\log n$ for some universal constant K . Both versions of this result are straightforward consequences of known bounds on the number of generators of a linear group.

As a consequence of [Theorem E](#) and [\[32\]](#), which relies on a deep result in Mori theory [\[5\]](#), we can obtain a new result on the essential dimension of an arbitrary finite group. It was asked in [\[22\]](#) whether $\text{ed}(G/N) \leq \text{ed}(G)$ for any finite group G and any $N \trianglelefteq G$. A negative answer to this question was given in [Theorem 1.5](#) of [\[30\]](#). In fact, the example of A. Meyer and Reichstein shows that we cannot hope for bounds better than exponential in [Theorem E](#), even if we assume that G is a p -group. We obtain the following bound for $\text{ed}(G/N)$ in terms of $\text{ed}(G)$.

Corollary G. *Let G be a finite group and $N \trianglelefteq G$. Then*

$$\text{ed}(G/N) \leq \text{ed}(G)h(\text{ed}(G))j(\text{ed}(G)h(\text{ed}(G))),$$

where j is the bounding function in Jordan’s theorem and h is the bounding function in Birkar’s [Corollary 1.5](#) of [\[5\]](#).

We close this Introduction with a remark on the style that we have used in this paper. It is a paper on character theory of finite groups that, we hope, will be of interest to other areas outside group theory, particularly to those areas where the essential dimension of a finite group plays a role. For this reason, we have decided to include some details in our proofs that we would not have included in a paper addressed exclusively to group theorists.

2. p -groups

Our approach will be character-theoretic. Our notation follows [\[21\]](#). We start with the proofs of [Theorems C](#) and [D](#). If χ is a character of a finite group then χ can be decomposed as a sum of irreducible characters, called the irreducible constituents, and it is easy to see that the kernel of χ , $\text{Ker } \chi$, is the intersection of the kernels of the irreducible constituents ([Lemma 2.21](#) of [\[21\]](#)). We thus have the first part of the following elementary result.

Lemma 2.1. *Let G be a finite group. Then*

$$\text{rdim } G = \min \left\{ \sum_{i=1}^s \chi_i(1) \mid s \in \mathbb{Z}^+, \chi_i \in \text{Irr}(G) \text{ for every } i = 1, \dots, s, \bigcap_{i=1}^s \text{Ker } \chi_i = 1 \right\}.$$

Furthermore, if $\chi_1, \dots, \chi_s \in \text{Irr}(G)$ are such that $\text{rdim } G = \sum_{i=1}^s \chi_i(1)$ and $\bigcap_{i=1}^s \text{Ker } \chi_i = 1$ then for every $i = 1, \dots, s$, $\text{Soc}(G) \not\subseteq \text{Ker } \chi_i$.

Proof. It suffices to prove the second part. This follows from the fact that if, say, $\text{Soc}(G) \leq \text{Ker } \chi_1$, then

$$\text{Soc}(G) \cap \left(\bigcap_{i=2}^r \text{Ker } \chi_i \right) \leq \bigcap_{i=1}^r \text{Ker } \chi_i = 1$$

so $\bigcap_{i=2}^r \text{Ker } \chi_i = 1$ and $\sum_{i=1}^r \chi_i(1) < \text{rdim } G$, contradicting the first part. □

Note that if G is a finite group and $1 < N \trianglelefteq G$, then $N \cap \text{Soc}(G) > 1$. Thus if χ is a (not necessarily irreducible) character of G , then χ is faithful if and only if $\text{Ker } \chi \cap \text{Soc}(G) = 1$, which happens if and only if $\chi_{\text{Soc}(G)}$ is faithful.

If G is a p -group, then the minimal normal subgroups have order p , so they are central. Thus $\text{Soc}(G) = \Omega_1(Z(G))$, where $\Omega_1(Z(G))$ is the subgroup generated by the central elements of order p . This group is elementary abelian and its rank coincides with the rank of $Z(G)$. Recall also that if A is a finite abelian group then $\hat{A} = \text{Irr}(A)$ is a group isomorphic to A . We have the following.

Lemma 2.2. *Let p be a prime and let A be an elementary abelian p -group. Let μ be a character of A . Then μ is faithful if and only if the irreducible constituents of μ form a generating set of $\text{Irr}(A)$.*

Proof. Let $\lambda_1, \dots, \lambda_s$ be the irreducible constituents of μ . We know that μ is faithful if and only if $\bigcap_{i=1}^s \text{Ker } \lambda_i = 1$. Assume that these irreducible constituent do not form a generating set of $\text{Irr}(A)$. Then $\text{Irr}(A) = \langle \lambda_1, \dots, \lambda_s \rangle \times I$ for some $I > 1$. By Problem 2.7 of [21], there exists $1 < B \leq A$ such that $B \leq \text{Ker } \lambda_i$ for every $i = 1, \dots, s$. Thus μ is not faithful. The converse is proved analogously. □

We will use the following elementary result, which follows from Corollary 2.30 of [21].

Lemma 2.3. *Let G be a finite group and let $\chi \in \text{Irr}(G)$. Then*

$$\chi(1) \leq |G : Z(G)|^{1/2}.$$

If G is any group, $N \trianglelefteq G$ and $\lambda \in \text{Irr}(N)$, then we set

$$\text{Irr}(G|\lambda) = \{ \chi \in \text{Irr}(G) \mid [\chi_N, \lambda] \neq 0 \}.$$

If χ is any of the characters in $\text{Irr}(G|\lambda)$, we say that χ lies over λ . Now we are ready to prove the following useful result to compute the representation dimension of p -groups.

Corollary 2.4. *Let p be a prime, let $G > 1$ be a group of order p^n and let r be the rank of $Z(G)$. Let χ be a faithful character of minimal degree of G . Then there exist $\chi_1, \dots, \chi_r \in \text{Irr}(G)$ such that $\chi = \chi_1 + \dots + \chi_r$ and $(\chi_i)_{\Omega_1(Z(G))} = e_i \lambda_i$ for some linear characters $\{\lambda_1, \dots, \lambda_r\} \subseteq \text{Irr}(\Omega_1(Z(G)))$ that form a minimal generating set of $\text{Irr}(\Omega_1(Z(G)))$. In particular,*

$$\text{rdim } G = \min_{\{\lambda_1, \dots, \lambda_r\}} \min \left\{ \sum_{i=1}^r \chi_i(1) \mid \chi_i \in \text{Irr}(G|\lambda_i) \text{ for every } i = 1, \dots, r \right\},$$

where $\{\lambda_1, \dots, \lambda_r\}$ runs over the minimal generating sets of $\text{Irr}(\Omega_1(Z(G)))$. Furthermore,

$$\text{rdim } G \leq rp^{(n-r)/2}.$$

Proof. Since χ is faithful, then $\mu = \chi_{\Omega_1(Z(G))}$ is faithful. By [Lemma 2.2](#), the irreducible constituents of μ form a generating set $\{\lambda_1, \dots, \lambda_r\}$ of $\text{Irr}(\Omega_1(Z(G)))$.

