GENERALISATIONS OF A CLASSICAL THEOREM ABOUT NILPOTENT GROUPS

BY

I. D. MACDONALD

1. Introduction

A classical problem in the theory of groups concerned the finite nonabelian groups of which every proper subgroup is abelian. Miller and Moreno considered this problem in 1903—see [10]—and Rédei gave a list of all such groups in his paper [11]. The corresponding problem with "abelian" replaced by "nilpotent" is the subject of [12] and [9], and in the many other generalisations attention has been concentrated on nonnilpotent groups; for instance, Suzuki in [13] showed that any finite simple group with every second maximal subgroup nilpotent has order 60.

The aim of the present paper is to generalise the classical problem in another direction—we study *nilpotent* groups of which every proper subgroup, or every m^{th} maximal subgroup, is nilpotent of given class, and while results can be found for infinite groups we shall keep matters simple by examining the finite case only.

The following facts can be assembled from [10], or deduced from Rédei's list in [11], or proved independently without hardship:

THEOREM. *Let G be a nonabelian group of order p^{r+1} in which every subgroup of order p^r is abelian. Then*

(i) *G is generated by two elements*;

(ii) *G has class* 2;

(iii) *$\gamma_2(G)$ has order p*;

(iv) *$G/\zeta_1(G)$ has order p^2*.

That is the theorem to be generalised. Two other points of interest emerge from Rédei's paper: there are two infinite sequences of these p-groups together with an exceptional 2-group namely the quaternion group of order 8; and ζ_1/γ_2 is unbounded.

In any group the product of normal subgroups with classes n_1 and n_2 respectively has class $n_1 + n_2$; that is a theorem of Fitting [2], and it is a best possible result because in [5], P. Hall gives an example, for any n, which is of class precisely n and which is the product of n abelian normal subgroups. (For what it is worth, we state that there are even metabelian groups with these properties.) Now, since every maximal subgroup of a finite p-group G is normal, G has class $2n$ when every proper subgroup has class n, and we ask when the class is precisely $2n$. This is certainly possible when $n = 1$,

Received May 27, 1963.

by the classical result. We shall prove

THEOREM 1. *Let G be a finite metabelian p-group of class precisely $2n$ with every proper subgroup of class n. Then $n = 1$.*

Without the metabelian assumption the problem is more intractable, though we shall show that the case $n = 2$ can never occur and we shall give an example for $n = 3$ in Theorem 4.

The other general result is

THEOREM 2. *Let G be a group of order p^{r+m} in which every subgroup of order p^r has class n, while G itself is not of class n. Then*

(i) *G has a set of at most $m + n$ generators;*
(ii) *the class of G is bounded by $f(m, n)$;*
(iii) *the order of $\gamma_{n+1}(G)$ is a factor of $p^{g(m,n)}$;*
(iv) *the order $G/\zeta_n(G)$ is a factor of $p^{h(m,n)}$.*

Here f, g, h are certain functions of m and n but not of r.

Again the classical case, which corresponds to $m = n = 1$, has been generalised. In particular, when $m = 1$ and so G has class $2n$, there are bounds on the orders of γ_{n+1} and G/ζ_n, but not on the order of ζ_n/γ_{n+1} as Theorem 5 will show.

Next we consider the class bounds in special cases; thus Theorem 3 (see Section 4) deals with groups for which $m = n = 2$. Finally we have examples.

THEOREM 4. *Let a prime $p \geqq 5$ be given. Then there is a finite p-group of class precisely 6 with every proper subgroup having class 3. In addition, the set of third Engel elements coincides with $\zeta_5(G)$, which has class 2.*

In this connection we note a result of Heineken [8, Satz 2]: every element a of order prime to 210, satisfying $(a, g, g, g) = 1$ and $(a^{-1}, g, g, g) = 1$ for all g in the group G, lies in $\zeta_k(G)$ where $k \leqq 2\cdot 3^9$. On the one hand this bound on k is generally thought to be large, on the other hand only the trivial lower bound $k \geqq 3$ seems known as yet. But Theorem 4 tells us that $k \geqq 5$.

THEOREM 5. *Let an odd prime p and positive integers m and n be given. Then there is a finite metacyclic p-group of class precisely $m + n$ with every subgroup of index p^m having class n. In addition, the group may be chosen so that ζ_n/γ_{n+1} has arbitrarily large order when $m = 1$.*

This example will serve to show that certain class bounds for small m and n are exact, but there is a big gap between the bound $m + n$ and the general bound given in Theorem 2(ii).

