GENERATING FINITE NILPOTENT IRREDUCIBLE LINEAR GROUPS

By J. D. DIXON *and* L. G. KOVÁCS

[Received 23 September 1991]

1. Introduction

In a recent paper [**2**], M. F. Newman and the second author proved the following.

THEOREM 1.0. *There is a constant c such that for each positive integer d (≥ 2), each nilpotent transitive permutation group of degree d can be generated by $[cd/\sqrt{\log d}]$ elements. Moreover for each prime p there is a positive constant c_p such that whenever d is a power of p there is a transitive p-group of degree d which cannot be generated by $[c_p d/\sqrt{\log d}]$ elements.*

(For simplicity, in the sequel we usually omit the square brackets indicating 'integer parts'.) The aim of this paper is to explore the corresponding questions concerning finite nilpotent irreducible linear groups over arbitrary fields.

For the field of complex numbers, Isaacs [**1**] had done this long before [**2**]. Let G be a finite irreducible linear group of degree d over the field of complex numbers, such that the order of G is a power of a prime p. It was shown by Isaacs [**1**] that there exist linear functions b of d such that each such G can be generated by b elements. He wrote down one b explicitly, namely

$$b = \frac{p+1}{p(p-1)}d + \frac{2p-4}{p-1},$$

and constructed examples to show that the multiplicative constant involved in a b cannot be as small as $1/(p-1)$. In particular, any sub-linear bound proposed would be violated by infinitely many of his examples: so the direct analogue of the first part of Theorem 1.0 is false, and that of the second part is not good enough.

Our results will show that there is in fact a good analogue of Theorem 1.0 over fields which are 'small': for example, over each field which has finite degree over its prime subfield. Even for the case considered in Isaacs [**1**], one can read off some small improvements. First, the multiplicative constant in his b can be brought arbitrarily close to $1/(p-1)$ (of course, only at the cost of increasing the additive constant). Second, that multiplicative constant can be lowered all the way to

$1/(p-1)$ (but no further) if one is prepared to add to the linear b a suitable constant multiple of $d/\sqrt{\log d}$.

In addition to [2] and the examples of [1] mentioned above, we make use of the determination of the Sylow subgroups of general linear groups by Leedham-Green and Plesken [4]. Somewhat less than the full strength of their results will suffice here; in particular, we can make do with just two invariants of fields.

DEFINITION 1.1. For each prime p and for each field $\mathbb{F}$ whose characteristic is different from p, let $\mathbb{F}(\sqrt[p]{1})$ denote the splitting field of x^p+1 over $\mathbb{F}$. Write $f(p, \mathbb{F})$ for the degree of $\mathbb{F}(\sqrt[p]{1})$ over $\mathbb{F}$, and let

$$a(p, \mathbb{F}) = \frac{1}{(p-1)f(p, \mathbb{F})} \quad \text{and} \quad b(p, \mathbb{F}) = \frac{\sqrt{\log p}}{p(p-1)f(p, \mathbb{F})}.$$

Further, define $e(p, \mathbb{F})$ by saying that the Sylow p-subgroup of the multiplicative group of $\mathbb{F}(\sqrt[p]{1})$ is a cyclic or quasicyclic group of type $C(p^{e(p,\mathbb{F})})$.

Note that $f(2, \mathbb{F})$ is 1 or 2 and $2 \leq e(2, \mathbb{F}) \leq \infty$, while if $p>2$ then $f(p, \mathbb{F})$ is a divisor of $p-1$ and $1 \leq e(p, \mathbb{F}) \leq \infty$. Neither invariant is defined when the characteristic of $\mathbb{F}$ is p, but this is no loss because in that case p cannot be involved in any finite nilpotent irreducible group over $\mathbb{F}$.

For linear groups of prime-power order, our results can now be stated as follows.

THEOREM 1.2. *There exists a constant c_1 (independent of p and $\mathbb{F}$) such that, for $d>1$, each finite irreducible p-subgroup G of $GL(d, \mathbb{F})$ can be generated by*

$$a(p, \mathbb{F})d + 2b(p, \mathbb{F})c_1 d/\sqrt{\log d} + 2$$

elements. If $e(p, \mathbb{F}) < \infty$, then each such G can in fact be generated by

$$((p-1)e(p, \mathbb{F}) + 2)b(p, \mathbb{F})c_1 d/\sqrt{\log d} + 4$$

elements.

The transitive p-groups of degree d constructed in [2] to prove the second half of Theorem 1.0 will be shown to admit faithful irreducible linear representations of degree at most d over any field of characteristic different from p. In view of the monotonicity of the function $x/\sqrt{\log x}$, one may then draw the following conclusion (with the same constants c_p as in Theorem 1.0).