We know that for any i , χ has some irreducible constituent χ_i lying over λ_i and that for any choice of these irreducible constituents χ_i , $\chi_1 + \dots + \chi_r$ is faithful. Since $\chi(1)$ is the minimal degree of a faithful character of G , we conclude that $\chi = \chi_1 + \dots + \chi_r$ with $\chi_i \in \text{Irr}(G|\lambda_i)$ of minimal degree among the characters in $\text{Irr}(G|\lambda_i)$ for every i . The result follows. (The upper bound for $\text{rdim } G$ follows from [Lemma 2.3](#) and the formula for $\text{rdim } G$.) □

The last statement in the previous lemma was also pointed out in the Introduction of [\[10\]](#).

As promised in the Introduction to this paper, we will deduce [Theorems C and D](#) from a more general result that characterizes the p -groups with center of rank r with $\text{rdim } G = rp^{\lfloor(n-r)/2\rfloor}$. Since the result has some differences according as to whether $n - r$ is even or odd we have split the result in two parts. We start with the $n - r$ even case.

Theorem 2.5. *Let p be a prime, let $G > 1$ be a group of order p^n and let r be the rank of $Z(G)$. Assume that $n - r$ is even. Then $\text{rdim } G = rp^{(n-r)/2}$ if and only if $Z(G)$ is elementary abelian of order p^r and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.*

Proof. First, note that by [Corollary 2.30](#) of [\[21\]](#), the degree of any irreducible character of G is at most $|G : Z(G)|^{1/2} \leq p^{(n-r)/2}$. Furthermore, it is easy to deduce that if G has irreducible characters of degree $p^{(n-r)/2}$, then $Z(G)$ is elementary abelian.

Let G be a p -group of order p^n , with center elementary abelian of order p^r and all characters in $\text{Irr}(G|Z(G))$ fully ramified with respect to $G/Z(G)$. We know by [Corollary 2.4](#) that

$$\text{rdim } G = \min_{\{\lambda_1, \dots, \lambda_r\}} \min \left\{ \sum_{i=1}^r \chi_i(1) \mid \chi_i \in \text{Irr}(G|\lambda_i) \text{ for every } i = 1, \dots, r \right\},$$

where $\{\lambda_1, \dots, \lambda_r\}$ runs over the minimal generating sets of $\text{Irr}(\Omega_1(Z(G)))$. Fix a set $\{\lambda_1, \dots, \lambda_r\}$ that attains the first minimum. By hypothesis, for any $\chi_i \in \text{Irr}(G|\lambda_i)$, $\chi_i(1) = |G : Z(G)|^{1/2} = p^{(n-r)/2}$. We deduce that $\text{rdim } G = rp^{(n-r)/2}$, as desired.

Conversely, assume that $\text{rdim } G = rp^{(n-r)/2}$. Assume, by way of contradiction, that there exists $\chi_1 \in \text{Irr}(G|Z(G))$ with $\chi_1(1) < p^{(n-r)/2}$. Let $\lambda_1 \in \text{Irr}(\Omega_1(Z(G)))$ lying under χ_1 . Now, prolong $\{\lambda_1\}$ to a minimal generating set $\{\lambda_1, \dots, \lambda_r\}$ of $\text{Irr}(\Omega_1(Z(G)))$ and choose $\chi_i \in \text{Irr}(G)$ lying over λ_i for every $i = 2, \dots, r$. Note that $\chi_i(1) \leq p^{(n-r)/2}$. Set $\chi = \chi_1 + \dots + \chi_r$ and note that $\chi(1) < rp^{(n-r)/2}$. Furthermore, all the members of $\{\lambda_1, \dots, \lambda_r\}$ are irreducible constituents of $\mu = \chi_{\Omega_1(Z(G))}$. By [Lemma 2.2](#), μ is faithful. Hence, χ is faithful. This contradicts the hypothesis $\text{rdim } G = rp^{(n-r)/2}$. Therefore, the degree of any character in $\text{Irr}(G|Z(G))$ is $p^{(n-r)/2}$. The result follows. □

The next proof is similar and we omit some details.

Theorem 2.6. *Let p be a prime, let $G > 1$ be a group of order p^n and let r be the rank of $Z(G)$. Assume that $n - r$ is odd. Then $\text{rdim } G = rp^{(n-r-1)/2}$ if and only if all characters in $\text{Irr}(G|\Omega_1(Z(G)))$ have degree*

$p^{(n-r-1)/2}$. In this case, $|Z(G) : \Omega_1(Z(G))| \leq p$, i.e., $Z(G)$ is either elementary abelian or isomorphic to $C_{p^2} \times C_p \times \cdots \times C_p$.

Proof. Again, the degree of any irreducible character of G is at most $p^{(n-r-1)/2}$. Furthermore, if G has irreducible characters of degree $p^{(n-r-1)/2}$, then $|Z(G) : \Omega_1(Z(G))| \leq p$.

If all characters in $\text{Irr}(G|\Omega_1(Z(G)))$ have degree $p^{(n-r-1)/2}$, then it follows from [Corollary 2.4](#) that $\text{rdim } G = rp^{(n-r-1)/2}$ (because a faithful character of minimal degree is the sum of r characters in $\text{Irr}(G|\Omega_1(Z(G)))$).

Conversely, assume that $\text{rdim } G = rp^{(n-r-1)/2}$. As in the previous theorem, we can see that the degree of any character in $\text{Irr}(G|Z(G))$ is $p^{(n-r-1)/2}$. The result follows. \square

Now, we are ready to deduce [Theorem D](#). It turns out that we just need the case $n - r$ even.

Proof of Theorem D. Let r be the rank of $Z(G)$. Assume first that n is odd. As mentioned in the table in p. 638 of [\[10\]](#), $f_p(n) = \max_{s \in \mathbb{N}}(sp^{\lfloor (n-s)/2 \rfloor}) = p^{(n-1)/2}$ in this case. It is easy to see that this maximum is achieved only at $s = 1$. Since $f_p(n) = \text{rdim } G \leq rp^{\lfloor (n-r)/2 \rfloor}$ we deduce that $r = 1$. Thus $n - r = n - 1$ is even and we are in the situation of [Theorem 2.5](#). We deduce that $Z(G)$ has order p and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$.

