SOME NORMALLY MONOMIAL p-GROUPS OF MAXIMAL CLASS AND LARGE DERIVED LENGTH

By L. G. KOVÁCS AND C. R. LEEDHAM-GREEN

[Received 13th February 1985]

1. A group of prime-power order p^m is obviously nilpotent of class at most $m-1$; if it has class precisely $m-1$, it is said to be of maximal class. The derived length of a p-group of maximal class is bounded by $\log_2(3p-3)$ if p is odd and by 2 if $p=2$. Indeed, if $m \geqslant 9p-40$, the derived length is at most 3 (Shepherd [**6**], Leedham-Green and McKay [**5**].) The question of whether there is an unconditional bound independent of p was answered in the negative, in a 1975 letter by Dr Shepherd to the second author. The pursuit of refinements and generalizations of the positive results mentioned above has continued with increasing momentum but, despite its importance, the negative result appears to have remained unpublished.

In this note we construct groups which prove Shepherd's claim (and are presumably those he had had in mind). What prompts us now is that these groups also answer a question which has arisen more recently. In his thesis [**1**], Guan Aun How investigated nM-groups: finite groups whose irreducible (complex) characters are all induced from linear characters of normal subgroups. He gave a characterization of these groups in purely structural terms (that is, without reference to characters). This enabled him to prove that the Frattini factor group is a direct product of groups which are either cyclic or Frobenius groups (whose kernels are abelian and) whose complements have cyclic derived groups. However, this characterization has so far proved frustratingly difficult to use on p-groups; for instance, the question of whether there is a bound on the derived lengths of nM-groups has remained open even for nilpotent groups.

The groups we present in this note show that there is no such bound. Namely, we construct, for each prime p, an nM-group of order p^p, exponent p, class $p-1$, and derived length the integer part of $\log_2(p+1)$. We also show that variants of these groups occur as kernels of Frobenius groups (with nonnilpotent complements) which are nM-groups, so even the metanilpotent residual of an nM-group can have arbitrarily large derived length. The constructions use Lie ring methods which were elaborated by M. Lazard in [**4**].

The maximal class groups above are perhaps the most complicated

p-groups with accessible character tables. In a subsequent paper [**3**], M. F. Newman and the first author explicitly calculate the irreducible characters and discuss some other remarkable properties of these groups.

The relevant special case of How's criterion ([**2**], or Lemma 5.2 in [**1**]) may be paraphrased as follows. Let G be a finite group with a unique minimal normal subgroup N, and A an abelian normal subgroup of maximal order in G. If G/N is an nM-group and if $N \leqslant [A, g]$ whenever g is an element of G outside A, then G is an nM-group. We shall also use part of Theorem 3.8 of his [**1**]: if F is a Frobenius group whose kernel is abelian and whose complement has cyclic derived group, then F is an nM-group.

2. Trivial examples exist when $p \leqslant 3$, so take $p > 3$. Let m be an integer with $3 \leqslant m \leqslant p$. Suppose that $g_1, \ldots, g_m$ are elements of a group G and that the following hold.

(1) Each element of G may be written uniquely as $g_1^{\alpha(1)} \cdots g_m^{\alpha(m)}$ with $0 \leqslant \alpha(i) \leqslant p-1$.

(2) $g_1^p = \cdots = g_m^p = 1$.

(3) $$[g_i, g_j] = \begin{cases} g_{i+j}^{i-j} \prod g_k^{\gamma(i,j,k)} & \text{if} \quad i+j \leqslant m \\ 1 & \text{if} \quad i+j > m \end{cases}$$

where the product is taken over $k = i+j+1, \ldots, m$ and the $\gamma(i, j, k)$ are suitable integers.

We defer for the moment the construction which meets these conditions, and show first that such a group must be an nM-group of derived length $[\log_2 (m+1)]$.

The first point to note is that the centre $Z(G)$ is just the subgroup $\langle g_m \rangle$ generated by g_m. Indeed, if $g \in G \backslash \langle g_m \rangle$ then $g = g_k^{\alpha(k)} \cdots g_m^{\alpha(m)}$ with $k < m$ and $0 < \alpha(k) \leqslant p-1$; hence it is easy to see that $[g, g_1] \neq 1$ when $k \neq 1$ and $[g, g_2] \neq 1$ when $k = 1$. (It is perhaps even easier to see that $[g, g_{m-k}] \neq 1$.) Next observe that $G/Z(G)$ is either of order p^2 or a group just like G with m replaced by $m-1$, so induction on m readily yields that the normal non-maximal subgroups of G are precisely the subgroups $\langle g_d, \ldots, g_m \rangle$ with $d \geqslant 3$.