THEOREM 1.3. *For each field $\mathbb{F}$ and for each prime p different from the characteristic of $\mathbb{F}$, there exist infinitely many positive integers d such that not all finite irreducible p-subgroups of $GL(d, \mathbb{F})$ can be generated by $c_p d/\sqrt{\log d}$ elements.*

In the negative direction, this is the best we can do in general. Under appropriate assumptions on $\mathbb{F}$, one can do better by exploiting the examples of Isaacs [**1**]. He constructed there one finite p-group for each prime power p^n with $n > 0$ which cannot be generated by $n + (p^n - 1)/(p - 1)$ elements but admits a faithful irreducible complex representation of degree p^n. We shall show that this group has a faithful irreducible representation of degree $p^n f(p, \mathbb{F})$ over any $\mathbb{F}$ such that $e(p, \mathbb{F}) \geq n + 1$.

THEOREM 1.4. *For each integer n such that $2 \leq n + 1 \leq e(p, \mathbb{F})$, there is a finite irreducible linear p-group of degree $p^n f(p, \mathbb{F})$ over $\mathbb{F}$ which cannot be generated by $n + (p^n - 1)/(p - 1)$ elements.*

COROLLARY .5. *If $e(p, \mathbb{F}) = \infty$, then there exist infinitely many d such that not all finite irreducible p-subgroups of $GL(d, \mathbb{F})$ can be generated by*

$$a(p, \mathbb{F})d + (\log d)/(\log p) - (p - 1)/p$$

elements.

This comes directly from Theorem 1.4, and matches the first part of Theorem 1.2 quite well.

Let us turn to the general nilpotent case now.

DEFINITION 1.6. For an arbitrary field $\mathbb{F}$, let $m_{\mathbb{F}}$ denote the maximum of $a(p, \mathbb{F})$ as p ranges over the primes (different from the characteristic of $\mathbb{F}$) such that $e(p, \mathbb{F}) = \infty$; if there is no such p, set $m_{\mathbb{F}} = 0$.

COROLLARY 1.7. *Given a field $\mathbb{F}$, to each positive ε there is an N (depending only on ε and $\mathbb{F}$) such that each finite nilpotent irreducible linear group of degree d over $\mathbb{F}$ can be generated by $(m_{\mathbb{F}} + \varepsilon)d + N$ elements.*

For some fields $\mathbb{F}$ with $m_{\mathbb{F}} = 0$, the second half of Theorem 1.2 yields a better result.

COROLLARY 1.8. *Let $\mathbb{F}$ be a field such that $m_{\mathbb{F}} = 0$ and such that $(p - 1)e(p, \mathbb{F})b(p, \mathbb{F})$ remains bounded while p ranges over all primes (other than the characteristic of $\mathbb{F}$); for example, this holds for any field which is of finite degree over its prime subfield. Then there is a constant $c_{\mathbb{F}}$ such that each finite nilpotent irreducible linear group of degree d over $\mathbb{F}$ can be generated by $c_{\mathbb{F}} d/\sqrt{\log d}$ elements.*

Together with Theorem 1.3, this shows that the behaviour of finite nilpotent irreducible linear groups over 'small' fields resembles that of finite nilpotent transitive permutation groups.

We note one more consequence of Theorem 1.4.

COROLLARY 1.9. *To each convergent sequence* $r(1), \ldots, r(d), \ldots$ *of positive real numbers with limit* 0, *there is a field* $\mathbb{F}$ *of characteristic* 0 *with* $m_{\mathbb{F}} = 0$ *and infinitely many* d *such that not all finite nilpotent irreducible subgroups of* $GL(d, \mathbb{F})$ *can be generated by* $r(d)d$ *elements.*

The point of this may be best explained in different terms. For each field $\mathbb{F}$ and for each positive integer d, let $t_{\mathbb{F}}(d)$ denote the smallest integer such that each finite nilpotent irreducible linear group of degree d over $\mathbb{F}$ can be generated by $t_{\mathbb{F}}(d)$ elements (Theorem 1.2 guarantees that such numbers exist). Corollaries 1.5 and 1.7 together give that $\limsup_{d\to\infty} t_{\mathbb{F}}(d)/d = m_{\mathbb{F}}$. In particular, if $m_{\mathbb{F}} = 0$ then $\lim_{d\to\infty} t_{\mathbb{F}}(d)/d = 0$. Under the hypotheses of Corollary 1.8, $t_{\mathbb{F}}(d)/d$ converges to 0 at least as fast as $c_{\mathbb{F}}/\sqrt{\log d}$ does. By contrast, Corollary 1.9 means that for suitable $\mathbb{F}$ with $m_{\mathbb{F}} = 0$ the convergence of $t_{\mathbb{F}}(d)/d$ is arbitrarily slow.

It is natural to ask what happens to our theorems if the assumptions are relaxed. To see that irreducibility cannot be replaced by complete reducibility in the second part of Theorem 1.2 or in Corollary 1.8, one only has to think of direct sums of copies of any one finite nilpotent irreducible linear group. On the other hand, Isaacs [**1**] had shown that each finite nilpotent completely reducible linear group of degree d can be generated by $3d/2$ elements, and G. R. Robinson and the second author [**3**] showed recently that in this result of Isaacs the nilpotency assumption is redundant. This encourages the hope that our present results, and also those of [**2**], remain valid if the nilpotency condition is omitted.