2. Preliminaries

Let $x_1, \cdots, x_n$ be a set of elements in a group G. Then $\{x_1, \cdots, x_n\}$ and $\langle x_1, \cdots, x_n\rangle$ denote respectively the least subgroup and the least normal subgroup in which the elements are contained. We shall denote $y^{-1}xy$ by

x^y and $x_1^{-1}x_2^{-1}x_1x_2$ by (x_1, x_2). For $n > 2$ we define the left-normed commutator $(x_1, \cdots, x_n)$ of weight n by induction:

$$(x_1, \cdots, x_n) = ((x_1, \cdots, x_{n-1}), x_n).$$

We repeat the standard list of commutator identities:

$$(2.1) \qquad (x^{-1}, y)^x = (x, y^{-1})^y = (x, y)^{-1},$$

$$(2.2) \qquad (uv, xy) = (u, y)^v(v, y)(u, x)^{vy}(v, x)^y,$$

$$(2.3) \qquad (z, x^{-1}, y)^x(x, y^{-1}, z)^y(y, z^{-1}, x)^z = 1.$$

It is easy to deduce

$$(2.4) \qquad (x, y, x^{-1}, y^{-1})^x(x, y, y^{-1}, x^{(x,y)}) = 1.$$

We say that G is metabelian whenever $(u, v; x, y) = 1$, defining $(u, v; x, y)$ to be $((u, v), (x, y))$, for all u, v, x, y in G. It is not difficult to show that in such a case we have

$$(2.5) \qquad (u, v, x, y) = (u, v, y, x),$$

and further that the value of $(x_1, \cdots, x_n)$ is unaltered when $x_3, \cdots, x_n$ are permuted in any way.

The members of the lower central series

$$G = \gamma_1 \geqq \gamma_2 \geqq \cdots \geqq \gamma_n \geqq \cdots$$

of G are defined thus: $\gamma_n = \gamma_n(G)$ is generated by the commutators $(x_1, \cdots, x_n)$ found as the x_i vary in G. Sometimes we write G' for $\gamma_2(G)$. The members of the upper central series

$$1 = \zeta_0 \leqq \zeta_1 \leqq \cdots \leqq \zeta_n \leqq \cdots$$

are defined thus: $\zeta_1 = \zeta_1(G)$ is the centre $Z(G)$ of G, and $\zeta_n = \zeta_n(G)$, when $n > 1$, is that subgroup of G for which $Z(G/\zeta_{n-1}) = \zeta_n/\zeta_{n-1}$. It can be shown that $\gamma_{n+1} = 1$ if and only if $\zeta_n = G$, in which case G is said to be "nilpotent of class n" or just "of class n". We shall say that the class of G is precisely n when the class is n but not $n - 1$.

Application of (2.3) and (2.4) in a group of class n, where $n \geqq 4$, gives

$$(2.6) \qquad \begin{aligned}&(x_1, \cdots, x_{n-2}; x_{n-1}, x_n)\\ &\quad = (x_1, \cdots, x_{n-2}, x_{n-1}, x_n)(x_1, \cdots, x_{n-2}, x_n, x_{n-1})^{-1},\end{aligned}$$

$$(2.7) \qquad (x, y, x, y, x_1, \cdots, x_{n-4}) = (x, y, y, x, x_1, \cdots, x_{n-4}).$$

It is easy to see that every two-generator subgroup in a group of class 4 is metabelian.

The Frattini subgroup $\Phi(G)$ of a finite p-group G is generated by G' and by the p^{th} powers of the elements of G. Such a group G is generated by n

elements but not by $n - 1$ if and only if the same is true of $G/\Phi(G)$, in which case $\Phi(G)$ has order p^{r-n} when G has order p^r.

Let x be an element of G for which $(x, y, \cdots, y) = 1$ for all $y \in G$, the commutator having weight $n + 1$. Then x is said to be an n^{th} Engel element, and if every element of G has this property G is said to satisfy the n^{th} Engel condition.

3. The general theorems

We assemble elementary facts in

LEMMA 1. *Let G be a finite p-group in which every maximal subgroup has class n. Then $\langle x\rangle$ has class n for each x in G, and G satisfies the $(n + 1)^{\text{st}}$ Engel condition. Further, if G has class precisely $2n$ then two elements generate G.*

Proof. Since $\langle x\rangle \leqq \{x, \Phi(G)\}$ and since either G is cyclic or $G/\Phi(G)$ is noncyclic, it follows that G is cyclic, or $\langle x\rangle$ is a proper subgroup of G and has class n. Consequently G satisfies the required Engel condition.

Suppose now that G has class precisely $2n$, and choose an element x in G but not in $\Phi(G)$. Then there is a maximal subgroup M of G such that $G = M\langle x\rangle$, which implies by Fitting's theorem that the class of $\langle x\rangle$ is precisely n. That is to say, there are elements $y, y_1, \cdots, y_{n-2}$ (we assume $n > 1$) for which

$$(x^y, x, x^{y_1}, \cdots, x^{y_{n-2}}) \neq 1.$$

Since it follows that

$$(x, y, x, x^{y_1}, \cdots, x^{y_{n-2}}) \neq 1$$

we see that $\langle x, y\rangle$ does not have class n; therefore $\{x, y\} = G$.

This completes the proof of Lemma 1.

Proof of Theorem 1. We shall assume that $n > 1$ and that G has class $2n$, and prove that G has class $2n - 1$. In accordance with Lemma 1 we choose a and b so that $G = \{a, b\}$. If

$$c = (x_1, \cdots, x_{2n}),$$

then $c = 1$ whenever $n + 1$ of the x_i are equal; we shall denote c by c_{ij} when

$$x_1 = a, \qquad x_2 = b,$$

$$x_3 = \cdots = x_{i+2} = a,$$

$$x_{i+3} = \cdots = x_{i+j+2} = b.$$

Therefore we have to prove that $c_{n-1,n-1} = 1$, as (2.5) makes clear.