Now, suppose that n is even. In this case, $f_p(n) = \max_{s \in \mathbb{N}}(sp^{\lfloor (n-s)/2 \rfloor}) = 2p^{(n-2)/2}$ and it is easy to see that this maximum is achieved only at $s = 2$. As in the n odd case, we can see that $r = 2$. Thus $n - r = n - 2$ is even and we are also in the situation of [Theorem 2.5](#). We conclude that $Z(G)$ is elementary abelian of order p^2 and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$. \square

Since the proof of [Theorem C](#) is analogous to that of [Theorem D](#), we omit some details.

Proof of Theorem C. Let r be the rank of $Z(G)$. If n is odd, then $f_2(n) = 3p^{(n-3)/2}$ and the maximum is achieved only at $s = 3$. We can see that $r = 3$, so $n - r$ is even and the result follows from [Theorem 2.5](#). If n is even, then $f_2(n) = 2p^{(n-2)/2}$ and the maximum is achieved only at $s = 2$ and $s = 4$. We can see that $r = 2$ or $r = 4$, so $n - r$ is even and the result also follows from [Theorem 2.5](#). \square

3. Arbitrary groups

In this section, we prove [Theorems A and B](#). We start by noting that [Theorem A](#) follows immediately from an elementary result in character theory for groups with a faithful irreducible character.

Proposition 3.1. *Let G be a finite group. Then*

$$\sum_{\chi \in \text{Irr}(G)} \chi(1)^2 = |G|.$$

In particular, if $G > 1$ then $\chi(1) < \sqrt{|G|}$ for any $\chi \in \text{Irr}(G)$.

Proof. The first part is [Corollary 2.7](#) of [\[21\]](#). \square

The problem of which finite groups have faithful irreducible characters is therefore relevant for our purposes. This problem has been studied since the beginning of the 20th century and there are several, perhaps not very well-known, characterizations of these groups. We refer the reader to Section 2 of [34] for a nice review of the history of this problem.

As in the p -group case, the socle of G is very relevant in these characterizations. Recall that $\text{Soc}(G) = A(G) \times T(G)$, where $A(G) = A_1 \times \cdots \times A_t$ is a direct product of *some* elementary abelian minimal normal subgroups of G and $T(G)$ is the direct product of *all* the nonabelian minimal normal subgroups of G (see Definition 42.6 and Lemma 42.9 of [20]). In the remaining of this article, we will use the notation introduced in this paragraph without further explicit mention. In particular, $t = t(G)$ is the number of elementary abelian minimal normal subgroups of G that appear in a decomposition of $A(G)$ as a direct product of minimal normal subgroups.

We will use the following consequence of Gaschütz's characterization (Theorem 42.7 of [20]) of finite groups with a faithful irreducible character.

Theorem 3.2. *If for every prime p every simple $\text{GF}(p)G$ -module appears at most with multiplicity one in $A(G)$, then G has a faithful irreducible character.*

Proof. This is Theorem 42.12(a) of [20]. □

Lemma 3.3. *Let G be a finite group. Then $T(G)$ has a faithful irreducible character. In particular, if $t = 0$ (or, equivalently, if G does not have any nontrivial abelian normal subgroup) then G has a faithful irreducible character and $\text{rdim } G < \sqrt{|G|}$.*

Proof. Note that $T(G)$ is a direct product of nonabelian simple groups. By Problem 4.3 of [21], for instance, the product φ of nonprincipal characters of each of the factors is a faithful irreducible character of $T(G)$.

If $\chi \in \text{Irr}(G)$ lies over φ then $\chi_{T(G)}$ is a sum of conjugates of φ , so by Lemma 2.21 of [21], $\chi_{T(G)}$ is faithful. This implies that

$$1 = \text{Ker } \chi \cap T(G) = \text{Ker } \chi \cap \text{Soc}(G),$$

so χ is a faithful irreducible character of G . Now, $\text{rdim } G \leq \chi(1) < \sqrt{|G|}$, by Corollary 2.7 of [21]. □

Lemma 3.4. *Let G be a finite group without nonabelian minimal normal subgroups. Let χ be a faithful character of G with $\text{rdim } G = \chi(1)$. Then $\text{Soc}(G) \not\leq \text{Ker } \psi$ whenever $\psi \in \text{Irr}(G)$ is an irreducible constituent of χ .*

Proof. Assume not. Then $\text{Soc}(G) = A(G) \leq \text{Ker } \psi$ for some $\psi \in \text{Irr}(G)$ irreducible constituent of χ . Consider $\Delta = \chi - \psi$. Since ψ is an irreducible constituent of χ , Δ is a character of G and $\Delta(1) < \chi(1) = \text{rdim } G$. Thus Δ is not faithful. Let ψ_1, \dots, ψ_s be the remaining irreducible constituents of χ . Since Δ is not faithful, the intersection of the kernels of the ψ_i 's is not trivial. But since $\text{Ker } \psi$ contains the whole socle, we deduce that the intersection of the kernels of all the irreducible constituents of χ is not trivial. This contradicts the hypothesis that χ is faithful. □

We write $d(G)$ to denote the minimal number of generators of G , that is, the rank of G . The following result is well-known.

Lemma 3.5. *Let G be a finite abelian group. Then $d(G) = \text{rdim } G$.*

Proof. Set $d(G) = m$. By the fundamental theorem of abelian groups, $G = C_1 \times \cdots \times C_m$ is a direct product of m cyclic groups $C_i = \langle x_i \rangle$. Let λ_i be a generator of $\text{Irr}(C_i)$ and let $\mu_i \in \text{Irr}(G)$ be the linear character determined by means of $\mu_i(x_i) = \varepsilon$, where ε is an $o(x_i)$ th primitive root of unity, and $\mu_i(x_j) = 1$ for $j \neq i$. Notice that $\text{Ker } \mu_i = C_1 \cdots C_{i-1} C_{i+1} \cdots C_m$. Put $\mu = \mu_1 + \cdots + \mu_m$. By Lemma 2.21 of [21], $\text{Ker } \mu = 1$, i.e., μ is faithful. Since $\mu(1) = m$ we deduce $\text{rdim } G \leq \mu(1) = m = d(G)$.

Conversely, let χ be any faithful character of G . Decompose $\chi = a_1 \chi_1 + \cdots + a_s \chi_s$ as a sum of irreducible (linear) characters χ_i . Since $G/\text{Ker } \chi_i$ is cyclic for every i and the intersection of the kernels of the characters χ_i is trivial, we deduce that G is isomorphic to a subgroup of the direct product of the cyclic groups $G/\text{Ker } \chi_i$. Write Γ to denote this group. Since $d(\Gamma) = s$ and Γ is abelian, we deduce that $d(G) \leq d(\Gamma) = s \leq \chi(1) \leq \text{rdim } G$. The result follows. \square

The next result, in conjunction with Lemma 2.1, lies at the core of our proof of Theorems A and B.