The organization of the paper is as follows. Section 2 contains preparatory material on Sylow subgroups of general linear groups and on subgroups of wreath products. Section 3 gives the proof of Theorem 1.2, apart from one lemma whose proof is deferred to the last section. The proofs of the other theorems and of Corollaries 1.7–1.9 occupy separate sections.

2. Generating subgroups of wreath products

The aim of this section is to collect all but one of the preliminary steps towards the proof of Theorem 1.2.

It is well known that if $\mathbb{F}$ is algebraically closed then each finite irreducible p-subgroup G of $GL(d, \mathbb{F})$ is monomial: d is a power of p, and G is a subgroup of the (permutational) wreath product $C(p^\infty)$ wr (Sym d) of the relevant quasicyclic group with the relevant symmetric group, such that the 'top projection' of G in Sym d is transitive (as subgroup of that permutation group). Over an arbitrary field the situation is rather more complicated; for the present purpose, it will be

sufficient to have the following consequence of the conclusive information provided by Leedham-Green and Plesken [**4**].

THEOREM 2.0. *Let $d > 1$ and let G be a finite irreducible p-subgroup of $GL(d, \mathbb{F})$. Then there is a nonnegative integer n such that $d = p^n f(p, \mathbb{F})$, and at least one of the following holds*:

(i) *G is a subgroup of $C(p^{e(p,\mathbb{F})})$ wr (Sym p^n) with transitive top projection*;

(ii) *$p = 2$ and $f(2, \mathbb{F}) = 2$ so $d = 2^{n+1}$, and G is a transitive subgroup of* Sym 2^{n+2};

(iii) *$p = 2$ and $f(2, \mathbb{F}) = 2$ so $d = 2^{n+1}$, $e(2, \mathbb{F}) > 2$, and there is a non-negative integer m ($=0$ if $e(2, \mathbb{F}) = \infty$) and a group D with a cyclic or quasicyclic subgroup $C(2^{m+e(2,\mathbb{F})})$ of index 2 such that G is a subgroup of D* wr (Sym 2^{n-m}) *with transitive top projection.*

We shall make repeated use of a basic fact.

LEMMA 2.1. *Let A be a submodule [or normal subgroup] of a module [or group] B. If each submodule [subgroup] of A can be generated by α elements and each submodule [subgroup] of B/A can be generated by β elements, then each submodule [subgroup] of B can be generated by $\alpha + \beta$ elements.*

As in Kovács and Newman [**2**], for each prime power p^n, we let $f(p^n)$ denote the least integer such that each transitive permutation group of p-power order and degree p^n can be generated by $f(p^n)$ elements. Further, we write $M(p^n)$ for the coefficient of $x^{[(p-1)n/2]}$ in the polynomial $(1 + x + \cdots + x^{p-1})^n$. It was proved there (combine (3.2) and (4.1)) that if P is a transitive p-group of degree p^n viewed as a group of permutation matrices over $\mathbb{Z}/p\mathbb{Z}$, then each submodule of the natural module for P can be generated by $M(p^n)$ elements. The second half of the proof of (2.5) there argued, in effect, that therefore each p-subgroup of $C(p)$ wr (Sym p^n) with transitive top projection can be generated by $M(p^n) + f(p^n)$ elements. Using Lemma 2.1, induction on e readily extends this argument to a proof of the following.

LEMMA 2.2. *If P is a transitive p-group of degree p^n viewed as a group of permutation matrices over $\mathbb{Z}/p^e\mathbb{Z}$, then each submodule of the natural module for P can be generated by $eM(p^n)$ elements.*

LEMMA 2.3. *Each p-subgroup of $C(p^e)$* wr (Sym p^n) *with transitive top projection can be generated by $eM(p^n) + f(p^n)$ elements.*

Remark. These results will do here for $n \geq e$, but they are unlikely to be best possible. Set $(1 + x + \cdots + x^{p-1})^n = \sum u(m, n)x^m$, so in particular $M(p^n) = u([(p-1)n/2], n)$. It seems plausible that *in Lemma* 2.2 *one*

could replace $eM(p^n)$ *by* $\max_k \sum_{i=0}^{e-1} u(k+i(p-1), n)$. This is certainly so when $e = 1$ (for then it is no improvement) and also when $n < e$ (for then it agrees with the next lemma). On the other hand, it is not hard to see (considering elementary abelian P) that no stronger statement could be hoped for.

LEMMA 2.4. *If P is a transitive p-group of degree p^n viewed as a group of permutation matrices over $\mathbb{Z}/p^e\mathbb{Z}$, then each submodule of the natural module for P can be generated by $1 + (p^n - 1)/(p - 1)$ elements.*

Before proving this, we note that an obvious analogue of the deduction of Lemma 2.3 from Lemma 2.2 will yield the following conclusion.