Let us take c and put

$$x_1 = a, \qquad x_2 = \cdots = x_{n+2} = ab,$$

$$x_{n+3} = \cdots = x_{n+r+2} = a,$$

$$x_{n+r+3} = \cdots = x_{2n} = b,$$

where $0 \leqq r \leqq n-2$, so that $c = 1$. Expansion by means of (2.2) gives[1]

$$c_{n-1,n-1}^{C(n,n-r-1)} = 1.$$

It is well known that when n is composite the highest common factor of $C(n, n-r-1)$ for $0 \leqq r \leqq n-2$ is 1; consequently we suppose that n is a power of some prime p' and as $c_{n-1,n-1}^{n} = 1$ we shall take $p' = p$.

Since $\{a^i b, \Phi(G)\}$ has class n we find

$$(3.1) \qquad (a^p, a^i b, \cdots, a^i b) = 1 \qquad \text{for } 0 \leqq i \leqq p-1,$$

the left-normed commutator being of weight $n + 1$. By (2.2) we have

$$\begin{aligned}(a^p, a^i b) &= (a^p, b)\\ &= c_{00}^{p} \cdots c_{j0}^{C(p,j+1)} \cdots c_{p-1,0},\end{aligned}$$

and thus (3.1) gives, again with the use of (2.2),

$$(3.2) \qquad \begin{aligned}&(c_{00}, a^i b, \cdots, a^i b)^p \cdots (c_{j0}, a^i b, \cdots, a^i b)^{C(p,j+1)}\\ &\qquad \cdots (c_{p-1,0}, a^i b, \cdots, a^i b) = 1,\end{aligned}$$

where the commutators now have weight n.

We deduce from (3.2) with $i = 0$ that

$$c_{0,n-1}^{p} \cdots c_{j,n-1}^{C(p,j+1)} \cdots c_{p-1,n-1} = 1,$$

and hence that

$$(3.3) \quad c_{n-p+j,n-1}^{p} = 1 \quad \text{for} \quad p-1 \geqq j \geqq 1, \qquad c_{n-p,n-1}^{p}\, c_{n-1,n-1} = 1;$$

similarly

$$(3.4) \quad c_{n-1,n-p+j}^{p} = 1 \quad \text{for} \quad p-1 \geqq j \geqq 1, \qquad c_{n-1,n-p}^{p}\, c_{n-1,n-1} = 1.$$

Thus $\gamma_{2n}(G)$ has exponent p.

Now we prove by induction that $\gamma_{2n-p+j+1}$ has exponent p for $p - 2 \geqq j > 0$, assuming as we must that $p > 2$. Identities (3.3) and (3.4) make it clear that the result holds for $j = p - 2$. We assume inductively that $\gamma_{2n-p+j+2}$ has exponent p where j is fixed and $p - 3 \geqq j > 0$, and we consider commutators of weight $2n - p + j + 1$. The inductive hypothesis enables us to deduce from (3.2) that

$$(3.5) \qquad (c_{n-p+j,0}, a^i b, \cdots, a^i b)^p = 1.$$

In expanding this by means of (2.2) let us put $d_k = c_{n-p+j+k,n-k-1}^{C(n-1,n-k+1)}$, so that we find

$$(3.6) \qquad d_0^{p} \cdots d_k^{p\,i^k} \cdots d_{p-j-1}^{p\,i^{p-j-1}} = 1.$$

As (3.6) holds for $i = 0, 1, \cdots, p-j-1$, we have a system of equations which can be solved for $d_0^p, \cdots, d_k^p, \cdots, d_{p-j-1}^p$, and evaluation of the

[1] $C(n, m)$ denotes the number of combinations of n things taken m at a time.

elementary determinant which appears shows that

$$d_0^p = \cdots = d_k^p = \cdots = d_{p-j-1}^p = 1.$$

Because n is a power of p we have $C(n-1, n-k-1) \equiv (-1)^k$ modulo p, and so

$$c_{n-p+j+k,n-k-1}^p = 1 \qquad \text{for } 0 \leqq k \leqq p-j-1.$$

This and the inductive hypothesis show that $\gamma_{2n-p+j+1}$ has exponent p.

Whether $p = 2$ or not the exponent of γ_{2n-p+2} is therefore p. Next γ_{2n-p+1} is to be tackled by the method of the inductive step above—by (3.2) we have

$$(3.7) \qquad (c_{n-p,0}, a^ib, \cdots, a^ib)^p(c_{n-1,0}, a^ib, \cdots, a^ib) = 1,$$

and so if d_k denotes $c_{n-p+k,n-k-1}^{C(n-1\ n-k-1)}$ we have

$$d_0^p \cdots d_k^{p\,i^k} \cdots d_{p-1}^{p\,i^{p-1}} c_{n-1,n-1} = 1.$$

By (3.3) we have $d_0^p c_{n-1,n-1} = 1$. Solution of the system of equations gives $d_{p-1}^p = 1$, which with (3.4) implies that $c_{n-1,n-i} = 1$.