In particular, the nonabelian proper factor groups of G are all just like G with m replaced by some smaller integer. Thus the paraphrase of How's criterion is well suited for a proof by induction on m of the claim that G is an nM-group. From the list of the normal subgroups of G we see that A can be taken as $\langle g_d, \ldots, g_m \rangle$ with $d = [(m+1)/2]$ (and indeed this is the only choice when $m > 3$). All we are required to show is that $Z(G) \leqslant [A, g]$ whenever $g \in G \backslash A$. Write $g = g_k^{\alpha(k)} \cdots g_m^{\alpha(m)}$ with $0 < \alpha(k) \leqslant p-1$; then $k \leqslant d-1$ and so, as $m \geqslant 2d-1$, we have $m-k \geqslant d$; hence $g_{m-k} \in A$ and $[g_{m-k}, g] = g_m^{(m-2k)\alpha(k)} \in [A, g]$. Since $p > m-2k \geqslant m-2(d-1) > 0$, we are done.

The list of the normal subgroups of G makes it easy to calculate the derived length of G. By (3), $\langle g_4, \ldots, g_m\rangle$ cannot contain G' but $\langle g_3, \ldots, g_m\rangle$ does, so $G' = \langle g_3, \ldots, g_m\rangle$. Introduction on k yields that $G^{(k)} = \langle g_d, \ldots, g_m\rangle$ with $d = 2^{k+1} - 1$. Thus the derived length of G is $[\log_2 (m+1)]$.

3. We have to establish the existence of G and $g_1, \ldots, g_m$ which satisfy (1), (2), (3). If such a G exists, the Lie ring U defined in the usual manner on the direct sum of the lower central factors of G will have an additive basis $u_1, \ldots, u_m$ such that

$$(u_i, u_j) = \begin{cases} (i-j)u_{i+j} & \text{if} \quad i+j \leq m, \\ 0 & \text{if} \quad i+j > m. \end{cases} \tag{4}$$

It is straightforward to check that (4) does indeed define a Lie ring on the additively written elementary abelian p-group with basis $u_1, \ldots, u_m$; we shall use this Lie ring U for the construction of our group G. An abstract procedure described in Lazard's thesis [**4**] could be used to this effect, but one can just as easily appeal to a concrete and classical method.

Suppose first that $m < p$. Consider $(m+1)$-by-$(m+1)$ matrices over the field of order p, with $e(i, j)$ denoting the matrix whose only nonzero entry is a 1 in the i, j position. Put

$$u_i = \sum_{k=1}^{m+1-i} ke(k, k+i)$$

and verify that these matrices satisfy (4) with respect to the Lie product $(x, y) = xy - yx$: thus we have realized U as a Lie subring of the associative ring T of the nilpotent upper triangular matrices. Note that T itself is nilpotent, with $T^m > T^{m+1} = 0$; in particular, $T^p = 0$. If $t \in T$, the usual power series for $\exp t$ makes sense (division by p not being called for until the powers of t vanish) and is finite, so $\exp t$ is a well-defined element of the multiplicative group $1 + T (= \{1 + t \mid t \in T\})$ of upper unitriangular matrices. Put $g_i = \exp u_i$ and $G = \{\exp u \mid u \in U\}$; by the Baker–Campbell–Hausdorff Theorem G is closed under multiplication and is therefore a subgroup of $1 + T$. As is well known, the $1 + T^k$ form a chain of normal subgroups of $1 + T$; clearly, $g_k \in 1 + T^k$ but $g_k \notin 1 + T^{k+1}$ (as $\{e(i, j) \mid i + k \leq j\}$ is an additive basis of T^k). Thus the $G \cap (1 + T^k)$ form a chain of $m+1$ pairwise distinct normal subgroups in G. By definition, $|G| \leq |U| = p^m$, so in fact $|G| = p^m$; one can now readily see that

$$G \cap (1 + T^k) = \langle g_k\rangle [G \cap (1 + T^{k+1})],$$

whence

$$G \cap (1 + T^k) = \langle g_k, \ldots, g_m\rangle,$$

and (1) follows. It is a formal property of the power series for exp that

$$(\exp t)^k = \exp(kt); \tag{5}$$

hence (2) also holds. To verify (3), one calculates formally (that is, without using explicit matrix forms) that

$$\begin{aligned}[\exp x, \exp y] &= \exp(-x)\exp(-y)\exp x \exp y\\ &= 1 + (x, y) + z\end{aligned}$$

where z is a sum of associative products with factors from the set $\{x, y\}$, each product having each of x and y among its factors at least once, and at least one of x and y at least twice. In particular

$$[g_i, g_j] = 1 + (u_i, u_j) + v \quad \text{with} \quad v \in T^{i+j+1}.$$

On the other hand, by (5)

$$g_{i+j}^{j-i} = 1 - (i-j)u_{i+j} + w \quad \text{with} \quad w \in T^{2(i+j)} \leqslant T^{i+j+1}.$$