LEMMA 2.5. *Each finite p-subgroup of $C(p^\infty)$ wr (Sym p^n) with transitive top projection can be generated by $1 + (p^n - 1)/(p - 1) + f(p^n)$ elements.*

Proof of Lemma 2.4. Let $\mathbb{Q}$ stand for the field of rational numbers and $\mathbb{Z}_{(p)}$ for the localization of the integers at the prime p, and let U be a nontrivial irreducible $\mathbb{Q}C(p)$-module. Then $\dim U = p - 1$. We shall make use of the well known fact that each $\mathbb{Z}_{(p)}C(p)$-submodule of each finitely generated $\mathbb{Z}_{(p)}C(p)$-submodule of U is *monogenic* in the sense that it can be generated by a single element. [As we have not been able to locate a convenient reference, we sketch a proof. Write R for the quotient of $\mathbb{Z}_{(p)}C(p)$ modulo the kernel of its action on U, and g for the image in R of a generator of $C(p)$. Check that the ideal generated by $g - 1$ is the only maximal ideal in R, and therefore argue that in this noetherian ring each (nonzero, proper) ideal is generated by some power of $g - 1$. Note that R has the same $\mathbb{Z}$-rank as U, and that U is torsion-free as R-module. Conclude first that all finitely generated R-submodules of U are R-free, and then that all R-submodules of the latter are also R-free. Finally, compare $\mathbb{Z}$-ranks to see that no R-free R-submodule of U can have R-free rank greater than 1.]

Next, let P be a finite p-group and V a nontrivial irreducible $\mathbb{Q}P$-module. There is then a subgroup, C say, between P and the kernel of the action of P on V, such that modulo that kernel C is central and of order p. By Clifford's Theorem, as $\mathbb{Q}C$-module V is the direct sum of $(\dim V)/(p - 1)$ nontrivial irreducibles. It follows that each finitely generated $\mathbb{Z}_{(p)}C$-submodule of V lies in a direct sum of $(\dim V)/(p - 1)$ modules, each submodule of each direct summand being monogenic. By repeated application of Lemma 2.1, one may now conclude that each finitely generated $\mathbb{Z}_{(p)}C$-submodule of V can be generated by $(\dim V)/(p - 1)$ elements. The same holds, of course, for all finitely

generated $\mathbb{Z}_{(p)}P$-submodules of V, even if V is not irreducible, as long as V has no trivial direct summand.

Finally, let P be a transitive group of permutation matrices of degree p^n over $\mathbb{Z}_{(p)}$, and W the natural $\mathbb{Z}_{(p)}P$-module. Then $W \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q}$ is a direct sum of a 1-dimensional trivial $\mathbb{Q}P$-module and a $\mathbb{Q}P$-module which has no trivial direct summand. As each $\mathbb{Z}_{(p)}P$-submodule of W is a finitely generated $\mathbb{Z}_{(p)}P$-submodule of $W \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q}$, one more appeal to Lemma 2.1 yields that each $\mathbb{Z}_{(p)}P$-submodule of W can be generated by $1 + (p^n - 1)/(p - 1)$ elements. This property is clearly inherited by W/p^eW. In view of $\mathbb{Z}_{(p)}/p^e\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^e\mathbb{Z}$, the proof is now complete.

LEMMA 2.6. *If D is any group of order p^k and G is a subgroup of D wr (Sym p^l) with transitive top projection, then G can be generated by $kM(p^l) + f(p^l)$ elements.*

Proof. Let E be a central subgroup of order p in D. The natural homomorphism of D onto D/E has a natural extension to a homomorphism of D wr (Sym p^l) onto (D/E) wr (Sym p^l); the kernel, K say, of that homomorphism is central in the base group, and as a module for the top group (Sym p^l) it is the natural permutation module over $\mathbb{Z}/p\mathbb{Z}$. If $E = D$, the claim is just the special case of Lemma 2.3 quoted from [2] above, so we have the initial step for a proof by induction on k. From the corresponding special case of Lemma 2.2 we know that, as a G-module, $G \cap K$ can be generated by $M(p^l)$ elements; on the other hand, the inductive hypothesis is clearly applicable to $G/(G \cap K)$: so that proof is complete.

LEMMA 2.7. *If P is a subgroup of* (Sym 2) wr (Sym 2^{n-m}) *with transitive top projection, then P is isomorphic either to that top projection or to a transitive subgroup of* Sym 2^{n-m+1}.

Proof. Consider (Sym 2) wr (Sym 2^{n-m}) a subgroup of Sym 2^{n-m+1} with a system of imprimitivity consisting of blocks of cardinality 2. By assumption, P permutes these blocks transitively, so each orbit of P on the 2^{n-m+1} points meets each block nontrivially. Thus if P has more than one orbit, it must have precisely two orbits, each containing precisely one point from each block: but then an element of P fixing each block setwise must fix each of them pointwise, so in this case P is isomorphic to that top projection.

LEMMA 2.8. *Let D be a 2-group with a cyclic or quasicyclic subgroup C of index 2. If G is a subgroup of D* wr (Sym 2^{n-m}) *with transitive top projection, then G can be generated by $2^{n-m} + f(2^{n-m+1})$ elements.*

Proof. Write A for the direct product of the 2^{n-m} 'coordinate copies' of C in the base group of that wreath product. This A is a normal

subgroup of the wreath product D wr (Sym 2^{n-m}); set $B = AG$. The quotient of that wreath product over A may be thought of as (Sym 2) wr (Sym 2^{n-m}), in such a way that the top projection of B/A is transitive. Obviously $A \cap G$, like every subgroup of A, can be generated by 2^{n-m} elements. From Lemma 2.7 we know that B/A is a transitive 2-group of degree 2^{n-m} or 2^{n-m+1}, so it can certainly be generated by $f(2^{n-m+1})$ elements.