Therefore G has class $2n-1$. We conclude that the only possible value of n is 1, and this completes the proof of Theorem 1.

Proof of Theorem 2. (i) Suppose that every set of generators of G contains $m+n+1$ or more elements. Then the subgroup generated by any $n+1$ elements has order dividing p^r and class n; consequently G has class n. Therefore G has a set of at most $m+n$ generators.

This result can be improved when $n > 2$. A theorem of Heineken [7] states that if $n > 2$ and if every n elements of a group G generate a subgroup of class n then G has class n. Therefore if $n > 2$ our group has a set of at most $m+n-1$ generators.

(ii) Fitting's theorem shows that when $m = 1$ G has class $2n$, and induction on m shows that $f(m, n) \leqq 2^m n$.

(iii) By (i) and (ii) we may assume that $G = \{a_1, \cdots, a_s\}$ where $s \leqq m+n$ and that G has class $f = f(m, n)$. For $1 \leqq i \leqq f-n$ the abelian groups $\gamma_{n+i}/\gamma_{n+i+1}$ are generated by a number of commutators like $(a_{j_1}, \cdots, a_{j_{n+i}})\gamma_{n+i+1}$ where $1 \leqq j_k \leqq s$, and this number is clearly bounded by a function of m and n. We shall show that each of these commutators has order dividing p^{mf}.

Because the subgroup $\{a_1^p, \cdots, a_s^p\}$ is contained in $\Phi(G)$ its index in G is at least $\min(p^2, p^{r+m})$. Similarly $\{a_1^{p^2}, \cdots, a_s^{p^2}\}$ lies in $\Phi(\Phi(G))$ and its index is at least $\min(p^4, p^{r+m})$. This argument with induction shows that $\{a_1^{p^m}, \cdots, a_s^{p^m}\}$ has index at least $\min(p^{2m}, p^{r+m})$ in G, and hence class n. Consequently

$$(a_{j_1}^{p^m}, \cdots, a_{j_{n+i}}^{p^m}) = 1,$$

$$(a_{j_1}, \cdots, a_{j_{n+i}})^{p^{m(n+i)}}\gamma_{n+i+1} = \gamma_{n+i+1},$$

for $1 \leqq i \leqq f-n$. Thus the commutators $(a_{j_1}, \cdots, a_{j_{n+i}})\gamma_{n+i+1}$ have orders dividing p^{mf}, which is the link showing that $\gamma_{n+i}/\gamma_{n+i+1}$ has its order bounded by a function p^{g_0} where $g_0 = g_0(m, n)$. Since $\gamma_{f+1} = 1$ we conclude that the order of γ_{n+1} is bounded by p^g, for a suitable function $g = g(m, n)$, and that proves (iii).

(iv) Since G/ζ_n has class f, since by (i) G/ζ_n is generated by at most $m + n$ elements, and since we shall show that G/ζ_n has finite exponent of the appropriate form, it will follow that the order of G/ζ_n is bounded by some function $p^{h(m,n)}$. In fact we shall prove that $x^{p^{fg}} \in \zeta_n$ for all $x \in G$.

Let $x_1, \cdots, x_n$ be arbitrary elements of G. Repeated applications of (2.2) and (2.3) show that

$$(x^{p^{fg}}, x_1, \cdots, x_n) = (x^{p^{(f-1)g}}, x_1, \cdots, x_n)^{p^g} c = c$$

by (iii), where c is the product of conjugates of left-normed commutators and inverses of weight $n + 2$ or more, with $x^{p^{(f-1)g}}$ occurring at least once in each. We continue this process with each of the commutators in c. The general step consists in expanding a left-normed commutator of weight $n + i$ where $1 \leqq i \leqq f - n$, in which $x^{p^{(f-i+1)g}}$ occurs; the result is by (iii) the product of conjugates of left-normed commutators of weight $n + i + 1$ or more, in each of which $x^{p^{(f-i)g}}$ occurs. Since $\gamma_{f+1} = 1$ we find that

$$(x^{p^{fg}}, x_1, \cdots, x_n) = 1,$$

and that G/ζ_n has exponent p^{fg}. That completes the proof of (iv) and of the theorem.

4. Some cases with small m and n

In this section G will denote a group of order p^{r+m} in which every subgroup of order p^r has class n, and we shall look at class bounds in special cases other than the classical case $m = n = 1$.

COROLLARY 1 TO THEOREM 1. *Let G be a group of order p^{r+1} in which every subgroup of order p^r has class 2. Then G has class 3.*

Proof. Clearly G has class 4, and by Theorem 2 we may assume that G has at most three generators. If no two elements generate G then each $\{x, y\}$ is a proper subgroup and has class 2. Thus G satisfies the second Engel condition, the facts about which are recorded on p. 322 of [3]. They lead us to the conclusion that G has class 3, and even class 2 if $p \neq 3$.

If two elements generate G then G is metabelian. Therefore Theorem 1 shows that the class of G cannot be precisely 4, and so is 3.