Hence by (4) and easy direct calculation

$$g_{i+j}^{j-i}[g_i, g_j] \in 1 + T^{i+j+1},$$

and (3) follows.

The hitherto excluded case $m = p$ can be dealt with in the same way after verifying that for the associative subring R of T generated by U one has $R^p = 0$ even then: this was all we really used.

4. It is more convenient to describe the promised Frobenius groups in terms of the abstract procedure of Lazard [4]. We shall apply that to a certain Lie ring U and a group K of automorphisms of U; we construct U and K first.

Let $\mathbb{F}$ be a finite field of order p^r, and m an integer with $3 \leqslant m < p$, both to be specified later. Take the Lie algebra over $\mathbb{F}$ with $\mathbb{F}$-basis $u_1, \ldots, u_m$ and multiplication defined by (4); forgetting $\mathbb{F}$ we obtain a nilpotent Lie ring U of characteristic p and nilpotency class less than p. Let Aut U be the automorphism group of U (note the elements of Aut U are not required to be $\mathbb{F}$-linear). The elements of U may be written uniquely as $\sum \varphi_i u_i$ with $\varphi_i \in \mathbb{F}$. For each nonzero φ in $\mathbb{F}$, define $\bar{\varphi}\colon U \to U$ by $(\sum \varphi_i u_i)\bar{\varphi} = \sum \varphi^i \varphi_i u_i$; check that $\bar{\varphi} \in \text{Aut } U$, and that $\varphi \mapsto \bar{\varphi}$ is an embedding of the multiplicative group $\mathbb{F}^+$of $\mathbb{F}$ in Aut U. Further, check that $\pi\colon\ U \to U$ defined by $(\sum \varphi_i u_i)\pi = \sum \varphi_i^p u_i$ is also an element of Aut U, and that $\pi^{-1}\bar{\varphi}\pi = \overline{\varphi^p} = \bar{\varphi}^p$ for all φ in $\mathbb{F}^\times$; clearly, the order of π is r.

We now specify our parameters further. Let r be a prime, $r > 3$; by Dirichlet's Theorem, there is a prime q such that $q \equiv 1 \bmod r$. Let s be an integer such that $s + q\mathbf{Z}$ has multiplicative order r in the field $\mathbf{Z}/q\mathbf{Z}$; again by Dirichlet's Theorem, we can choose a prime p such that $p \equiv q+s-qs \bmod qr$: so $p \equiv s \bmod q$ and hence

$$p \not\equiv p^r \equiv 1 \bmod q \quad \text{and} \quad p \equiv 1 \bmod r.$$

Let t be the largest integer such that r^t divides $p-1$; then r^{t+1} divides p^r-1. Finally, choose m so that $3 \leqslant m < r$ (and a fortiori $m < p$ and $m < q$). Note that as r can be chosen arbitrarily large, so can m.

Let ψ and ρ be elements of $\mathbb{F}$, of multiplicative orders q and r^{t+1}, respectively; then $\bar{\psi}$ and $\bar{\rho}$ commute; the cyclic subgroup they generate is normalized by π; and $\bar{\rho}^r$ commutes with π. As π has order r, it follows that the subgroup generated by π and $\bar{\rho}$ is an r-group of class 2. Put $\pi\bar{\rho} = \kappa$: then κ has order r^{t+1}, $\langle \kappa^r \rangle = \langle \bar{\rho}^r \rangle$, κ normalizes and κ^r centralizes $\langle \bar{\psi} \rangle$. Take K as the subgroup of Aut U generated by κ and $\bar{\psi}$. The only subgroups of prime order in K are $\langle \kappa^{r^t} \rangle (= \langle \bar{\rho}^{r^t} \rangle)$ and $\langle \bar{\psi} \rangle$, and (as $m < r$ and $m < q$) each of these acts fixed point free on U: hence each nontrivial element of K acts fixed point free. Note also that K is metacyclic but not nilpotent.