3. Proof of Theorem 1.2

We are now ready to prove Theorem 1.2 modulo one result whose proof will be deferred to the last section.

LEMMA 3.1. *There is a constant c_0 such that $M(p^n) < c_0 p^{n-1}/\sqrt{n}$ for every prime p and every positive integer n.*

Theorem 1.2 will be proved with $c_1 = c_0\sqrt{6}$. Since $(n+1)/n \leq \frac{3}{2}$ when $n \geq 2$, we can make use of Lemma 3.1 via the following.

COROLLARY 3.2. *If p is a prime and $n \geq 2$, then*

$$M(p^n) < 2M(p^n) < c_1 p^{n-1}/\sqrt{(n+1)}.$$

Let G be as in Theorem 1.2. Then Theorem 2.0 applies; we take up its notation and case distinctions. Note that from $d = p^n f(p, \mathbb{F})$ it follows that

$$a(p, \mathbb{F})d + 2 = p^n/(p-1) + 2 \tag{1}$$

and

$$b(p, \mathbb{F})d/\sqrt{\log d} \geq p^{n-1}/(p-1)\sqrt{(n+1)} \tag{2}$$

(because $d \leq p^{n+1}$ by the comments after Definition 1.1).

It is easy to deduce from Theorem 2.0 that if $n = 0$ or if we are in case (iii) and $n - m = 0$, then either G is cyclic or G is a 2-generator 2-group. Similarly, if $n = 1$ or if we are in case (iii) and $n - m = 1$, then either G can be generated by 3 elements or G is a 4-generator 2-group. The additive constants in Theorem 1.2 have been chosen generously enough to ensure that, in view of (1), there is no work to be done in these situations. For the rest of the proof we can therefore assume that $n \geq 2$, and in case (iii) also $n - m \geq 2$.

We shall use repeatedly that, by (2.1) of **[2]**,

$$f(p^n) \leq \frac{2}{p-1} M(p^n) \quad \text{whenever } n \geq 2. \tag{3}$$

For case (i), Theorem 1.2 already follows from Lemmas 2.5 and 2.3 and Corollary 3.2.

Two other references will also be needed several times:

$$f(p^n) \leq f(p^{n-1}) + M(p^{n-1}) \quad \text{whenever } n \geq 2 \tag{4}$$

by (2.5) of [**2**], while

$$f(2^n) \leq 2^{n-1} \quad \text{whenever } n \geq 2 \tag{5}$$

by Lemma 2.2 of Ronse [**5**].

In the remaining cases, $p = 2$ and therefore

$$e(p, \mathbb{F}) \geq 2. \tag{6}$$

Consider case (ii) next; then G can be generated by $f(2^{n+2})$ elements. In view of (1) and (2), the first claim of Theorem 1.2 holds because

$$\begin{aligned} f(2^{n+2}) &\leq f(2^{n+1}) + M(2^{n+1}) && \text{by (4)}, \\ &\leq 2^n + M(2^{n+1}) && \text{by (5)}, \\ &\leq 2^n + c_0 2^n/\sqrt{(n+1)} && \text{by Lemma 3.1}, \\ &\leq 2^n + c_1 2^n/\sqrt{(n+1)}. \end{aligned}$$

The second case also holds, because

$$\begin{aligned} f(2^{n+2}) &\leq 2M(2^{n+2}) && \text{by (3)}, \\ &< c_1 2^{n+1}/\sqrt{(n+3)} && \text{by Corollary 3.2}, \\ &< 4c_1 2^{n-1}/\sqrt{(n+1)} \\ &\leq (e(p, \mathbb{F}) + 2) c_1 2^{n-1}/\sqrt{(n+1)} && \text{by (6)}. \end{aligned}$$

In case (iii), we know from Lemma 2.8 that G can be generated by $2^n + M(2^{n+1})$ elements. In view of (1) and (2),

$$\begin{aligned} f(2^{n+1}) &\leq 2M(2^{n+1}) && \text{by (3)}, \\ &\leq 2c_0 2^n/\sqrt{(n+1)} && \text{by Lemma 3.1}, \\ &\leq c_1 2^n/\sqrt{(n+1)} \end{aligned}$$

therefore proves the first statement of Theorem 1.2. For the proof of the second statement, we apply Lemma 2.6 to deduce that G can be generated by $(m + e(2, \mathbb{F}) + 1)M(2^{n-m}) + f(2^{n-m})$ elements, and then use (3) to conclude that $(m + e(2, \mathbb{F}) + 3)M(2^{n-m})$ suitable elements will generate G. From (3.1) of [**2**] we know that

$$M(2^{n-m}) \leq (\tfrac{2}{3})^m M(2^n),$$

while of course

$$(e(2, \mathbb{F}) + 2)(\tfrac{2}{3})^m \leq e(2, \mathbb{F}) + 2$$

and

$$(m+1)(\tfrac{2}{3})^m < 2 < e(2, \mathbb{F}) + 2,$$

so it follows that G can be generated by $(e(2, \mathbb{F}) + 2)2M(2^n)$ elements. In view of (2) and Corollary 3.2, this completes the proof.