COROLLARY 2 TO THEOREM 1. *Let G be a group of order p^{r+2} in which every subgroup of order p^r is abelian. Then G has class 3.*

Proof. This is an immediate consequence of Corollary 1.

When $m = 1$ and $n = 3$ we have 6 for the class of G, and Theorem 4 will show that sometimes the class is precisely 6. The crude means at out disposal enable us to say a little more about this case when G is generated by precisely three elements. Then $\{x, y\}$ is a proper subgroup and G satisfies the third Engel condition, which has been investigated by Heineken in [6]. His results tell us that G has class 4 if $p \neq 2$ and $p \neq 5$.

We now consider the case $m = n = 2$, which is harder.

THEOREM 3. *Let G be a group of order p^{r+2} in which every subgroup of order p^r has class 2. Then the class of G is 4; and G is metabelian if $p = 2$.*

Proof. We know from Theorem 2 that either G has class 2 or G can be generated by a set of fewer than five elements. By the results for $m = 1$, every proper subgroup has class 3 and G has class 6.

If G is not generated by any set of three elements then every $\{x, y\}$ in G has class 2 and the second Engel condition holds. Thus G has class 3, G is metabelian, and if the class is precisely 3 then $p = 3$.

Next suppose that G cannot be generated by any pair of its elements. If every maximal subgroup has less than three generators a theorem of Blackburn (see [1, Theorem 3.1]) enables us to establish that G has class 2. Assume therefore that there is a maximal subgroup M generated by no pair of its elements, so that $p = 3$ or M has class 2 by the results for $m = 1$ and $n = 2$ applied to M. Since $G = M\langle x\rangle$ for some $x \notin M$ we see that G has class 4 or $p = 3$, but in the latter case the fact that G satisfies the third Engel condition proves that G has class 4 anyway.

Let $G = \{a, b, c\}$. To show that G is metabelian it will suffice to verify that $(a, b; a, c) = 1$. We start by using (2.6):

$$(a, b; a, c) = (a, b, a, c)(a, b, c, a)^{-1}.$$

Since $\{x, \Phi(G)\}$ has class 2, and now $p = 2$,

$$((a, b), ac, ac) = 1,$$

$$(a, b, a, c)(a, b, c, a) = 1.$$

Hence we have

$$(a, b; a, c) = (a, b, a, c)^2.$$

Since $\{a, \Phi(G)\}$ has class 2,

$$1 = ((a, b), a, c^2) = (a, b, a, c)^2,$$

and so $(a, b; a, c) = 1$; G is metabelian.

We are left with the formidable final case in which G can be generated by two elements a and b.

If each maximal subgroup is generated by a suitably chosen pair of elements we have a situation in which further theorems of Blackburn can be brought to bear. Theorems 4.2 and 5.1 of [1] assert that G has order dividing p^5 (and so class 4), or G is metacyclic, or G/γ_3 has order p^3 and γ_3 coincides with the subgroup P_1 generated by the p^{th} powers of the elements of G. If G is metacyclic then we may suppose that $\{a\}$ is normal while $\langle b\rangle$ has class 3 as usual, so $G = \langle a\rangle\langle b\rangle$ has class 4. If G/γ_3 has order p^3 and $\gamma_3 = P_1$ then each $\{x, \gamma_3\}$ has class 2 and the identity

$$(u, v, w, x, x) = 1$$

follows; in order to prove that G has class 5 it will suffice to show that $(a, b, a, b, a, b) = 1$. Since

$$(a, b, a, b, a, b) = (a, b, b, a, a, b),$$

by (2.7), G does indeed have class 5. Considering commutators of weight 5 we find that

$$\begin{aligned}(a, b, a, ab, ab) &= 1,\\ (a, b, a, a, b) &= (a, b, a, b, a)^{-1}\\ &= (a, b, b, a, a)^{-1},\end{aligned}$$

the last step following from (2.7). These facts are enough to establish that G has class 4.

In the next situation to be considered there exists a maximal subgroup $M = \{a, \Phi(G)\}$ of G which cannot be generated by any pair of its elements. Application to M of the facts for the case $m = 1$ and $n = 2$ contained in the proof of Corollary 1 above shows that M is second Engel, and so of class 3 if $p = 3$ and of class 2 otherwise. Hence $G = M\langle b\rangle$ has class 6 if $p = 3$ and class 5 otherwise.

Considering the case $p = 3$ we show that the classes of G and M are in fact 5 and 2 respectively. Note carefully that $(x, a, a) = 1$ for all x in M. The fact that the class of $\langle ab\rangle$ is 3 gives

$$(a, ab, ab, a, ab, ab) = 1, \qquad (a, b, b, a, b, a) = 1.$$

Thus we may deduce by means of (2.7) that

$$(a, b, a, b, b, a) = 1.$$

Similarly (2.7) gives

$$(a, b, a, b, a, b) = (a, b, b, a, a, b) = 1,$$

and we see that G has class 5. In M we have the laws

$$(x, y, z) = (y, z, x) = (y, x, z)^{-1},$$

as shown on p. 322 of [3], and M is generated by a, b^3 and the commutators in G. The classes of G and M being what they are, it will follow that M has class 2 as soon as we prove that $(c, a, b^3) = 1$ where c is any commutator in G, and where we can assume that c is of weight 2 or 3. If $c = (a, b)$ we have

$$\begin{aligned}((a, b)\ a, b^3) &= (a, b^3, (a, b))\\ &= ((a, b)^3(a, b, b)^3, (a, b))\\ &= (a, b, b, (a, b))^3\\ &= ((a, b), b^3, (a, b))\\ &= 1.\end{aligned}$$