Lemma 3.6. *Let G be a finite group. Assume that $t > 0$. For $i = 1, \dots, t$, write $B_i = A_1 \times \cdots \times A_{i-1} \times A_{i+1} \times \cdots \times A_t$. Then*

(i) *For every $i = 1, \dots, t$, there exists $\chi_i \in \text{Irr}(G)$ such that $\text{Ker } \chi_i \cap \text{Soc}(G) = B_i$. Furthermore,*

$$\chi_i(1) \leq |G/B_i : Z(G/B_i)|^{1/2}.$$

(ii) *We have $\bigcap_{i=1}^t \text{Ker } \chi_i = 1$. In particular, if $\chi = \chi_1 + \cdots + \chi_t$, then $\text{rdim } G \leq \chi(1)$.*

Proof. Let $\lambda_i \in \text{Irr}(A_i)$ be nonprincipal for $i = 1, \dots, t$ and $\varphi \in \text{Irr}(T(G))$ be faithful. Recall that $A(G) = A_i \times B_i$. Put

$$\mu_i = \lambda_i \times 1_{B_i} \times \varphi \in \text{Irr}(\text{Soc}(G)).$$

Let $\chi_i \in \text{Irr}(G)$ lying over μ_i . Since μ_i is an irreducible constituent of $(\chi_i)_{\text{Soc}(G)}$,

$$\text{Ker } \chi_i \cap \text{Soc}(G) \leq \text{core}_G(\text{Ker } \mu_i) = B_i.$$

Since $(\mu_i)_{B_i}$ is a multiple of the principal character, we clearly have that $B_i \leq \text{Ker } \chi_i$. The first claim of part (i) follows. The second claim holds by Corollary 2.30 of [21].

By the definition of the subgroups B_i , their intersection is trivial. Thus

$$1 = \bigcap_{i=1}^t (\text{Ker } \chi_i \cap \text{Soc}(G)) = \left(\bigcap_{i=1}^t \text{Ker } \chi_i \right) \cap \text{Soc}(G).$$

Since $\bigcap_{i=1}^t \text{Ker } \chi_i$ is a normal subgroup of G , we deduce that it has to be the trivial subgroup. The inequality $\text{rdim } G \leq \chi(1)$ follows from Lemma 2.1. \square

Now, we can obtain our first approximation to Theorem A when $t > 0$. In the remaining results in this section, we will also use the notation from Lemma 3.6. In particular, the characters χ_i and λ_i will be the characters that have appeared in the statement of Lemma 3.6 and its proof.

Lemma 3.7. *Let G be a finite group. Assume that $t \geq 1$. Write $|A_i| = a_i$ for every $i = 1, \dots, t$. Then*

$$\text{rdim } G < \sqrt{|G|} \left(\sum_{j=1}^t \prod_{k \neq j} \frac{1}{\sqrt{a_k}} \right).$$

Proof. Since $\chi_i \in \text{Irr}(G/B_i)$, we note that

$$\chi_i(1) < \sqrt{\frac{|G|}{a_1 \cdots a_{i-1} a_{i+1} \cdots a_t}},$$

(It suffices to observe that $|B_i| = a_1 \cdots a_{i-1} a_{i+1} \cdots a_t$.)

Hence, if $\chi = \chi_1 + \cdots + \chi_t$,

$$\text{rdim } G \leq \chi(1) < \sum_{i=1}^t \sqrt{\frac{|G|}{a_1 \cdots a_{i-1} a_{i+1} \cdots a_t}} = \sqrt{|G|} \left(\sum_{j=1}^t \prod_{k \neq j} \frac{1}{\sqrt{a_k}} \right). \quad \square$$

Lemma 3.7 implies that Theorem A holds when $\sum_{j=1}^t \prod_{k \neq j} 1/\sqrt{a_k} \leq 1$. In the next elementary lemma we see that this is the case most of the time.

Lemma 3.8. *Let $t \geq 2$ be an integer and let $a_1 \geq \cdots \geq a_t \geq 2$ be t integers. If*

$$\sum_{j=1}^t \prod_{k \neq j} \frac{1}{\sqrt{a_k}} > 1, \tag{*}$$

then we are in one of following cases:

- (i) $t = 2$ and $(a_1, a_2) \in \{(x, 2), (y, 3) \mid 2 \leq x \leq 11, 3 \leq y \leq 5\}$.
- (ii) $t = 3$ and $(a_1, a_2, a_3) \in \{(x, 2, 2), (4, 3, 2), (3, 3, 2) \mid 2 \leq x \leq 7\}$.
- (iii) $t = 4$ and $(a_1, a_2, a_3, a_4) \in \{(x, 2, 2, 2), (3, 3, 2, 2) \mid 2 \leq x \leq 5\}$.
- (iv) $t = 5$ and $(a_1, a_2, a_3, a_4, a_5) \in \{(2, 2, 2, 2, 2), (3, 2, 2, 2, 2)\}$.
- (v) $t = 6$ and $(a_1, a_2, a_3, a_4, a_5, a_6) = (2, 2, 2, 2, 2, 2)$.

Proof. The left of (*) has t summands, each no greater than $1/\sqrt{2^{t-1}}$. Thus

$$\frac{t}{2^{(t-1)/2}} \geq \sum_{j=1}^t \prod_{k \neq j} \frac{1}{\sqrt{a_k}} > 1$$

and it follows from basic calculus that $t \leq 6$. The possible values for (a_1, \dots, a_t) for each of the possibilities for t can also be obtained in an elementary way. We omit the details. □

Now, we can complete the proof of Theorems A and B by analyzing the exceptional cases that appear in Lemma 3.8. We will use several times that if G is a finite group and $\chi \in \text{Irr}(G)$ then $\chi(1) \leq |G : Z(G)|^{1/2}$ by Lemma 2.3. Groups with an irreducible character χ such that $\chi(1) = |G : Z(G)|^{1/2}$ are called groups of central type. They have been rather studied. By a celebrated theorem of Howlett and Isaacs [19] they are solvable. We will not need the Howlett–Isaacs theorem, but we will use a more elementary previous

result that says that if G is a group of central type then the set of primes that divide $|Z(G)|$ coincides with the set of primes that divide $|G|$ (see Theorem 2 of [12]).

The next result includes both [Theorem A](#) and [Theorem B](#).