4. Proof of Theorem 1.3

We start by recalling the relevant construction from [2]. Let A be an elementary abelian group of order p^n with $n > 1$; write R for the radical of the group algebra $\mathbb{F}_pA$, and G for the semidirect product of A and R^m with $m = [(p-1)n/2]$. The centralizer of R^m in A must be a characteristic subgroup of A; and it cannot be A, for the largest trivial submodule of $\mathbb{F}_pA$ has dimension 1 while $\dim (R^m/R^{m+1}) = M(p^n) > 1$ by (3.2) of [2]. It follows first that R^m is its own centralizer in G, and then that the centre of G has order p: so G has only one minimal normal subgroup.

In view of the paragraph introducing Theorem 1.3, our task is to show that this G has, over any field $\mathbb{F}$ whose characteristic is different from p, a faithful irreducible representation of degree at most p^{n+1}. Since G is a p-subgroup of $C(p)$ wr Sym p^n, over such an $\mathbb{F}$ it has a faithful completely reducible representation of degree $f(p, \mathbb{F})p^n$. As we noted, $f(p, \mathbb{F}) \leq p$. If no irreducible constituent of this representation were faithful, their kernels would all have to contain the only minimal normal subgroup of G, so the direct sum of these constituents would not be faithful either. At least one of these constituents is therefore a faithful irreducible representation, and has degree at most p^{n+1}.

5. Proof of Theorem 1.4

It will be convenient here to give a new construction for the relevant examples of Isaacs [1].

Let $\mathbb{F}$ be an arbitrary field, p a prime different from the characteristic of $\mathbb{F}$, and n an integer such that $2 \leq n+1 \leq e(p, \mathbb{F})$. Consider an elementary abelian group A of order p^n: then A has $(p^n - 1)/(p-1)$ maximal subgroups B. In the integral group ring $\mathbb{Z}A$, set

$$u_A = \sum_{a \in A} a \quad \text{and} \quad u_B = -u_A + p \sum_{b \in B} b.$$

It is straightforward to verify that

$$u_A^2 = p^n u_A \notin p^{n+1}\mathbb{Z}A,$$

$$u_B^2 = p^n u_B \notin p^{n+1}\mathbb{Z}A,$$

$$u_A u_B = u_{B_1} u_{B_2} = 0 \quad \text{whenever } B_1 \neq B_2, \text{ and}$$

$$u_A + \sum_B u_B = p^n.$$

Let U denote the $\mathbb{Z}A$-submodule generated in $\mathbb{Z}A$ by u_A and the $(p^n-1)/(p-1)$ elements u_B (one for each maximal subgroup B of A). The last displaced equation implies that $U \geqslant p^n\mathbb{Z}A$. Set $V = U/p^{n+1}\mathbb{Z}A$: this quotient cannot be generated by any proper subset of the generating set it inherits from U [for, the submodule generated by a subset excluding $u_B + p^{n+1}\mathbb{Z}A$, say, is annihilated by u_B while $u_B + p^{n+1}\mathbb{Z}A$ itself is not]. The intersection of the maximal submodules can be omitted from each module generating set, so the claim of the previous sentence also holds for the largest semisimple quotient $V/\operatorname{rad} V$ of V. Since A and V are both p-groups, $V/\operatorname{rad} V$ is an elementary abelian group with trivial A-action. In such a module, the size of any irredundant generating set is the minimal number of generators. We can therefore conclude that $V/\operatorname{rad} V$ cannot be generated by $(p^n-1)/(p-1)$ elements. It follows that the semidirect product, G say, of A and V has an elementary abelian quotient which cannot be generated by $n + (p^n-1)/(p-1)$ elements, and so neither can G.

Consider the normal subgroup $\Omega_1(V)$ of G consisting of the elements of V which have order at most p. As $U \geqslant p^n\mathbb{Z}A$, we have $\Omega_1(V) = p^n\mathbb{Z}A/p^{n+1}\mathbb{Z}A$. In particular, it follows that V is its own centralizer in G.

The map $\mathbb{Z}A \to \mathbb{Z}$, $\sum_{a\in A} z_a a \mapsto z_1$ yields a homomorphism $\varphi\colon V \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ which is nontrivial on $\Omega_1(V)$; this φ is surjective, because $(u_A + p^{n+1}\mathbb{Z}A)\varphi = 1 + p^{n+1}\mathbb{Z}$. It is easy to see also that $\Omega_1(V) \cap \ker\varphi$ contains no nontrivial normal subgroup of G, and that the normalizer of this intersection in G is just V.