If $c = (a, b, a)$ we have

$$((a, b, a), a, b^3) = ((a, b), a, a, b^3)$$
$$= 1.$$

If $c = (a, b, b)$ we have

$$((a, b, b), a, b^3) = (a, b, (a, b, b))^3$$
$$= ((a, b), b^3, (a, b))^{-1}$$
$$= 1.$$

Therefore M has class 2.

It is now our intention to prove that G has class 4, first in the case which arises when p is odd. If the subgroup $\{b, (a, b)\}$ is not maximal then it has class 2 and so, as we shall prove, does $\langle b\rangle$. We have

$$(b^x, b, b^y) = (b, x, b; b, y)(b, x, b, b),$$

by (2.2). Since $\{b, (a, b)\}$ has class 2 we have

$$(b, a, b; b, a) = 1$$

and hence

$$(b, x, b; b, y) = 1.$$

If $x = a^\alpha b^\beta c$ with $c \in G'$ then use of (2.2) gives

$$\begin{aligned}(b, x, b, b) &= (b, c, b, b)(b, a^\alpha, b, b)(b, a^\alpha, b^\beta c, b, b)\\ &= (b, a^\alpha, b, b)\\ &= (b, a, b, b)^\alpha (b, a, a, b, b)^{\alpha(\alpha-1)/2}\\ &= (b, a, a, b, b)^{\alpha(\alpha-1)/2}\end{aligned}$$

since $\{b, (a, b)\}$ has class 2, and it remains to consider (b, a, a, b, b). Thus

$$\begin{aligned}(b, a, a, b, b) &= (b, a, b, b)^{-1}((b, a)^a, b, b)\\ &= (b, a, b^{a^{-1}}, b^{a^{-1}})^a\\ &= (b, a, b(b, a)^{-1}, b(b, a)^{-1})^a\\ &= 1.\end{aligned}$$

We have now shown that $(b^x, b, b^y) = 1$, so $\langle b\rangle$ and $G = M\langle b\rangle$ have classes 2 and 4 respectively.

At this point we may suppose that $\{b, (a, b)\}$ is maximal and so contains (a, b, a):

$$(a, b, a) = b^{\beta_1}(a, b)^{\beta_2}(a, b, b)^{\beta_3} \quad \text{modulo } \gamma_4(G),$$

$$(a, b, a, b, b) = (a, b, b, b)^{\beta_2},$$

$$1 = (a, b, b, b, a)^{\beta_2},$$

for some β_1, β_2, β_3. Since M has class 2 we find

$$((a, b, b), b^p, a) = 1, \qquad (a, b, b, b, a)^p = 1.$$

Therefore either G has class 4 or $\beta_2 \equiv 0$ modulo p. Since $\{b, \Phi(G)\}$ has class 3 we find

$$(a^p, b, b, b) = 1,$$
$$(a, b, b, b)^p(a, b, a, b, b)^{p(p-1)/2} = 1.$$

This with the fact that $(a, b, a, b, b) = (a, b, b, b)^{\beta_2}$ shows that $(a, b, b, b)^p = 1$ and $(a, b, a, b, b) = 1$, and by means of (2.7) we deduce that $(a, b, b, a, b) = 1$. Finally, expansion of

$$(a, ab, ab, ab, ab) = 1$$

will show that $(a, b, b, b, a) = 1$, so G has class 4.

There remains the case $p = 2$. Since $M = \{a, \Phi(G)\}$ has class 2, we find after manipulation of (2.4) with $x = b$ and $y = a$ that

$$(a, b, a, b) = (a, b, b, a).$$

Further

$$((a, b), a, b^2) = 1,$$
$$(a, b, a, b)^2(a, b, a, b, b) = 1;$$
$$((a, b), b^2, a) = 1,$$
$$(a, b, b, a)^2(a, b, b, b, a) = 1.$$

This establishes the relation

$$(a, b, a, b, b) = (a, b, b, b, a),$$

and of course we have

$$(a, b, a, b, b) = (a, b, b, a, b)$$

by (2.7). Now expansion of

$$(a, ab, ab, ab, ab) = 1$$

will lead to

$$(a, b, a, b, b)^3 = 1;$$

since $p = 2$ we have $(a, b, a, b, b) = 1$, and G has class 4.

We have thus proved that if G is generated by two elements then G has class 4. As it follows at once that G is metabelian the proof of Theorem 3 is complete.

Corollary to Theorem 3. *Let G be a group of order p^{r+3} in which every subgroup of order p^r is abelian. Then the class of G is 4, and G is metabelian.*

5. The examples

Proof of Theorem 4. Some of the numerous but easy details in the construction of the required group G will be omitted in order to shorten the exposition. We start from a group A isomorphic to G' and reach G by two cyclic extensions.