Theorem 3.9. *Let $G > 1$ be a finite group. Then one of the following holds:*

- (i) $\text{rdim } G < \sqrt{|G|}$.
- (ii) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$. For any such group G , $\text{rdim } G = \frac{3}{\sqrt{8}}|G|^{1/2}$.
- (iii) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$. For any such group G , $\text{rdim } G = \sqrt{|G|}$.
- (iv) G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2 \times C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$. For any such group G , $\text{rdim } G = \sqrt{|G|}$.

Proof. We have already seen that (i) holds if $t = 0$. This also holds when $t = 1$ by [Theorem 3.2](#). Hence, using [Lemmas 3.7](#) and [3.8](#), we may assume that $2 \leq t \leq 6$. We consider these five cases separately.

Case $t = 2$. We need to consider the values for (a_1, a_2) that appear in [Lemma 3.8](#). By [Theorem 3.2](#), G has an irreducible faithful character if $a_1 \neq a_2$, so it suffices to consider the cases $(a_1, a_2) = (2, 2)$ and $(a_1, a_2) = (3, 3)$.

- Suppose that $(a_1, a_2) = (2, 2)$. Then $\chi_1 \in \text{Irr}(G/A_2)$ and $|A(G)/A_2| = 2$, so $A(G)/A_2$ is central in G . Hence,

$$\chi_1(1) \leq |G/A_2 : Z(G/A_2)|^{1/2} \leq |G : A(G)|^{1/2} = |G|^{1/2}/2.$$

Arguing analogously with χ_2 , we obtain that $\chi_2(1) \leq |G|^{1/2}/2$, so

$$\chi(1) = \chi_1(1) + \chi_2(1) \leq |G|^{1/2}.$$

If $\chi(1) = |G|^{1/2}$ then all inequalities so far are equalities. In particular, $A(G) = A_1 \times A_2 = Z(G)$ is a Klein 4-group and G is a group of central type. Since $Z(G)$ is a 2-group, [Theorem 2](#) of [12] implies that G is also a 2-group. Thus $T(G) = 1$ and $\text{Soc}(G) = A(G) = Z(G)$ is elementary abelian of order 4. Write $|G| = 2^n$. By [Corollary 2.4](#),

$$\text{rdim } G \leq 2 \cdot 2^{(n-2)/2} = 2^{n/2} = |G|^{1/2}.$$

Furthermore, by [Theorem D](#) equality holds if and only if G is a 2-group with socle $\text{Soc}(G) = Z(G) = C_2 \times C_2$ and all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $Z(G)$. We deduce that either (i) or (iii) holds.

- Suppose instead that $(a_1, a_2) = (3, 3)$. Recall that χ_1 is an irreducible character of G that lies over a nonprincipal character of $A(G)/A_2$. Write $C/A_2 = C_{G/A_2}(A(G)/A_2)$. Note that G/C is isomorphic to a subgroup of $\text{Aut}(A(G)/A_2)$ and since $|A(G)/A_2| = 3$, $|G/C| \leq 2$. Notice also that $A(G)/A_2$ is central

in C/A_2 . If $C = G$, then $A(G)/A_2$ is central in G/A_2 and

$$\chi_1(1) \leq |G : A(G)|^{1/2} = |G|^{1/2}/3.$$

If $|G : C| = 2$ and $\gamma \in \text{Irr}(C)$ lies under χ_1 , then $\gamma(1) \leq |C : A(G)|^{1/2}$. By Clifford theory,

$$\chi_1(1) \leq 2\gamma(1) \leq 2|C : A(G)|^{1/2} = 2(|G|/18)^{1/2} = |G|^{1/2}(2/3\sqrt{2}).$$

Thus, in both cases, $\chi_1(1) \leq |G|^{1/2}(2/3\sqrt{2})$. Analogously, $\chi_2(1) \leq |G|^{1/2}(2/3\sqrt{2})$. Hence,

$$\chi(1) = \chi_1(1) + \chi_2(1) \leq |G|^{1/2}(4/3\sqrt{2}) < |G|^{1/2},$$

and (i) holds.

Case $t = 3$. Using [Theorem 3.2](#) again, together with [Lemmas 3.7](#) and [3.8](#), we may suppose that $(a_1, a_2, a_3) = (x, 2, 2)$ for some $2 \leq x \leq 7$ or $(a_1, a_2, a_3) = (3, 3, 2)$.

• Suppose first that $(a_1, a_2, a_3) = (3, 3, 2)$. Arguing as in the case of (a_1, a_2) just above, one can see that $\chi_1(1) \leq |G|^{1/2}/3$, $\chi_2(1) \leq |G|^{1/2}/3$, and $\chi_3(1) \leq |G|^{1/2}/(3\sqrt{2})$. Thus

$$\chi(1) = \chi_1(1) + \chi_2(1) + \chi_3(1) \leq |G|^{1/2} \left(\frac{1}{3} + \frac{1}{3} + \frac{1}{3\sqrt{2}} \right) < |G|^{1/2},$$

and again (i) holds.

• $(a_1, a_2, a_3) = (7, 2, 2)$. Recall that χ_1 is an irreducible character of G that lies over a nonprincipal character of $A(G)/A_2A_3$. Write $C/A_2A_3 = C_{G/A_2A_3}(A(G)/A_2A_3)$. Note that G/C is isomorphic to a subgroup of $\text{Aut}(A(G)/A_2A_3)$ and since $|A(G)/A_2A_3| = 7$, $|G/C| \leq 6$. Arguing again as in previous cases, we have that the worse bound for $\chi_1(1)$ is obtained when $|G : C| = 6$ and in that case

$$\chi_1(1) \leq 6|C : A(G)|^{1/2} = 6(|G|/168)^{1/2} = |G|^{1/2}(3/\sqrt{42}).$$

Also, $\chi_2(1) \leq |G|^{1/2}/2\sqrt{7}$ and $\chi_3(1) \leq |G|^{1/2}/2\sqrt{7}$. Thus

$$\chi(1) \leq |G|^{1/2} \left(\frac{3}{\sqrt{42}} + \frac{1}{2\sqrt{7}} + \frac{1}{2\sqrt{7}} \right) < |G|^{1/2}.$$

We conclude that (i) holds too.

• The cases $(a_1, a_2, a_3) = (5, 2, 2)$ and $(a_1, a_2, a_3) = (3, 2, 2)$ are handled analogously; we omit details.