Now let $\rho\colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to GL(f(p,\mathbb{F}),\mathbb{F})$ be a faithful irreducible representation, and consider the composite map $\varphi\rho$ as an irreducible representation of the normal subgroup V of G. The inertia group of $\varphi\rho$ in G is V itself, because that inertia group must normalize $\Omega_1(V) \cap \ker\varphi$. It follows that the representation of G induced from $\varphi\rho$ is irreducible. The kernel of the induced representation intersects $\Omega_1(V)$ in a normal subgroup of G contained also in $\ker\varphi$, so this intersection is trivial. Thus the kernel of the induced representation avoids the self-centralizing normal subgroup V and therefore must be trivial.

This proves that the group G, which cannot be generated by $n + (p^n-1)/(p-1)$ elements, has a faithful irreducible representation of degree $p^n f(p,\mathbb{F})$ over $\mathbb{F}$.

6. Proof of Corollary 1.7

If each Sylow subgroup of a finite nilpotent group can be generated by n elements, so can the group itself, Corollary 1.7 will therefore be proved

if we show that to each positive ε there is an N (depending only on ε and $\mathbb{F}$) which, for each prime p, has the following property:

(P) each finite irreducible linear p-group of degree at most d over $\mathbb{F}$ can be generated by $(m_{\mathbb{F}} + \varepsilon)d + N$ elements.

For, if G is a finite nilpotent group with a faithful irreducible representation over $\mathbb{F}$, then the restriction of that representation to a Sylow subgroup is a direct sum of pairwise equivalent irreducibles which must therefore all be faithful: thus by (P) each Sylow subgroup of G can be generated by $(m_{\mathbb{F}} + \varepsilon)d + N$ elements.

Let $\mathbb{F}$ be an arbitrary field. It is immediate from Definition 1.1 that $b(p, \mathbb{F}) \leq 1$ for all p. This, Definition 1.6, and the first half of Theorem 1.2, together yield that a number N will have (P) for all p with $e(p, \mathbb{F}) = \infty$ provided

$$(m_{\mathbb{F}} + \varepsilon)d + N \geq m_{\mathbb{F}}d + 2c_1 d/\sqrt{\log d + 2} \quad \text{for all positive } d.$$

From Definition 1.1 we see that $a(p, \mathbb{F}) \leq 1/(p-1)$; hence the first half of Theorem 1.2 also yields that N has (P) for all p with $1/(p-1) \leq \varepsilon/2$ provided

$$(m_{\mathbb{F}} + \varepsilon)d + N \geq (\varepsilon/2)d + 2c_1 d/\sqrt{\log d + 2} \quad \text{for all positive } d.$$

This leaves finitely many primes p with $e(p, \mathbb{F}) < \infty$ to consider. By the second half of Theorem 1.2, N has (P) for such a p provided

$$(m_{\mathbb{F}} + \varepsilon)d + N \geq ((p-1)e(p, \mathbb{F}) + 2)b(p, \mathbb{F})c_1 d/\sqrt{\log d + 4}$$

for all positive d.

The three displayed conditions on N (the last being required for finitely many primes) are clearly compatible: they all hold for all sufficient large N.

7. Proof of Corollary 1.8

The only thing to prove is the claim that if $\mathbb{F}$ has finite degree over its prime subfield then

$$\frac{e(p, \mathbb{F})}{f(p, \mathbb{F})} \frac{\sqrt{\log p}}{p}$$

has an upper bound which (may depend on $\mathbb{F}$ but) is independent of p. In proving that a function of p is bounded one may disregard its value at $p = 2$: this will be convenient later. Consider first the case of finite $\mathbb{F}$; say, of $\mathbb{F}$ with cardinality q. Then $p^{e(p,\mathbb{F})}$ divides $q^{f(p,\mathbb{F})} - 1$ whenever $p \nmid q$, so

$e(p, \mathbb{F}) \log p < f(p, \mathbb{F}) \log q$ and hence

$$\frac{e(p, \mathbb{F})}{f(p, \mathbb{F})} \frac{\sqrt{\log p}}{p} < \frac{\log q}{p\sqrt{\log p}} \leq \frac{\log q}{2\sqrt{\log 2}}$$

for every relevant p. Next, suppose that $p > 2$ and $\mathbb{F}$ is a finite extension of the rational field $\mathbb{Q}$: as noted after Definition 1.1, then $|\mathbb{F}(\sqrt[p]{-1}): \mathbb{F}| \leq p - 1$. By that definition, this field contains a cyclic multiplicative subgroup of order $p^{e(p,\mathbb{F})}$. The unique smallest extension of $\mathbb{Q}$ to contain such a subgroup has degree $(p-1)p^{e(p,\mathbb{F})-1}$: so

$$(p-1)p^{e(p,\mathbb{F})-1} \leq |\mathbb{F}(\sqrt[p]{-1}): \mathbb{Q}| \leq (p-1)\,|\mathbb{F}: \mathbb{Q}|.$$

This proves that $e(p, \mathbb{F}) \leq 1 + (\log |\mathbb{F}: \mathbb{Q}|)/(\log p) \leq 1 + (\log |\mathbb{F}: \mathbb{Q}|)/(\log 2)$.