Let A_0 be the group generated by the elements c, d_1, d_2 and defined by the relations

$$c^p = d_i^p = 1, \qquad (d_i, c) = f_i^6, \qquad (d_1, d_2) = z^6,$$

$$(c, f_i) = (d_i, f_j) = (c, z) = (d_i, z) = 1,$$

where i and j each take the values 1 and 2. Thus A_0 has class 2 and order p^6. Let elements e_i generate groups of order p where $1 \leqq i \leqq 3$, and define A to be the direct product of A_0, $\{e_1\}$, $\{e_2\}$, $\{e_3\}$.

Now the group A has an automorphism α such that

$$c\alpha = cd_1, \qquad d_1\alpha = d_1 e_1, \qquad d_2\alpha = d_2 e_2 f_1^{-6} f_2^{-6} z^{-6},$$

$$e_1\alpha = e_1, \qquad e_2\alpha = e_2 f_1^{-2} z^{-1}, \qquad e_3\alpha = e_3 f_2^{-4} z^{-1}.$$

It is easy to verify that α is an automorphism and that

$$f_1\alpha = f_1, \qquad f_2\alpha = f_2 z^{-1}, \qquad z\alpha = z;$$

the fact that α has order p follows from the identities

$$c\alpha^r = c\, d_1^r\, e_1^{C(r,2)}, \qquad d_2\alpha^r = d_2\, e_2^r (f_2^{-6})^r (f_1^{-6} z^{-6})^r (f_1^{-2} z^{-1})^{C(r,2)} z^{6C(r,2)}$$

which hold for any positive integer r. Form the splitting extension of A by a group of order p, a generator of which induces α in A. This gives $B = \{A, a\}$ in which defining relations are those of A and

$$a^p = 1, \qquad (c, a) = d_1,$$

$$(d_1, a) = e_1, \qquad (d_2, a) = e_2 f_1^{-6} f_2^{-6} z^{-6},$$

$$(e_1, a) = 1, \qquad (e_2, a) = f_1^{-2} z^{-1}, \qquad (e_3, a) = f_2^{-4} z^{-1}.$$

The group B has an automorphism β such that

$$a\beta = ac, \qquad c\beta = cd_2,$$

$$d_1\beta = d_1 e_2, \qquad d_2\beta = d_2 e_3,$$

$$e_1\beta = e_1 f_1^4 z^{-1}, \qquad e_2\beta = e_2 f_2^2 z^5, \qquad e_3\beta = e_3,$$

from which it follows that

$$f_1\beta = f_1 z, \qquad f_2\beta = f_2, \qquad z\beta = z.$$

A calculation typical of those verifying that β is an automorphism is the following:

$$
\begin{aligned}
(c\beta, a\beta) &= (cd_2, ac) \\
&= (d_2, c)(c, a)^{d_2 c}(d_2, a)^c \\
&= f_2^6 \cdot d_1^{d_2 c} \cdot (e_2 f_1^{-6} f_2^{-6} z^{-6})^c \\
&= f_2^6 \cdot d_1 z^6 f_1^6 \cdot e_2 f_1^{-6} f_2^{-6} z^{-6} \\
&= d_1 e_2 \\
&= (c, a)\beta.
\end{aligned}
$$

The most difficult step in establishing that β has order p comes from the identity

$$a\beta^r = ac^r d_2^{C(r,2)} e_3^{C(r,3)} f_2^{6C(r,3)},$$

which holds for any positive integer r. Form the splitting extension of B by a group of order p, a generator of which induces β in B. This gives $G = \{B, b\}$ in which defining relations are those of B and

$$b^p = 1, \qquad (a, b) = c,$$

$$(c, b) = d_2, \qquad (d_1, b) = e_2, \qquad (d_2, b) = e_3,$$

$$(e_1, b) = f_1^4 z^{-1}, \qquad (e_2, b) = f_2^2 z^5, \qquad (e_3, b) = 1.$$

It is clear that G has order p^{11} and that $G' \cong A$. The class of G is at least 6 because

$$
\begin{aligned}
(a, b, a, b, a, b) &= (c, a, b, a, b) \\
&= (d_1, b, a, b) \\
&= (e_2, a, b) \\
&= (f_1^{-2} z^{-1}, b) \\
&= z^{-2}.
\end{aligned}
$$

Thus it will follow that G has class precisely 6 when we have shown that each maximal subgroup M has class 3. We may take M to be $\{a^\xi b^\eta, G'\}$ with $0 < \xi < p$ or $0 < \eta < p$. After some calculation we have

$$
\begin{aligned}
\gamma_2(M) &= \{d_1^\xi d_2^\eta e_1^{-\xi/2} e_3^{-\eta/2}, e_1^\xi e_2^\eta, e_2^\xi e_3^\eta, f_1, f_2, z\}, \\
\gamma_3(M) &= \{e_1^{\xi^2} e_2^{2\xi\eta} e_3^{\eta^2} f_1^{-7\xi\eta} f_2^{-5\xi\eta}, f_1^\xi f_2^\eta, z\}, \\
\gamma_4(M) &= 1;
\end{aligned}
$$

the details are omitted. The class of G is precisely 6.