• $(a_1, a_2, a_3) = (4, 2, 2)$. Recall that $\chi_2 \in \text{Irr}(G/A_1A_3)$. As before, $A(G)/A_1A_3$ is central in G/A_1A_3 . Thus $\chi_2(1) \leq |G : A(G)|^{1/2} = |G|^{1/2}/4$. Assume first that $\chi_2(1) = |G : A(G)|^{1/2}$. Then $Z(G/A_1A_3) = A(G)/A_1A_3$ and G/A_1A_3 is a group of central type with χ_2 fully ramified with respect to the center. Since $Z(G/A_1A_3)$ is a 2-group and G/A_1A_3 is of central type, we deduce that G/A_1A_3 , and hence G , is a 2-group (by [Theorem 2](#) of [\[12\]](#)). Notice that $\chi_2(1) = |G|^{1/2}/4$. Analogously, we have that $\chi_3(1) \leq |G|^{1/2}/4$. Next, we bound $\chi_1(1)$. As usual, let $C/A_2A_3 = C_{G/A_2A_3}(A(G)/A_2A_3)$. Recall that G/C is isomorphic to a subgroup of $\text{Aut}(A(G)/A_2A_3) = \text{Aut}(C_2 \times C_2) \cong S_3$ and since G is a 2-group,

$|G/C| \leq 2$. As in previous cases, we deduce that

$$\chi_1(1) \leq 2|C : A(G)|^{1/2} = |G|^{1/2}(1/2\sqrt{2}).$$

We conclude that $\chi(1) < |G|^{1/2}$. Hence, we may assume that $\chi_2(1) < |G : A(G)|^{1/2}$. This implies that there exist at least two irreducible characters of G lying over the nonprincipal irreducible character λ_2 of $A(G)/A_1A_3$. Since

$$\sum_{\chi \in \text{Irr}(G/A_1A_3|\lambda_2)} \chi(1)^2 = |G : A(G)|,$$

we deduce that for some of the characters χ in this sum, $\chi(1)^2 \leq |G : A(G)|/2 = |G|/32$. Hence, we may assume that $\chi_2(1) \leq |G|^{1/2}/4\sqrt{2}$. Repeating the same reasoning, we may also assume that $\chi_3(1) \leq |G|^{1/2}/4\sqrt{2}$. Now, we bound $\chi_1(1)$. With our usual notation and arguments, we may assume that $|G : C| = 6$ and one can see that

$$\chi_1(1) \leq 6|C : A(G)|^{1/2} = 6(|G|^{1/2}/4\sqrt{6}) = |G|^{1/2}\sqrt{6}/4.$$

Thus

$$\chi(1) \leq |G|^{1/2} \left(\frac{\sqrt{6}}{4} + \frac{1}{4\sqrt{2}} + \frac{1}{4\sqrt{2}} \right) < |G|^{1/2}.$$

In this case, (i) also holds.

- $(a_1, a_2, a_3) = (2, 2, 2)$. In particular, $A(G) \leq Z(G)$. If $A(G) < Z(G)$ then $|Z(G)| \geq 2^4$ and $\psi(1) \leq |G : Z(G)|^{1/2} \leq |G|^{1/2}/4$ for every $\psi \in \text{Irr}(G)$. Since χ is the sum of 3 irreducible characters of G , we deduce that $\chi(1) < |G|^{1/2}$ and (i) holds. Thus we may assume that $A(G) = Z(G)$. In particular, if $\psi \in \text{Irr}(G)$ then $\psi(1) \leq |G : Z(G)|^{1/2} \leq |G|^{1/2}/\sqrt{8}$.

Assume that $\text{rdim } G \geq \sqrt{|G|}$. Let $\lambda \in \text{Irr}(Z(G))$ be a nonprincipal character and $K = \text{Ker } \lambda$. We claim that $Z(G/K) = Z(G)/K$. We argue by way of contradiction. Assume that $Z(G/K) > Z(G)/K$. Let $\psi \in \text{Irr}(G|\lambda)$. Then $\psi(1) \leq |G/K : Z(G/K)|^{1/2} \leq |G|^{1/2}/4$. We deduce that there exists a faithful character χ of G such that

$$\chi(1) \leq |G|^{1/2}/4 + |G|^{1/2}/\sqrt{8} + |G|^{1/2}/\sqrt{8} < |G|^{1/2}.$$

This is a contradiction. Hence, we have proved the claim. This argument also shows that $\psi(1) = |G : Z(G)|^{1/2} = |G|^{1/2}/\sqrt{8}$ for every $\psi \in \text{Irr}(G|Z(G))$, as desired. We deduce that (ii) holds. This concludes the case $t = 3$.

The remaining cases can be handled with the same techniques. Therefore, we will omit details.

Case $t = 4$. Again, using [Theorem 3.2](#), together with [Lemma 3.7](#) and [3.8](#), we may suppose that $(a_1, a_2, a_3, a_4) = (2, 2, 2, 2)$ or $(a_1, a_2, a_3, a_4) = (3, 3, 2, 2)$. In the first subcase, one can see arguing as in Subcase 1.1 that either (i) or (iv) holds. In the second subcase, it follows from an analysis of the degrees of $\chi_i, i = 1, \dots, 4$, that $\text{rdim } G < \sqrt{|G|}$.

Case $t = 5$. Again, using [Theorem 3.2](#), together with [Lemma 3.7](#) and [3.8](#), we may suppose that $(a_1, a_2, a_3, a_4, a_5) = (2, 2, 2, 2, 2)$. Thus $A(G)$ is the direct product of 5 minimal normal subgroups of order 2. Thus $A(G)$ is central. Hence $\chi_i(1) \leq |G|^{1/2}/\sqrt{32}$ for $i = 1, \dots, 5$ and $\chi(1) < |G|^{1/2}$. We deduce that (i) holds.

Case $t = 6$. Then $(a_1, a_2, a_3, a_4, a_5, a_6) = (2, 2, 2, 2, 2, 2)$, and thus $A(G)$ is the direct product of 6 minimal normal subgroups of order 2. Thus $A(G)$ is central. Hence $\chi_i(1) \leq |G|^{1/2}/\sqrt{64}$ for $i = 1, \dots, 6$ and $\chi(1) < |G|^{1/2}$. We deduce that (i) holds.

Now, it remains to determine $\text{rdim } G$ when G is one of the groups that appear in part (ii), (iii) or (iv). This has been done in [Theorem 2.5](#). □

4. Proof of [Theorem E](#), [Theorem F](#) and [Corollary G](#)

In this section we provide the short proofs of the remaining results. We start with [Theorem E](#).