8. Proof of Corollary 1.9

Let φ denote Euler's function, as usual. If m is a positive integer, then there are precisely $\varphi(m)$ complex numbers of multiplicative order m, and adjoining any one of these to the rational field $\mathbb{Q}$ gives a field $\mathbb{Q}(\sqrt[m]{1})$ which contains them all and so depends only on m, and whose degree over $\mathbb{Q}$ is $\varphi(m)$. From the multiplicative property of φ one can see that if m is even and n is a multiple of m then $\varphi(m) < \varphi(n)$ and so $\mathbb{Q}(\sqrt[m]{1}) < \mathbb{Q}(\sqrt[n]{1})$. It follows that if m is even then the torsion part of the multiplicative group of $\mathbb{Q}(\sqrt[m]{1})$ has order precisely m.

For each prime p, choose a positive integer $e(p)$, subject at first only to the condition that $e(2) > 1$. For each positive integer k, let $m(k) = \prod_{p \leq k} p^{e(p)}$. Then each $\mathbb{Q}(\sqrt[m(k)]{1})$ has precisely $m(k)$ elements of finite multiplicative order, and these fields form an ascending chain. Let $\mathbb{F}$ be their union: then clearly $f(p, \mathbb{F}) = 1$ and $e(p, \mathbb{F}) = e(p)$ for all p; in particular, $m_{\mathbb{F}} = 0$. If $e(p) > 1$ for all p, then for each p there is, by Theorem 1.4, a finite irreducible linear p-group of degree $p^{e(p)-1}$ which cannot be generated by $(p^{e(p)-1} - 1)/(p-1)$ elements. Given a sequence $r(1), \ldots, r(d), \ldots$ as in Corollary 1.9, restricting the choice of the $e(p)$ so that also $r(p^{e(p)-1}) < 1/(p-1)$ will therefore yield a field $\mathbb{F}$ for which the claim of that corollary holds.

9. Proof of Lemma 3.1

Since $M(p) = 1$ and since it was shown on p. 369 of [2] that

$$\frac{M(p^n)}{p^n} = \frac{1}{2\pi} \int_0^{\pi/2} \left(\frac{\sin px}{p \sin x}\right)^n dx$$

it will suffice to prove the existence of a number C such that

$$\int_0^{\pi/2} \left(\frac{\sin px}{p \sin x}\right)^n dx < C/p\sqrt{n} \quad \text{whenever } p \geq 2 \text{ and } n \geq 2.$$

To this end, set

$$h(u) = \frac{\sin u}{u} e^{u^2/6}$$

and verify that h is decreasing on the interval $(0, \pi/2]$, whence $h(x) \geq h(px)$ whenever $p \geq 1$ and $x \in (0, \pi/2p]$. This yields that on the latter interval

$$0 < \frac{\sin px}{p \sin x} \leq e^{-(p^2-1)x^2/6}$$

and therefore

$$\int_0^{\pi/2p} \left(\frac{\sin px}{p \sin x}\right)^n dx < \int_0^{\infty} e^{-n(p^2-1)x^2/6} dx$$

$$= \frac{1}{\sqrt{\{n(p^2-1)\}}} \int_0^{\infty} e^{-t^2/6} dt \quad \text{with} \quad t = x\sqrt{\{n(p^2-1)\}}$$

$$\leq \frac{C_1}{p\sqrt{n}} \quad \text{with} \quad C_1 = \frac{2}{\sqrt{3}} \int_0^{\infty} e^{-t^2/6} dt$$

whenever $p \geq 2$. On the other hand, $|\sin px| \leq 1$ and $0 < \sin x < 2x/\pi$ on $(0, \pi/2)$, so on this interval

$$\left|\frac{\sin px}{p \sin x}\right| \leq \frac{1}{p\,|\sin x|} < \frac{\pi}{2px};$$

therefore

$$\int_{\pi/2p}^{\pi/2} \left(\frac{\sin px}{p \sin x}\right)^n dx = \int_{\pi/2p}^{\pi/2} \left(\frac{\pi}{2px}\right)^n dx$$

$$= \frac{\pi}{2p(n-1)} - \frac{\pi}{2p^n(n-1)} < \frac{C_2}{p\sqrt{n}}$$

with $C_2 = \pi/\sqrt{2}$, whenever $p \geq 1$ and $n \geq 2$.

This completes the proof of Lemma 3.1, and so also the proof of Theorem 1.2.

REFERENCES

1. I. M. Isaacs, 'The number of generators of a linear p-group', *Canad J. Math* 24 (1972), 851–858.
2. L. G. Kovács and M. F. Newman, 'Generating transitive permutation groups', *Quarterly J. Math. Oxford* (2) 39 (1988), 361–372.
3. L G. Kovács and Geoffrey R. Robinson, 'Generating finite completely reducible linear groups', *Proc. Amer Math. Soc.* 112 (1991), 357–364.
4. C. R. Leedham-Green and W Plesken, 'Some remarks on Sylow subgroups of general linear groups', *Math. Z.* 191 (1986), 529–535.
5. Christian Ronse, 'On permutation groups of prime power order', *Math. Z.* 173 (1980), 211–215.

Department of Mathematics
Carleton University
Ottawa
Ontario K1S 5B6
Canada

Mathematics IAS
Australian National University
GPO Box 4
Canberra ACT 2601
Australia