Next we consider the Engel properties of G. It is clear that if $g \in G'$ then $\{x, g\}$ has class 3 and $(g, x, x, x) = 1$. If $g \notin G'$ then $g = a^\xi b^\eta g'$ where $0 < \xi < p$

or $0 < \eta < p$, and $g' \epsilon G'$; suppose $0 < \xi < p$. Working modulo $\gamma_5(G)$ we have

$$(a^{\xi} b^{\eta} g', b, b, b) \equiv (a, b, b, b)^{\xi} \equiv e_3^{\xi},$$

so $(g, b, b, b) \notin \gamma_5(G)$, and $(g, b, b, b) \neq 1$. Thus if $g \notin G'$ then g is not a third Engel element. Clearly $G' = \zeta_5(G)$ as G has class precisely 6 and G/G' has order p^2, so we have proved all the assertions in Theorem 4.

It is of interest that G satisfies the fourth Engel condition, by Lemma 1; and that if $p > 5$ then G has exponent p as it is a regular p-group generated by elements of order p (see [4, Theorem 4.26]).

Proof of Theorem 5. Consider the group G generated by elements a and b with defining relations

$$a^b = a^{1+p}, \qquad a^{p^{m+n}} = 1, \qquad b^{p^{m+n-1}} = 1.$$

It is easily verified that the order is $p^{2m+2n-1}$ and that the class is precisely $m + n$.

Now any subgroup S of G is cyclic modulo $S \cap \{a\}$. Therefore if S has order p^{m+2n-1} we may suppose that elements a^{p^r} and $b^{p^s}a^{\alpha}$ generate S, where $0 \leqq r \leqq m + n$ and $0 \leqq s \leqq m + n - 1$. The order of a^{p^r} is p^{m+n-r}, and the order modulo $\{a\}$ of $b^{p^s}a^{\alpha}$ is $p^{m+n-s-1}$, so on considering the order of S we arrive at the inequality

$$m + 2n - 1 \geqq (m + n - r) + (m + n - s - 1),$$
$$r + s \geqq m.$$

The left-normed commutator $(a^{p^r}, b^{p^s}a^{\alpha}, \cdots, b^{p^s}a^{\alpha})$ of weight $i + 1$ is equal to $a^{\omega(i)}$ since it must lie in $\{a\}$, and it may be shown by induction that

$$\omega(i) = \{ -1 + (1 + p)^{p^s}\}^i p^r$$

for all $i > 0$. Since $p > 2$, $p^{(s+1)n+r}$ is a factor of $\omega(n)$; and

$$(s + 1)n + r \geqq (r + s) + n \geqq m + n.$$

Therefore $a^{\omega(n)} = 1$. It follows that S has class n.

The modification when $m = 1$ consists in replacing the third defining relation $b^{p^n} = 1$ by $b^{p^{n+k}} = 1$, and we omit the proof that G still has the required properties together with the property that ζ_n/γ_{n+1} has order p^{2n+k-2}.

Theorem 5 shows that, for p odd, the class bounds in the corollaries to Theorem 1, in Theorem 3 and in the corollary to Theorem 3 are best possible. But the bound $m + n$ is not always best possible, as Theorem 4 showed in the case $m = 1$ and $n = 3$.

References

1. N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. (3), vol. 11 (1961), pp. 1–22.

2. H. Fitting, *Beiträge zur Theorie der Gruppen endlicher Ordnung*, Jber. Deutsch. Math. Verein., vol. 48 (1938), pp. 77–141.
3. M. Hall, *The theory of groups*, New York, Macmillan, 1959.
4. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2), vol. 36 (1934), pp. 29–95.
5. ———, *Some sufficient conditions for a group to be nilpotent*, Illinois J. Math., vol. 2 (1958), pp. 787–801.
6. H. Heineken, *Engelsche Elemente der Länge drei*, Illinois J. Math., vol. 5 (1961), pp. 681–707.
7. ———, *Über ein Levisches Nilpotenzkriterium*, Arch. Math., vol. 12 (1961), pp. 176–178.
8. ———, *Endomorphismenringe und engelsche Elemente*, Arch. Math., vol. 13 (1962), pp. 29–37.
9. K. Iwasawa, *Über die Struktur der endlichen Gruppen, deren echte Untergruppen sämtlich nilpotent sind*, Proc. Phys. - Math. Soc. Jap., vol. 23 (1941), pp. 1–4.
10. G. A. Miller and H. C. Moreno, *Non-abelian groups in which every subgroup is abelian*, Trans. Amer. Math. Soc., vol. 4 (1903), pp. 398–404.
11. L. Rédei, *Das schiefe Produkt in der Gruppentheorie*, Comment. Math. Helv., vol. 20 (1947), pp. 225–264.
12. O. Schmidt, *Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind*, Rec. Math. Moscou, vol. 31 (1924), pp. 366–372.
13. M. Suzuki, *The nonexistence of a certain type of simple groups of odd order*, Proc. Amer. Math. Soc., vol. 8 (1957), pp. 686–695.

The Australian National University
Canberra, Australia