Proof of [Theorem E](#). By Jordan's theorem, there exists an abelian subgroup $A \leq G$ such that $|G : A| \leq j(n)$ for some function j . Since $NA/N \cong A/A \cap N$ is abelian, we deduce that

$$\text{rdim } NA/N = d(NA/N) \leq d(A) \leq n.$$

Thus NA/N has a faithful character Δ of degree at most n . Hence the induced character Δ^G is faithful and has degree at most $nj(n)$. The result follows. □

Proof of [Corollary G](#). Write $\text{rdim } G = n$. By [Proposition 4.15](#) of [\[3\]](#),

$$\text{ed}(G/N) \leq \text{rdim } G/N.$$

Furthermore, by [Theorem E](#), $\text{rdim } G/N \leq nj(n)$. On the other hand, by [Theorem 2](#) of [\[32\]](#), $n \leq \text{ed}(G)h(\text{ed}(G))$. The result follows. □

As we already mentioned in the Introduction, it is not true that $\text{rdim } G/N \leq \text{rdim } G$ when G/N does not have any nontrivial abelian normal subgroup. This is false even when G is a p -group with an abelian maximal subgroup: consider $G = \text{SmallGroup}(2^5, 38)$. This group has an abelian maximal subgroup, it has faithful irreducible characters of degree 2, but $\text{rdim } G/G' = d(G/G') = 3$. [Theorem F](#) follows immediately from a result of Kóvacs and Robinson [\[25\]](#).

Theorem 4.1. *Each finite completely reducible linear group of dimension n can be generated by at most $3n/2$ elements. In particular, if G is a finite group, $N \trianglelefteq G$ and G/N is abelian, then $\text{rdim } G/N \leq 3 \text{rdim } G/2$.*

Proof. The first part is the main result of [\[25\]](#). For the second part, write $\text{rdim } G = n$. Therefore, G is a subgroup of $\text{GL}(n, \mathbb{C})$. By Maschke's theorem, G is completely reducible. Now, the first part implies that $d(G) \leq 3n/2$. Since G/N is abelian,

$$\text{rdim } G/N = d(G/N) \leq d(G) \leq 3n/2,$$

as wanted. □

Note that the bound in [25] relies on the classification. Using the weaker (but classification-free) bound in [14], we get that $\text{rdim } G/N \leq Kn^2/\log n$ for some constant K .

5. Concluding remarks and questions

The Heisenberg groups mentioned in the Introduction are just one example of the nonabelian groups that appear in the statement of Theorems A and B. Recall that a finite p -group G is called extraspecial if $G' = Z(G) = \Phi(G)$ has order p . A finite p -group G is called semiextraspecial if G/N is extraspecial for any N maximal subgroup of $Z(G)$. Any semiextraspecial group with center of the specified order also satisfies those hypotheses. As discussed in [27], these form a rather large family of groups. However, all of them have class 2. This suggests the question of whether or not there are groups of nilpotence class larger than 2 among the exceptional groups in Theorem A and Theorem B. Using the SmallGroups library [4] in GAP we have found groups of order 2^8 and nilpotence class 3 with the properties of those in the statement of Theorem B(i) (for instance, $\text{SmallGroup}(2^8, 3196)$). We suspect that there should also exist 2-groups of class 3 among the exceptional groups in Theorem A and also among those in Theorem B(ii). In fact, we expect the following question to have an affirmative answer:

Question 5.1. *Let $r \geq 1$ be an integer. Do there exist p -groups G with $Z(G)$ elementary abelian of order p^r and all characters in $\text{Irr}(G|Z(G))$ fully ramified with respect to $G/Z(G)$ of arbitrarily large nilpotence class?*

We have been informed by Z. Reichstein that he asked this question in the cases $r = 1$ and $r = 2$ at a conference in Banff on permutation groups in 2009. More precisely, he asked whether given a prime p and a positive integer n , there exists a p -group G of order p^n , with maximal representation dimension among groups of order p^n , and nilpotence class > 2 . Subsequently, C. Parker and R. Wilson constructed groups G of order p^{2p+3} , for any odd prime p . This appears in [9]. These are examples of groups of class > 2 that satisfy the conditions of Question 5.1 with $r = 1$. It turns out that Question 5.1 has an affirmative answer when $r = 1$, by Theorem 6.3 of [16].

We remark also that the condition that all characters in $\text{Irr}(G|Z(G))$ are fully ramified with respect to $G/Z(G)$ is equivalent to the condition that $(G, Z(G))$ is a Camina pair. This means that for any $g \in G \setminus Z(G)$, g is conjugate to any element in the coset $gZ(G)$. We refer the reader to [26], where these groups were studied (see also [8]). In particular, there is a character-free characterization of these groups (in terms of conjugacy classes). This seems tougher for the groups that appear in Theorem 2.6

Question 5.2. *Describe the p -groups G that are not of central type with all characters in $\text{Irr}(G|\Omega_1(Z(G)))$ of the same degree. Is there a character-free characterization of these groups? Are there groups of arbitrarily large nilpotence class among them?*

By the above-mentioned theorem of S. Gagola, any p -group is isomorphic to a subgroup of $G/Z(G)$ for some p -group G of central type with $Z(G)$ of order p , so it would be interesting to decide whether

the same happens when the degree of the common degree of the characters in $\text{Irr}(G|\Omega_1(Z(G)))$ is not $|G : Z(G)|^{1/2}$.

The proof of Theorem 1.5 of [30] shows that the best bounds one can hope for in Theorem E and Corollary G are exponential. The bounds we have obtained, even with the help of results that depend on the classification of finite simple groups, are superexponential. This, together with the known bounds and examples known for the analog problem for permutation representations mentioned in the Introduction, suggests the following questions. (Note, however, that we have already seen several differences between results for minimal faithful permutation representations and minimal dimensions of faithful linear representations.)

Question 5.3. *Does there exist a constant $c_1 > 1$ such that if G is a finite group and $N \trianglelefteq G$ then $\text{rdim } G/N \leq c_1^{\text{rdim } G}$?*

Question 5.4. *Does there exist a constant $c_2 > 1$ such that if G is a finite group and $N \trianglelefteq G$ then $\text{ed}(G/N) \leq c_2^{\text{ed}(G)}$?*