Each $\mathbb{F}u_i$ admits K but no proper additive subgroup of an $\mathbb{F}u_i$ does (because $\bar{\psi}$ acts on $\mathbb{F}u_i$ as ψ^i and $i \leqslant m < q$ implies that ψ^i generates $\mathbb{F}$ as ring). As the central element $\bar{\rho}^r$ of K acts by different scalars ρ^{ri} (from the prime field) on different $\mathbb{F}u_i$, the K-admissible additive subgroups of U are just the $\oplus \mathbb{F}u_i$ with the sum being over some subset of $\{1, \ldots, m\}$. (Here $m < r$ was used once more.) It follows that the K-admissible ideals of U are precisely the $\bigoplus_{i=d}^{m} \mathbb{F}u_i$ and $\bigoplus_{i \neq 2} \mathbb{F}u_i$, a K-admissible abelian ideal A of maximal order being obtained with $d = [(m+1)/2]$. If u is any element of U outside A, then $u = \sum_{i=k}^{m} \varphi_i u_i$ with $k < d$ and $\varphi_k \neq 0$, and $(A, u) \geqslant (\mathbb{F}u_{m-k}, u) = \mathbb{F}u_m$: in fact,

(6) each element of $\mathbb{F}u_m$ is of the form (a, u) with $a \in A$.

Now we are ready to apply the method elaborated in Chapter II (see Section 4 in particular) of Lazard [**4**]. This defines, for each nilpotent Lie ring U of characteristic p and nilpotency class less than p, a multiplicative group $U^\times$ on the set of elements of U, such that

(7) a subset is a subgroup (abelian normal subgroup) if and only if it is a Lie subring (abelian ideal);

(8) a permutation is a group automorphism if and only if it is a Lie ring automorphism;

(9) within an abelian Lie subring, group product and Lie ring sum are the same; and

(10) within any Lie subring of class 2, group commutator and Lie product are the same.

(Half of this is stated in Lazard's Theorem 4.6; the other half has to be read off the explicit definitions of the various operations.) It follows that the derived length of the group $U^{\times}$ and of the Lie ring U are the same: with our choice of U, this is clearly $[\log_2(m+1)]$. Further, K may be viewed as a group of automorphisms of $U^{\times}$, and the semidirect product F of $U^{\times}$ by K is then a Frobenius group with kernel $U^{\times}$ and (nonnilpotent) complement K. (Thus $U^{\times}$ is also the metanilpotent residual of F.) The unique minimal normal subgroup N of F is the unique minimal K-admissible ideal of U, namely $\mathbb{F}u_m$. The factor group F/N is just like F with m replaced by $m-1$, except when $m=3$. In that case F/N is a Frobenius group with abelian kernel and metacyclic complement: hence an nM-group by the result of How quoted at the end of our Section 1. The paraphrase of his criterion given there can now be used to prove, by induction on m, that F is an nM-group. The ideal A of U is now an abelian normal subgroup of maximal order in F; we are required to show that $N \leqslant [A, f]$ whenver $f \in F\backslash A$. If $f \notin U^{\times}$ then the centralizer of f in $U^{\times}$ is 1, hence $[A, f] = A \geqslant N$. If $f \in U^{\times}$ and $b \in N$ then by (6) there is an a in A such that $(a, f) = b$; as b is central in U, the Lie subring generated by a and f has class 2, so (10) applies: $b = (a, f) = [a, f] \in [A, f]$. This completes the proof.

Remark (added in proof, 25 September 1985). It has just been brought to our attention that groups like those presented in the first half of this paper were also constructed by B. A. Panfërov, ('Nilpotent groups with lower central factors of minimal ranks', *Algebra i Logika*, 19 (1980), 701–706).

REFERENCES

1. Guan Aun How, *Some classes of monomial groups*, PhD thesis, Australian National University, 1980.
2. Guan Aun How, 'Some classes of monomial groups' (PhD thesis abstract), *Bull. Austral. Math. Soc.* 22 (1980), 477–478.
3. L. G. Kovács and M. F. Newman, 'Some groups of maximal class' (in preparation).
4. M. Lazard, 'Sur les groupes nilpotents et les anneaux de Lie', *Ann. École Norm. Sup.* (3) 71 (1954), 101–190.
5. C. R. Leedham-Green and Susan McKay, 'On p-groups of maximal class I', *Quart. J. Math. Oxford* (2), 27 (1976), 297–311.
6. Raymond T. Shepherd, *p-groups of maximal class*, PhD thesis, University of Chicago, 1970.

Australian National University
GPO Box 4
Canberra ACT 2601

and

Queen Mary College
Mile End Road
London E1 4NS