References

- [1] M. Bardestani, K. Mallahi-Karai, and H. Salmasian, “Minimal dimension of faithful representations for p -groups”, *J. Group Theory* **19**:4 (2016), 589–608. [MR](#)
- [2] M. Bardestani, K. Mallahi-Karai, and H. Salmasian, “Kirillov’s orbit method and polynomiality of the faithful dimension of p -groups”, *Compos. Math.* **155**:8 (2019), 1618–1654. [MR](#)
- [3] G. Berhuy and G. Favi, “Essential dimension: a functorial point of view (after A. Merkurjev)”, *Doc. Math.* **8** (2003), 279–330. [MR](#)
- [4] H. U. Besche, B. Eick, and E. A. O’Brien, “A millennium project: constructing small groups”, *Internat. J. Algebra Comput.* **12**:5 (2002), 623–644. [MR](#)
- [5] C. Birkar, “Singularities of linear systems and boundedness of Fano varieties”, *Ann. of Math. (2)* **193**:2 (2021), 347–405. [MR](#)
- [6] J. Bourgain and A. Gamburd, “Uniform expansion bounds for Cayley graphs of $\text{SL}_2(\mathbb{F}_p)$ ”, *Ann. of Math. (2)* **167**:2 (2008), 625–642. [MR](#)
- [7] J. Buhler and Z. Reichstein, “On the essential dimension of a finite group”, *Compositio Math.* **106**:2 (1997), 159–179. [MR](#)
- [8] S. T. Burkett and M. L. Lewis, “Partial GVZ-groups”, *J. Algebra* **581** (2021), 50–62. [MR](#)
- [9] S. Cernele, *Maximal representation dimension for groups of order p^n* , Master’s essay, University of British Columbia, 2010.
- [10] S. Cernele, M. Kamgarpour, and Z. Reichstein, “Maximal representation dimension of finite p -groups”, *J. Group Theory* **14**:4 (2011), 637–647. [MR](#)
- [11] M. J. Collins, “On Jordan’s theorem for complex linear groups”, *J. Group Theory* **10**:4 (2007), 411–423. [MR](#)
- [12] F. R. DeMeyer and G. J. Janusz, “Finite groups with an irreducible representation of large degree”, *Math. Z.* **108** (1969), 145–153. [MR](#)
- [13] D. Easdown and C. E. Praeger, “On minimal faithful permutation representations of finite groups”, *Bull. Austral. Math. Soc.* **38**:2 (1988), 207–220. [MR](#)
- [14] R. K. Fisher, “The number of generators of finite linear groups”, *Bull. London Math. Soc.* **6** (1974), 10–12. [MR](#)
- [15] C. Franchi, “On minimal degrees of permutation representations of abelian quotients of finite groups”, *Bull. Aust. Math. Soc.* **84**:3 (2011), 408–413. [MR](#)
- [16] S. M. Gagola, Jr., “Characters vanishing on all but two conjugacy classes”, *Pacific J. Math.* **109**:2 (1983), 363–385. [MR](#)

- [17] W. T. Gowers, “Quasirandom groups”, *Combin. Probab. Comput.* **17**:3 (2008), 363–387. [MR](#)
- [18] D. F. Holt and J. Walton, “Representing the quotient groups of a finite permutation group”, *J. Algebra* **248**:1 (2002), 307–333. [MR](#)
- [19] R. B. Howlett and I. M. Isaacs, “On groups of central type”, *Math. Z.* **179**:4 (1982), 555–569. [MR](#)
- [20] B. Huppert, *Character theory of finite groups*, Expositions in Mathematics **25**, de Gruyter, Berlin, 1998. [MR](#)
- [21] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976. Reprinted 2006, AMS/Chelsea. [MR](#)
- [22] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials: constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications **45**, Cambridge University Press, 2002. [MR](#)
- [23] N. A. Karpenko and A. S. Merkurjev, “Essential dimension of finite p -groups”, *Invent. Math.* **172**:3 (2008), 491–508. [MR](#)
- [24] L. G. Kovács and C. E. Praeger, “On minimal faithful permutation representations of finite groups”, *Bull. Austral. Math. Soc.* **62**:2 (2000), 311–317. [MR](#)
- [25] L. G. Kovács and G. R. Robinson, “Generating finite completely reducible linear groups”, *Proc. Amer. Math. Soc.* **112**:2 (1991), 357–364. [MR](#)
- [26] M. L. Lewis, “On p -group Camina pairs”, *J. Group Theory* **15**:4 (2012), 469–483. [MR](#)
- [27] M. L. Lewis, “Semi-extraspecial groups”, pp. 219–237 in *Advances in algebra*, Springer Proc. Math. Stat. **277**, Springer, 2019. [MR](#)
- [28] A. S. Merkurjev, “Essential dimension: a survey”, *Transform. Groups* **18**:2 (2013), 415–481. [MR](#)
- [29] A. S. Merkurjev, “Essential dimension”, *Bull. Amer. Math. Soc. (N.S.)* **54**:4 (2017), 635–661. [MR](#)
- [30] A. Meyer and Z. Reichstein, “Some consequences of the Karpenko–Merkurjev theorem”, *Doc. Math.* Suslin extra volume (2010), 445–457. [MR](#)
- [31] P. M. Neumann, “Some algorithms for computing with finite permutation groups”, pp. 59–92 in *Proceedings of groups* (St. Andrews, 1985), London Math. Soc. Lecture Note Ser. **121**, Cambridge Univ. Press, 1986. [MR](#)
- [32] Z. Reichstein, “The Jordan property of Cremona groups and essential dimension”, *Arch. Math. (Basel)* **111**:5 (2018), 449–455. [MR](#)
- [33] G. R. Robinson, “On linear groups”, *J. Algebra* **131**:2 (1990), 527–534. [MR](#)
- [34] F. Szechtman, “Groups having a faithful irreducible representation”, *J. Algebra* **454** (2016), 292–307. [MR](#)
- [35] B. Totaro, *Group cohomology and algebraic cycles*, Cambridge Tracts in Mathematics **204**, Cambridge University Press, 2014. [MR](#)

Communicated by Michael J. Larsen

Received 2022-09-25

Revised 2024-07-10

Accepted 2025-02-11

alexander.moreto@uv.es

*Departament de Matemàtiques, Universitat de València,
46100 Burjassot, València, Spain*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2026 is US \$590/year for the electronic version, and \$865/year (+\$75, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published continuously online.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2026 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 20 No. 2 2026

On the minimal dimension of a faithful linear representation of a finite group	219
ALEXANDER MORETÓ	
Moments of one-level densities in families of holomorphic cusp forms in the level aspect	237
PETER COHEN, JUSTINE DELL, OSCAR E. GONZÁLEZ, SIMRAN KHUNGER, CHUNG-HANG KWAN, STEVEN J. MILLER, ALEXANDER SHASHKOV, ALICIA REINA SMITH, CARSTEN SPRUNGER, NICHOLAS TRIANTAFILLOU, NHI TRUONG, ROGER VAN PESKI and STEPHEN WILLIS	
Murmurations of modular forms in the weight aspect	299
JONATHAN BOBER, ANDREW R. BOOKER, MIN LEE and DAVID LOWRY-DUDA	
The Alperin weight conjecture and the Glauberman correspondence via character triples	333
J. MIQUEL MARTÍNEZ, NOELIA RIZO and DAMIANO ROSSI	
Asymptotics of extensions of simple \mathbb{Q}-algebras	383
FABIAN GUNDLACH and BÉRANGER SEGUIN	